H 7625

FIfF-Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

27. Jahrgang 2010 Einzelpreis: 7 EUR

4/2010 - Dezember 2010

@Welt

ISSN 0938-3476

• Jahrestagung • Studienpreis • Volkszählung • Personalausweis •

FIfF-Kommunikation

Titelbild: @Welt
von Berthold Schroeder

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Inhalt

Ausgabe 4/2010

inhalt

Editorial

Wer sich in den letzten Ausgaben der FIfF-Kommunikation die vorletzte Seite jeweils aufmerksam durchgelesen hat, wird sich beim Anblick des Covers und dem Titel „@Welt“ ein wenig gewundert haben. Eigentlich sollte es in dieser Ausgabe einen Schwerpunkt zu Verkehrsthemen geben, den wir aber leider kurzfristig auf eine Ausgabe im nächsten Jahr verschieben müssen. Denn zum einen ist es gar nicht mal so einfach, bei all den Innovationen beim Einsatz von Informatik auch kritische Töne zu finden, die sich etwas distanzierter mit der Thematik befassen. Zum anderen sind viele dieser Leute im Moment mit tagesaktuellen Themen – hier im Speziellen der Protest gegen Stuttgart 21 – vielfach ausgelastet. Wir werden den Schwerpunkt auf jeden Fall weiter verfolgen, denn es gibt dabei viele interessante Entwicklungen, auf die es sich lohnt, ein Auge zu werfen

Nun stattdessen also „@Welt“ als Subsumierung der aktuellen Themen, mit denen sich kritische Informatik im Moment befassen muss. Ein Glücksfall scheint für die kritische Informatik seit einiger Zeit zu sein, dass ihr die Themen nie auszugehen scheinen, ja sogar im Gegenteil immer mehr werden. Insbesondere in Deutschland richtet sich immer mehr Aufmerksamkeit auf die Beurteilung von informationstechnischen Neuerungen, was sich unter anderem zeigt an den immer häufigeren Erwähnungen selbst in wichtigen, „gestandenen“ Nachrichtenformaten wie der *Tagesschau*. *Michael Ebeling*, *Thilo Weichert* und *Werner Hülsmann* beschäftigen sich in ihren Artikeln mit dem kommenden Zensus 2011 und der Geschichte der Volkszählung in Deutschland, *Herbert Kubicek* mit dem neuen Personalausweis, und *Lew Palm* beleuchtet die Überwachung in Arztpraxen.

International wird es dann mit den Artikeln von *Jochen Topf* über die Kartenalternative *Open Street Maps* und dem Workshop-Bericht von *Wolfgang Coy* zum Bann autonomer Waffensysteme. *Nazir Peroz* berichtet von nachhaltigen IT-Versorgungssystemen an afghanischen Hochschulen. Dann geht es um das Studienprogramm *Informatik für Migrantinnen und Migranten*, welches von *Susanne Boll, Rolf Meinhardt, Sabine Gronewold* und *Larissa Krekeler* vorgestellt wird, und die Medienbildung in einer digital geprägten Kultur, über die Ralf E. Streibl *Heidi Schelhowe* interviewt. Es folgt konkrete Technik, wenn *Maike Hecht*, *Carola Schirmer* und *Susanne Maaß* Erkenntnisse einer Studie über Diversität und Beteiligung in Software-Migrationsprozessen zusammenfassen. *Dagmar Boedicker* rundet dies im Anschluss noch mit *Datenschutz* ab*, für den man keinen Euro zahlt*.

Nicht zu vergessen sind natürlich die Neuigkeiten aus dem FIfF: Neben der wiederum erfolgreich durchgeführten Jahrestagung, die dieses Mal zusammen mit der DVD in der alten Feuerwache in Köln veranstaltet wurde, gibt es zum ersten Mal Ergebnisse des im letzten Jahr beschlossenen Studienpreises. Somit finden sich ein Kurzbericht der Jahrestagung in dieser Ausgabe, das Protokoll der Mitgliederversammlung sowie ein Rückblick auf die Preisverleihung nebst dem Jury-Ergebnis. Zwei der Preisträger – namentlich *Andrea Knaut* und *Michael Prinziger* – geben darüber hinaus auch einen Einblick in ihre Arbeiten.

Abschließend sei festgehalten, dass die oben aufgestellte These zur wachsenden Zahl aktueller Themen, in welche sich kritische Informatik einmischen muss, fast schon allein durch die Art und Weise der Entstehung dieses Hefts bewiesen ist. Was als Notruf begonnen hat, ist binnen kürzester Zeit zu einer vielfältigen Sammlung von Artikeln geworden, deren Aktualität zeigt, wie wichtig es ist, am Ball zu bleiben. Wir wünschen eine angenehme Lektüre des vorliegenden Hefts und einen erfolgreichen Start in das Jahr 2011.

Carsten Büttemeier und Stefan Hügel
für die Redaktion.

Schwerpunktredaktion

Stuttgart und anderswo

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

eines der beherrschenden Themen der letzten Wochen ist der Protest gegen *Stuttgart 21* – und die Reaktionen darauf. Ich meine damit weniger den Umgang einzelner Polizeibeamter mit Bürgern, die ihre demokratischen Rechte wahrnehmen. Interessanter sind die Reaktionen in der Politik und in manchen Medien: Während einige eine neue Protestkultur begrüßen, die im Gegensatz zu früher auch das gehobene Bürgertum einbindet, sehen manche die Beteiligung der Bevölkerung als Gefahr: „Deutschland droht der totale Stillstand", so war auf *Spiegel Online*, dem Internet-Ableger des „Sturmgeschützes der Demokratie" zu lesen.

Verscherzt sich das Volk gerade das Vertrauen der Regierung – oder nur des *Spiegel*? „Wäre es da nicht doch einfacher, die Regierung löste das Volk auf und wählte ein anderes?" schrieb Bertolt Brecht 1953 – freilich in anderem Zusammenhang.

Neben Demokratie und Bürgerrechten interessiert das FIfF stets auch die Militärpolitik. Hier wird eine besorgniserregende Entwicklung immer offener betrieben: Vor kurzem noch ist Horst Köhler vom Amt des Bundespräsidenten aufgrund eines Interviews zurückgetreten, in dem er unter anderem die Sicherung freier Handelswege als legitimes Ziel deutscher Militärpolitik bezeichnete. Er löste damit große Empörung in der politischen Szene aus – ich hatte an dieser Stelle darauf hingewiesen.

Nun sprach sich auch Bundesverteidigungsminister *Karl-Theodor zu Guttenberg* nach einem Bericht der Zeit dafür aus, in der Militärpolitik „‚offen und ohne Verklemmung' auf wirtschaftliche Interessen einzugehen. Denn dieser Zusammenhang sei im Grunde etwas Selbstverständliches."

Etwas Selbstverständliches? Wirklich?

Womit wir wieder bei der IT-Politik wären: Zu Guttenbergs Ehefrau *Stephanie*, Präsidentin der Kinderschutzorganisation *Innocence in Danger* – die vehement Internet-Sperren als Mittel des Kinderschutzes anpreist –, macht gerade im Fernsehen von sich reden: *Tatort Internet – wer schützt unsere Kinder*, so lautet der Titel einer neuen Serie des Privatsenders RTL2, an der sie als Moderatorin beteiligt ist. Der Sender, dem die Welt sonst eine Reihe eher zwielichtiger Sendungen verdankt, hat sich nun also dem Kinderschutz verschrieben.

Die Sendung berichtet über den Missbrauch von Kindern und die Gefahren des Internet – ein sicherlich wichtiges und ehrenwertes Anliegen. Wenn das aber zur Sensationsmache verkommt, bei der Persönlichkeitsrechte – auch die der Opfer – scheinbar zweitrangig sind, kann man die eigentliche Zielsetzung der Sendung schon hinterfragen. Andere Kinderschutzorganisationen haben sich Berichten zufolge bereits von der „reißerischen und vorurteilsstärkenden" Darstellung distanziert.

Eine effektivere Bekämpfung der Kriminalität versprechen sich deren Befürworter auch von der Vorratsdatenspeicherung – akzeptanzfördernd nun „Mindestspeicherfrist" genannt. Im September sind wieder Tausende auf die Straße gegangen, um unter dem Motto „Freiheit statt Angst" dagegen zu demonstrieren. Doch nun scheint die Front zu bröckeln: Der Bundesdatenschutzbeauftragte Peter Schaar hat sich für eine Vorratsdatenspeicherung mit einer Speicherfrist von zwei Wochen ausgesprochen – und damit heftiger Kritik ausgesetzt. Er begründet den Vorstoß mit der Notwendigkeit, alternative, datenschutzfreundliche Lösungen aufzuzeigen. Der Datenschutzbeauftragte Schleswig-Holsteins, Thilo Weichert, unterstützt diesen Vorschlag. Die Konferenz der Datenschutzbeauftragten Anfang November hatte erklärt, an der „grundsätzlich ablehnenden Haltung" festhalten zu wollen, sich aber mit „Alternativen zum massenhaften anlass- und verdachtslosen Speichern von Verkehrsdaten der Telekommunikation auseinanderzusetzen". Ob eine bloße Verkürzung der Speicherfrist da ausreicht?

Zurück zum FIfF. Gerade ist in Köln die diesjährige Jahrestagung zu Ende gegangen. Gemeinsam mit der Deutschen Vereinigung für Datenschutz diskutierten wir zwei Tage lang unter dem Motto *transparenz.arbeit.kontrolle* über Beschäftigtendatenschutz – eine gelungene Tagung, für die ich allen Mitwirkenden herzlich danke. Ein erster Bericht ist auf den folgenden Seiten zu lesen.

Ein schönes Ergebnis der Arbeit im FIfF sahen wir am Samstagabend während der Tagung. Den *FIfF-Studienpreis*, letztes Jahr durch die Mitgliederversammlung eingerichtet, haben wir erstmals verliehen. Vielen Dank an dieser Stelle für die Einreichungen und allen Beteiligten für ihre Mitarbeit. Besonders möchte ich an dieser Stelle auch Raffael Rittmeier danken, dem wir die Initiative für den Studienpreis zu verdanken haben.

Licht und Schatten gab es dann auf der Mitgliederversammlung am Sonntag. Licht, wenn man das große Spektrum der Aktivitäten im FIfF des letzten Jahres betrachtet – Schatten, angesichts der finanziellen Situation, die sich vor allem aus gestiegenen Fixkosten ergibt. Nach kontroverser Diskussion im Vorstand hatten wir bei der Mitgliederversammlung einen Antrag auf Änderung der Mitgliedsbeiträge gestellt. Die Mitgliederversammlung ging nun – ebenfalls nach kontroverser Diskussion – sogar über unseren Antrag hinaus. Die Ergebnisse sind im Protokoll der Mitgliederversammlung auf Seite 7 nachzulesen. Beitragserhöhungen sind immer unerfreulich - ich bitte alle Mitglieder, auch den künftigen Weg mit dem FIfF zu gehen.

Wenn dieses Heft erscheint, ist das Jahr 2010 fast vorbei. Ich wünsche allen Leserinnen und Lesern und dem FIfF ein gutes und erfolgreiches Jahr 2011.

Mit fiffigen Grüßen

Stefan Hügel

Stefan Hügel

transparenz.arbeit.kontrolle

Jahrestagung 2010 gemeinsam mit der DVD in Köln

Am Sonntag, den 7. November 2010, ist mit den Mitgliederversammlungen von FIfF und DVD – der Deutschen Vereinigung für den Datenschutz e.V. – die gemeinsame Jahrestagung der beiden Organisationen zu Ende gegangen. Unter dem Motto ***transparenz. arbeit.kontrolle*** *haben sich ca. 100 Mitglieder und Freunde von DVD und FIfF – darunter viele Datenschutzexperten – zwei Tage lang mit dem Thema Beschäftigtendatenschutz auseinandergesetzt. Auf der Tagung haben wir auch erstmalig den Studienpreis des FIfF verliehen. Mit dem Preis wollen wir herausragende Arbeiten auszeichnen, die die gesellschaftlichen Auswirkungen der Informatik und Informationstechnik zum Thema haben.*

„Die Datenschutzdiskussionen der letzten zwei Jahre haben gezeigt, dass nicht nur der Datenhunger staatlicher Stellen begrenzt werden muss. Auch die Begehrlichkeiten der Privatwirtschaft haben ein teilweise erschreckendes Ausmaß angenommen", erläuterte *Karin Schuler*, Vorsitzende der DVD. *Stefan Hügel*, Vorsitzender des FIfF ergänzt: „Wir haben in den vergangenen Monaten Datenschutzverletzungen in einem Umfang miterlebt, den wir nicht mehr hinnehmen können. Manchen Arbeitgebern scheint kein Anlass zu gering zu sein, ihre Mitarbeiter zu überwachen und zu kontrollieren."

Die gemeinsamen Veranstalter FIfF und DVD setzen sich für ein nachhaltiges Beschäftigtendatenschutzgesetz ein, das den Umgang mit personenbezogenen Daten in verfassungsgemäße Bahnen lenkt und wachsenden allseitigen Kontrolltendenzen von Arbeitgebern/Dienstherrn und Mitarbeitern angemessene Grenzen setzt.

Die Tagung, zu der *Karin Schuler* für die DVD und *Dietrich Meyer-Ebrecht* für das FIfF begrüßten, begann mit zwei Vorträgen am Freitag Abend. Prof. Dr. jur. *Marie-Theres Tinnefeld* eröffnete die Veranstaltung mit einer kritischen Darstellung des aktuellen Regierungsentwurfs zum Beschäftigtendatenschutz. Sie stellte dabei dar, wie die vielen Datenskandale der letzten Monate den Gesetzgeber nach vielen vergeblichen Ansätzen endlich veranlassten, einen Regierungsentwurf für das *Gesetz zur Regelung des Beschäftigtendatenschutzes* einzubringen, der in das BDSG integriert werden soll. Ob der Gesetzgeber aus den Skandalen gelernt hat, zeigte sie insbesondere im Spiegel des Persönlichkeitsrechts Beschäftigter:

- Verdachtslose Massendatenabgleiche oder verlässliche Regelungen zur Korruptionsbekämpfung?
- Heimliche Videoüberwachung rundum oder offene Videoüberwachung mit Respekt vor privaten Lebensbereichen?
- Telefonrazzien oder angemessene Kontrollen der Verkehrs- und Inhaltsdaten bei einer betrieblichen/privaten TK-Nutzung?
- Fristlose Kündigung verantwortungsbewusster Whistleblower oder ein Beschwerderecht, das Beschäftigte bei der Meldung von datenschutzrechtlichen Missständen bei Datenschutzinstanzen bzw. der Presse schützt?

Ein Schlaglicht auf die Auswirkungen von Überwachung warf Prof. Dr. Marc Solga. Er hat untersucht, wie sich die damit verbundene ständige Verpflichtung zur Rechenschaft auf das Erleben und Verhalten auswirkt und ob sie geeignet ist, unerwünschtes Verhalten wie Korruption oder Mobbing zu unter-

Prof. Dr. Marc Solga

drücken. In seinem Vortrag stellte er die Ergebnisse seines wirtschaftspsychologischen Forschungsprogramms vor, das nach den Auswirkungen von erlebter Rechenschaftsverpflichtung auf das Erleben und Verhalten von Menschen im Arbeitsleben fragt. Erlebte Rechenschaftsverpflichtung ist das Bewusstsein,

- kontrolliert und beurteilt zu werden,
- Rechenschaft geben – d.h. sich erklären und rechtfertigen – zu müssen, und
- für Verstöße gegen Regeln, Standards und Leistungserwartungen bestraft werden zu können.

Er beantwortete dabei auch die Frage, ob forcierte Rechenschaftsverpflichtung – eingesetzt im Sinne eines Kontrollinstruments – geeignet ist, kontraproduktivem Verhalten, wie Dienst nach Vorschrift, Mobbing, Korruption etc., entgegen zu wirken.

Malte Arnsperger, Reporter von Stern und stern.de, berichtete am Samstagfrüh von seinen Recherchen zu den Skandalen bei der Lebensmittelkette Lidl, die seinerzeit vom Stern aufgedeckt wurden. Der Vortrag erklärte unter anderem die Recherchemethoden der Journalisten, und wie der Discounter darauf reagierte. Er erläuterte, welche Gründe es für Lidl gegeben hat, auf diese Art und Weise zu handeln, welche Rechte Lidl gebrochen hat, und welche Gesetze Arbeitgeber beim Arbeitnehmerdatenschutz beachten müssen.

In fünf Arbeitsgruppen setzen sich die Teilnehmer im weiteren Verlauf der Tagung mit einzelnen Aspekten des Beschäftigtendatenschutzes auseinander:

- *BewerberInnen-Datenschutz*, vorbereitet und moderiert von *Sören Jungjohann*,
- *Forensik*, vorbereitet von *Karin Schuler* und *Sönke Hilbrans und* moderiert von *Sönke Hilbrans*,
- *Korruptionsbekämpfung*, vorbereitet und moderiert von *Roland Schäfer* und *Sylvia Schenk*,
- *Privacy-Tools und Selbstdatenschutz*, vorbereitet und moderiert von *Sylvia Johnigk, Kai Nothdurft und Barbara Wiesner*,
- *Kommunikationsüberwachung im Beschäftigungsverhältnis*, vorbereitet und moderiert von *Britta Mester*.

Zusammengeführt wurde das Ganze anschließend in einer *Fishbowl* zur Beschäftigtenüberwachung, die *Katharina Just-Hahn* moderierte.

In einer Feierstunde wurde am Samstag Abend erstmalig der FIfF-Studienpreis verliehen. Der ausführliche Bericht findet sich auf Seite 8 in diesem Heft.

Den Ausklang bildete die vom FIfF als Partner mitgetragene Premiere des Dokumentarfilmes *Plug & Pray* von *Jens Schanze* im Kölner Filmhaus. Der Film gibt einen Einblick in die Laboratorien

Malte Arnsperger

Spannung im Publikum

Karin Schuler

AG Privacy-Tools und Selbstdatenschutz
Fotos: Dagmar Boedicker

der künstlichen Intelligenz, einer Welt, in der Computertechnologie, Robotik, Biologie, Neurowissenschaft und Entwicklungspsychologie verschmelzen. „So ist das mit Computern. High Speed Electronic Computing, man steckt es rein und es funktioniert – oder manchmal eben auch nicht …", wird der 2008 verstorbene *Joseph Weizenbaum* zitiert, ehemaliger MIT-Professor im Bereich Computer und Künstliche Intelligenz, Mitinitiator der Gründung des FIfF im Jahre 1984 und langjähriges Vorstandsmitglied des FIfF. An die Filmvorführung im Kölner Filmhaus schloss sich ein angeregtes Publikumsgespräch mit dem Filmemacher und mit Hans-Jörg Kreowski (FIfF) an.

Die Mitgliederversammlungen von DVD und FIfF bildeten am Sonntag den Abschluss einer gelungenen Jahrestagung.

Mitgliederversammlung des FIfF

Köln, Alte Feuerwache – 7. November 2010, 9:20-13:15 Uhr

– Beschlussprotokoll (redaktionell leicht bearbeitet) **–**

Sitzungsleitung: Stefan Hügel als Vorsitzender des FIfF

1. Begrüßung und Feststellung der Beschlussfähigkeit und der Protokollführung

Zur Versammlung ist ordentlich eingeladen worden und dadurch beschlussfähig.
Das Protokoll führt: Jens Rinne

2. Beschlussfassung über Tages- und Geschäftsordnung

Die Tages- und Geschäftsordnung wird von den Anwesenden in bekannter Form genehmigt.

3. Bericht des Vorstands (einschl. Kassenbericht)

Stefan Hügel berichtet über die Vorstandsarbeit in 2010 und den Haushalt 2010 (siehe *http://fiff.de/about/fiff-vorstandsbericht-2010*).
Zu diesem TOP werden keine Beschlüsse gefasst.

4. Bericht der Kassenprüfer

Für die am 26.10.2010 in Bremen durchgeführte Kassenprüfung berichten Michael Ahlmann und Kurt Fussangel der MV (derzeitige Kassenprüfer: Michael Ahlmann, Kurt Fussangel und Gernot Lucks). Aus dem Kassenprüfungsprotokoll: „Dem Vorstand wird eine dem Vereinszweck entsprechende, ordnungsgemäße Kassenführung bescheinigt." Im Rahmen ihrer Überprüfung stellten die Kassenprüfer unberechtigte Abbuchungen fest. Sie schlagen eine strafrechtliche Anzeige wegen versuchten Betruges durch Dritte vor. (Diese ist inzwischen veranlasst worden. Die Red.) Die unberechtigten Abbuchungen hat die Geschäftsstelle rückgängig machen können.
Zu diesem TOP werden keine Beschlüsse gefasst.

5. Diskussion der Berichte

Es werden keine Beschlüsse gefasst.
Die MV dankt für die engagierte, sehr gut strukturierte Kassenprüfung.

6. Entlastung des Vorstands

Die Kassenprüfer schlagen die Entlastung des Vorstands vor. Der Vorstand wird einmütig bei 7 Enthaltungen entlastet.

7. Neuwahl der Kassenprüfer

Die MV wählt Michael Ahlmann (zugestimmt), Kurt Fussangel (zugestimmt), und Gernot Lucks (vorbehaltlich der Zustimmung), einmütig bei einer Enthaltung zu den neuen Kassenprüfern des FIfF.

8. Diskussion über Ziele und Arbeit des FIfF, aktuelle Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen

Zu diesem TOP werden keine Beschlüsse gefasst.

9. Anträge an die Mitgliederversammlung

1. Änderung der Mitgliedsbeiträge (veröffentlicht in der FIfF-Kommunikation 3/2010, Seite 15)
   Nach lebhafter Diskussion über den Vorschlag des Vorstands entscheidet die MV für die Erhöhung der Mitgliedsbeiträge für Normalzahler von 60 € auf 80 € (mehrheitlich bei 1 Nein und 2 Enthaltungen) und Erhöhung für „Studierende und Menschen in vergleichbarer Situation" von 15 € auf 20 € (mehrheitlich bei 5 Nein und 3 Enthaltungen).

2. Weitere Anträge
   Der MV liegen keine weitere Anträge vor.

10. Verschiedenes

Zu diesem TOP werden keine Beschlüsse gefasst.
Die Anwesenden danken für die tolle Organisation dieser Jahrestagung.

11. Genehmigung des Protokolls

Das Protokoll wird einstimmig genehmigt.

Köln, den 07. November 2010

Stefan Hügel

Verleihung des FIfF-Studienpreises

Ausgezeichnete Arbeiten zur Anonymität, zur Biometrie und zum Datenschutz im Schulunterricht

Im Rahmen unserer Jahrestagung vom 5. bis 7. November 2010 in Köln haben wir erstmals einen Studienpreis verliehen. Wir zeichnen damit herausragende Arbeiten aus, die die Informatik mit ihren gesellschaftspolitischen Auswirkungen verbinden. Der FIfF-Studienpreis war 2009 durch die Mitgliederversammlung des FIfF eingerichtet worden.

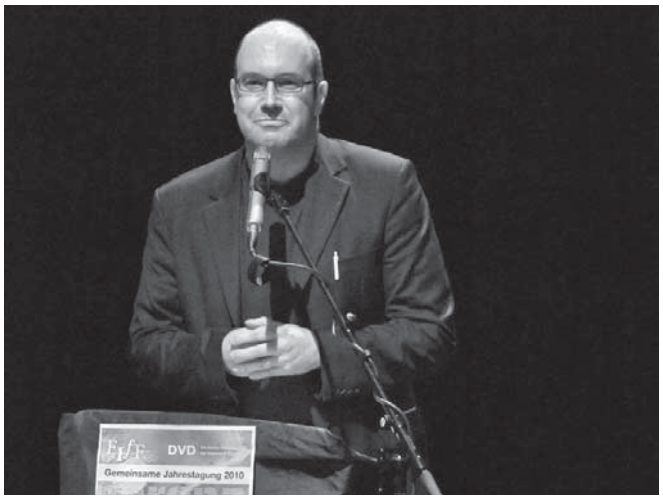
Forschung zu den gesellschaftlichen Auswirkungen der Informationstechnik ist für eine sozialverträgliche Technikgestaltung unverzichtbar. Aber gerade dort wirken sich die Sparzwänge an den Hochschulen besonders aus. Mit unserem Studienpreis wollen wir dazu beitragen, das Thema wieder auf die Agenda zu setzen und ihm die notwendige Aufmerksamkeit zu verschaffen.

Auswahlkommission

Eingerichtet wurde der Studienpreis auf Beschluss der Mitgliederversammlung 2009 in Bremen. Für die Vergabe haben wir eine Auswahlkommission aus sechs Jurorinnen und Juroren gebildet:

- Heidi Schelhowe,
- Britta Schinzel,
- Marie-Theres Tinnefeld,
- Klaus Köhler,
- Christian Pfaab – Vertreter der KIF,
- Stefan Hügel – Vertreter des FIfF-Vorstands.

Aus den eingereichten Arbeiten hat diese Auswahlkommission vier Arbeiten als Preisträger ausgewählt. Vergeben wurde ein erster und drei zweite Preise, die wir in einer Feierstunde am Samstag abend auf der Jahrestagung verliehen haben.



Stefan Hügel führt durch die Preisverleihung

Erster Preis

Mit dem ersten Preis haben wir *Phillip W. Brunst* für seine juristische Dissertation *Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen*[1] ausgezeichnet, die er an der Universität Erlangen-Nürnberg verfasst hat. Die Arbeit untersucht das Thema Anonymität im Internet unter technischen und unter rechtlichen Gesichtspunkten: Unter technischen Aspekten werden Anonymisierungs- und Verschleierungsverfahren untersucht; dabei liegt ein Schwerpunkt auf dem Einfluss dieser Verfahren auf evt. spätere Strafverfolgung und die Möglichkeit einer De-Anonymisierung zu diesem Zweck. Unter rechtlichen Aspekten werden einerseits die Regelungen dargestellt, die die anonyme Nutzung von Internet-Diensten ermöglichen oder sogar dazu verpflichten, andererseits werden die Regelungen betrachtet, die die anonyme Nutzung verhindern oder einschränken.

Marie-Theres Tinnefeld bei der Laudatio auf die Arbeit von Phillip W. Brunst

„Ist Politik wirklich stark, wenn sie maßlos reagiert und Grundrechte zugunsten einer (vermeintlichen) Sicherheit missachtet? Brunst gibt mit ausgeprägten Problembewusstsein Antwort auf diese Frage in einer Zivilgesellschaft", so Marie-Theres Tinnefeld in ihrer Laudatio (siehe Seite 10). „Die Dissertation zeigt, dass er neben einem umfassenden rechtlichen Wissen auch profunde Kenntnisse der Informations- und Kommunikationstechnologie besitzt." Mit dem ersten Preis betont das FIfF den interdisziplinären Charakter der Ausschreibung und anerkennt die Ernsthaftigkeit, mit der die Arbeit einen gesellschaftskritischen Beitrag auf unserem Wirkungsfeld leistet.

Zweite Preise

Ein aktuelles Thema von hoher praktischer Relevanz hat *Andrea Knaut* (Humboldt-Universität zu Berlin) untersucht: Biometrische Erkennungsverfahren bei Personenkontrollen an Nationalstaatengrenzen[2]. Die Arbeit untersucht, inwiefern biometrische Identifikationsverfahren die sozialen Prozesse verschleiern, die an die Identitätsfeststellung gekoppelt sind. Der Zweck

sicherer, effizienter und bequemer Grenzkontrollen durch biometrische Systeme wird auf zwei Weisen hinterfragt: Die Zerlegung eines biometrischen Systems in die Probleme seiner Komponenten wirkt dem Eindruck seiner in sich abgestimmten Geschlossenheit entgegen. Die Analyse der Einbettung der Systeme in unterschiedliche Akteurskontexte zeigt die unterschiedlichen Interessen bei der Nutzung. Die Technik erweist sich dabei als manifestiertes Sozialverhalten. Durch die Delegation der Identitätsfeststellung an vermeintlich objektive Maschinen wird die Verantwortung für weitgehende Entscheidungen abgegeben.

Andrea Knaut, Preisträgerin des zweiten Preises, stellt die Ergebnisse ihrer Arbeit vor

Die Arbeit bewegt sich damit im Bereich der Grundlagen der Modellbildung; hier am Beispiel der Ähnlichkeitsmessung bei Personen. In seinen Auswirkungen handelt es sich beim Gegenstand der Arbeit um einen gesellschaftspolitisch hochrelevanten Prozess, der in der praktischen Anwendung erhebliche Auswirkungen hat – bis hin zur Entscheidung über Menschenleben. Diese Entscheidungen werden an Maschinen delegiert und damit scheinbar objektiviert; die Arbeit stellt dar, dass diese Objektivität der Entscheidungen tatsächlich nur eine scheinbare ist. Das zeigt sich auch durch die differierenden Interessen unterschiedlicher Akteure, die in diesem Kontext eine Rolle spielen. In diesem Sinne gibt sie einen Überblick über die Thematik und die Konsequenzen technischer Lösungen in der Biometrie für gesellschaftliche Prozesse (vgl. auch den Beitrag von Andrea Knaut ab Seite 12).

Die Urkunde wird überreicht, Foto: Pascal Hahulla

In seiner technisch geprägten Arbeit[3] analysiert *Michael Prinzinger* (Universität Erlangen-Nürnberg) das Anonymisierungsverfahren Phantom und untersucht die Auswirkungen von Anonymität auf die Gesellschaft unter sozialen und politischen Aspekten. Die Arbeit untersucht das Thema Anonymität unter zwei Gesichtspunkten: Im ersten Teil wird ein Teil des Protokolls Phantom – die Erstellung von Routing-Pfaden – implementiert und das Protokoll auf seine Stärken und Schwächen untersucht. Dabei wird es mit anderen Anonymisierungsansätzen verglichen.

Klaus Köhler würdigt die Arbeit von Michael Prinzinger

Grundsätzliche Betrachtungen stellt der Autor im zweiten Teil der Arbeit an. Sie umfassen die Themenbereiche Überwachung und Anonymität. Es werden Methoden der Überwachung – beispielsweise Überwachungskameras oder die Analyse sozialer Netzwerke – dargestellt und die involvierten Institutionen und Organisationen beschrieben. Die Behandlung der Anonymität erfolgt entlang ihrer technischen, sozialen, politischen und rechtlichen Aspekte. Der Autor folgert abschließend, dass gesetzliche Regelungen nicht in der Lage sind, Privatheit effektiv zu gewährleisten. Er betont die Bedeutung des Selbstschutzes und die Notwendigkeit von Werkzeugen, um diesen Selbstschutz zu gewährleisten. Das Phantom-Protokoll kann nach Ansicht des Autors solch ein Werkzeug sein, da es alle Anforderungen erfüllt, um die Identität und die Privatheit der Menschen zu schützen (vgl. den Beitrag von Michael Prinzinger ab Seite 16).

Die Diplomarbeit wurde ausgezeichnet wegen ihres Ansatzes, Informatik für die Sicherung von Privatheit einzusetzen (im Sinne einer *Privacy Enhancing Technology*). Sie zeugt von einer hohen Sensibilisierung gegenüber den Möglichkeiten und Gefahren der Informationstechnik.

Jens Jacobi (Studienseminar für Lehrämter an Schulen in Hamm) untersucht in seiner Arbeit die Behandlung des Datenschutzes im Schulunterricht[4]. In der Arbeit wird ein Konzept entwickelt, Lernprozesse so zu organisieren, dass datenschutzrechtliche Fragen mit dem Unterrichtsgegenstand „Netzwerke“ verbunden werden können. Dazu wird eine kurze Lernsequenz konzipiert, die Schülerinnen und Schüler für den Datenschutz in Bezug auf Netzwerke sensibilisieren soll und sich sowohl in gesellschaftswissenschaftliche als auch in technische Unterrichtsreihen integrieren lässt. Seine Arbeit zeichnet sich durch die enge Verbindung von Fragestellungen der Informatik und der Praxis des Unterrichts aus. Das

zeigt sich in der Verknüpfung von allgemeinen Bildungstheorien mit dem Anspruch des Informatikunterrichts, wie sie in der Informatik-Didaktik Konsens ist; insbesondere in der Ausarbeitung des Unterrichtsbeispiels/Rollenspiels, in dem technische Kompetenzen sehr eng mit Datenschutzbewusstsein verknüpft werden.

Fazit

Durch die Preisvergabe wollen wir Aufmerksamkeit für ein Thema schaffen, dessen praktische Bedeutung kaum überschätzt werden kann. All zu häufig wird die Informatik auf ihre technischen Gesichtspunkte reduziert. Das ist einer der Gründe für das Scheitern vieler Projekte – mit allen wirtschaftlichen und sozialen Folgekosten.

Das FIfF gratuliert der Preisträgerin und den Preisträgern herzlich und wird auch im nächsten Jahr wieder einen Studienpreis vergeben. Einreichungen dafür sind hochwillkommen: Näheres unter *http://www.fiff.de/studienpreis*.

Anmerkungen

1 Phillip W. Brunst (2009): Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen. Zum Spannungsfeld zwischen einem Recht auf Anonymität bei der elektronischen Kommunikation und den Möglichkeiten zur Identifizierung und Strafverfolgung. Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht. Berlin: Duncker & Humblot

2 Andrea Knaut (2009): Die Konstruktion menschlicher Identität durch biometrische Erkennungsverfahren bei Personenkontrollen an Nationalstaatengrenzen. Diplomarbeit. http://waste.informatik.hu-berlin.de/knaut/texts/Diplomarbeit_v1_1.pdf. Berlin: Humboldt-Universität

3 Michael Prinzinger (2009): Constructing the Phantom-Protocol Routing Path. Diplomarbeit. Erlangen, Nürnberg: Friedrich-Alexander-Universität

4 Jens Jacobi (2008): Entwicklung eines Konzepts zur Umsetzung des Unterrichtsgegenstands „Netzwerke“ unter Einbeziehung datenschutzrechtlicher Fragen vor dem Hintergrund der informatischen Bildung. Hamm: Studienseminar für Lehrämter an Schulen

Fotos, wo nicht anders angegeben: Dagmar Boedicker

Marie-Theres Tinnefeld

Laudatio zur Verleihung des FIfF-Studienpreises an Phillip W. Brunst

Die Dissertation von Phillip W. Brunst führt den Titel „Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen. Zum Spannungsfeld zwischen einem Recht auf Anonymität und den Möglichkeiten zur Identifizierung und Strafverfolgung.“

Damit wird bereits im Titel eine Antwort auf die mögliche Frage, ob es ein Recht auf Anonymität gibt, bejahend vorweggenommen. Was bedeutet dieses Recht angesichts einer Entwicklung, in der die akustische Wohnraumüberwachung ausgeweitet, der Telefonverkehr zunehmend präventiv und flächendeckend abgehört, und durch die Vorratsdatenspeicherung oder die Online-Durchsuchung anonymes Handeln als integraler Bestandteil des Rechts auf Privatheit ausgehöhlt wird? Ist derjenige, der seit dem 11. September 2001 noch von einer geschützten, ureigensten Intimsphäre als Kernbereich der Privatheit spricht, nicht hoffnungslos antiquiert? Welche komplexe Beziehungen bestehen zwischen Privatheit, Achtung der Wohnung, Telekommunikationsgeheimnis und Datenschutz einerseits und Demokratie andererseits?

„Demokratie ist gewiss ein preisenswertes Gut, Rechtsstaat aber ist wie das tägliche Brot, wie Wasser zum Trinken und wie Luft zum Atmen, und das Beste an der Demokratie gerade dieses, dass nur sie geeignet ist, den Rechtsstaat zu sichern.“[1] Diese Worte schrieb im Jahr 1947 der bedeutende Rechtsphilosoph *Gustav Radbruch* angesichts des Trümmerfeldes, das die nationalsozialistische Terrorherrschaft in Deutschland hinterlassen hatte. Da Demokratie zwar eine notwendige, aber keine hinreichende Voraussetzung für die Bewahrung von Rechtsstaatlichkeit sei, bedürfe es über demokratische verfassungsrechtliche Vorgaben hinaus eines inhaltlich-wertenden Schutzmechanismus für Kernbereiche menschlicher Freiheit und Würde. Nur so können sie auch den Zweck erfüllen, die demokratische Struktur einer Gesellschaft zu erhalten und zu stärken. Ohne die Fesseln des Rechtsstaates kann auch die Politik den Zusammenhang von individueller Menschenwürde, Persönlichkeitsentfaltung und Eigenverantwortung nicht erkennen.

Gesetze der Rechtsordnung sind Regeln, die unvollständig sind, und die auf die Natur einer Sache, etwa auf die tatsächlichen Rahmen-Bedingungen des Internets verweisen, die zu regeln sind. Anzustreben ist immer eine „sachgerechte“ Regelung, sei es im Strafrecht, Strafprozessrecht oder anderen Rechtsgebieten, die zugleich auch mit dem Grundrechtsschutz im Europa des Lissaboner Vertrags übereinstimmen.

Phillip Brunst hat als Leiter des Referats Informationsrecht und Rechtsinformatik im Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg wohl wie kaum ein anderer Einblick in (Internet-) Rechtssysteme, in deren Rahmen die „Vorstellungen, Wertungen und Tendenzen des inter- und supranationalen Rechts nicht unbeachtet bleiben dürfen“. Die Dissertation zeigt, dass er neben einem umfassenden rechtlichen Wissen auch profunde Kenntnisse der Informations- und Kommunikationstechnologie besitzt. Mit diesen Technologien lassen sich nicht nur Instrumente entwickeln, welche den wachsenden Kontrollinteressen in Staat und Gesellschaft vielversprechend entgegenkommen. Sie bieten auch Möglichkeiten des Selbstdatenschutzes in Form von Anonymitätsverfahren, wodurch Bürgerinnen und Bürger über Kontinente hinweg (relativ) vertraulich kommunizieren und Informationen unzensiert verbreiten oder abrufen können. Die Kehrseite der Medaille ist allerdings, dass unter der Tarnkappe der Anonymität auch Straftaten be-

gangen werden, die schwer oder gar nicht rückverfolgbar sind. Wie verhält sich Anonymität zur Strafverfolgung?

Jede ausdifferenzierte Gesellschaft hat daher – pragmatisch betrachtet – nicht nur einen Bedarf an anonymer Kommunikation im Sinne einer persönlichen Nichtzurechnung, sondern auch an einer Kommunikation im Sinne persönlicher Zurechnung. Das betrifft z.B. die Rolle des Wählers bei demokratischen Wahlen. Die Tatsache der Wahlteilnahme wird registriert. Der Inhalt der Wahlentscheidung soll aber auch bei elektronischen Wahlen im Internet geheim bleiben. Andere Bereiche der Einschränkung persönlicher Zurechnung finden sich ähnlich wie bei der Frage der Pseudonymität im Rahmen der Forschung und zur Aufdeckung der Identität bei (Standard-)Kommunikationsbeziehungen im Internet.

Phillip Brunst befasst sich in einem glasklaren Begriffsteil zunächst mit Formen der Anonymität, die noch ein relativ junger Gegenstand des Informationsrechts als Querschnittsmaterie ist. Sodann erörtert er die wirtschaftliche Bedeutung von Anonymisierungsdiensten (z.B. Adressübersetzungen). Die technischen Grundlagen zur Anonymisierung und ihre Umsetzung im Rahmen des WWW und bei der Nutzung von E-Mail werden im Hinblick auf kriminalistische Analysen detailliert bearbeitet. Dabei geht es nicht nur um Daten, die bei dem Nutzer selbst anfallen, sondern auch um Daten, die von einem Access-Provider erhoben werden können. Die konkreten Auswirkungen dieser Zuordnungen machen deutlich, dass die Strafverfolgung in der Praxis Schwierigkeiten mit einem „Recht auf Anonymität" haben kann. Schon am Beispiel des AN.ON-Projekts zeigt sich, dass identifizierende Ermittlungsverfahren im Internet nur dann erfolgen können, wenn alle Betreiber der Zwischenstationen gemeinsam den Nutzer sabotieren. Ein weiteres Problem sind die Online-Börsen. Wegen der hohen Anonymität soll E-Gold insbesondere von Internet-Betrugsgeschäften, Identitätsdiebstählen und Kinderpornografie-Geschäften verwandt worden sein. Die Beispiele lassen sich beliebig fortsetzen.

Sie leiten über zu der Frage nach der rechtlichen Verankerung des Rechts auf Anonymität und seine Wirkung im virtuellen Raum.

Der Autor untersucht den verbindlichen rechtlichen Rahmen für Anonymität – unabhängig davon, ob dies technisch durchführbar ist oder nicht. Er wertet das Verhältnis von Sicherheit und Freiheit gerade auch im Umfeld aktueller Terrorwarnungen nach Maßgabe verbindlicher verfassungsrechtlicher Vorgaben. *„Grundsätzlich sollte daher"*, so der Autor, *„Einigkeit darüber herrschen, dass die Grundrechte und Freiheiten des Einzelnen über die Möglichkeiten einer allumfassenden Straf- und Rechtsverfolgung zu stellen sind und zu diesen Gunsten ein Minus an Sicherheit und Aufklärung bewusst in Kauf genommen werden muss"*. Er prangert die gegenteilige Entwicklung im Internet an, wonach *„alle Daten, die sich potentiell erfassen lassen und die zu irgendeinem späteren Zeitpunkt zur Verfolgung einer Straftat geeignet erscheinen ... möglichst auf Vorrat gespeichert werden."* Insoweit wird nicht nur das inzwischen wichtigste Prinzip der Freiheitssicherung, das Prinzip der Verhältnismäßigkeit ausgehöhlt. Damit fallen auch alle Grenzen für die Überwachung, die etwa durch den grundrechtlichen Schutz des Telekommunikationsgeheimnisses geschaffen worden sind.

Wann darf der Betroffene davon ausgehen, dass er bei einer Kommunikation unbeobachtet bleibt? Darf er, weil er mit Beobachtung rechnet, entgegensteuernde Vorkehrungen treffen etwa mit Hilfe von Anonymisierungsverfahren? Diese Fragen rund um das Anonymitätsproblem prüft Brunst nicht nur im Kontext der Freiheitsrechte im Grundgesetz, sondern auch im Zusammenhang mit der Europäischen Menschenrechtskonvention und der EU-Grundrechte-Charta, die nahezu wortgleich Regelungen mit der EMRK zum Recht auf Privatheit, der Unantastbarkeit der Wohnung und der Sicherung vertraulicher Kommunikation enthält. Er kommt zu dem Schluss, dass das Recht auf Anonymität einen Mosaikstein bildet im Gesamtgefüge der angesprochenen Freiheitsrechte. Davon werden alle Fälle erfasst, die dem Einzelnen ein Recht zugestehen, „nicht erkannt zu werden".

Es ist an dieser Stelle unmöglich, die weitausgreifenden Untersuchungen des Autors zur Anonymität in der globalen Internetkommunikation unter dem Dach des menschenrechtlichen Kerngehalts der Allgemeinen Erklärung der Menschenrechte sowie der OECD u.a. wiederzugeben.

Deshalb soll hier noch einmal die eigentliche Frage erörtert werden, inwieweit Privatheit – Anonymität im Rahmen des Internets zulässig und möglich ist, aber auch rechtlich gefährdet wird. Es geht um das Problem der Vorratsdatenspeicherung: Das bisherige datenschutzrechtliche Grundprinzip, *„dass nur solche Daten gespeichert werden (und bleiben), die für konkrete vertragliche Zwecke benötigt werden, wird durch die Vorratsdatenspeicherung in ihr Gegenteil verkehrt. Statt einer am tatsächlichen Be-*

Phillip W. Brunst ist der Studienpreis des FIfF zugesprochen worden. Mit der Zuerkennung des ersten Platzes betont das FIfF die interdisziplinären Charakter der Ausschreibung und erkennt „die Ernsthaftigkeit an, mit der in einer Arbeit das Ziel verfolgt wird, einen gesellschaftskritischen Beitrag auf unserem Wirkungsfeld zu leisten."

(Dietrich Meyer-Ebrecht)

Phillip W. Brunst

Anonymität im Internet
– rechtliche und tatsächliche Rahmenbedingungen

Zum Spannungsfeld zwischen einem Recht auf Anonymität und den Möglichkeiten zur Identifizierung und Strafverfolgung

Doktorvater und Erstgutachter: Prof. Dr. Hans Kudlich
Zweitgutachter: Prof. Dr. Matthias Jahn

Dissertation angenommen: im Fachbereich Rechts- und Wirtschaftswissenschaft der Friedrich-Alexander-Universität, Erlangen-Nürnberg, WS 2008/2009

Erschienen: Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht. Strafrechtliche Forschungsberichte Hrg. Ulrich Sieber
Duncker&Humblot , Berlin 2009

darf im Einzelfall orientierten Speicherung, die beim Vorliegen eines Verdachts verlängert werden kann, folgt eine Speicherung über einen Zeitraum von sechs Monaten." Die seit dem Volkszählungsurteil im Jahre 1983 eingerichteten tragenden Säulen des Datenschutzes, das Zweckbindungsprinzip und der Grundsatz der Erforderlichkeit als Teil des Verhältnismäßigkeitsprinzips stürzen unter dieser Regelungen zusammen. Die Rechte auf Privatheit und vertrauliche Kommunikation können ohne sie auch im Internet nicht überleben.

Nicht von ungefähr hat das Prinzip der Verhältnismäßigkeit etwas mit dem Gedanken des Maßhaltens zu tun. Der Philosoph *Seneca* (4-65 n. Chr.) schreibt in seiner Abhandlung „De otio" (stoische Ruhe, Muße): *„Mehr Wissen zu wollen als das, was ausreichend ist"*, stelle eine Verletzung des Gebotes der Mäßigung und des Maßhaltens dar und sei dem Glück des Menschen unzuträglich.[2] In diesen Kontext lässt sich die Aussage von *Spiros Simitis* einfügen, der vom *„Informationsverzicht als freiheitssicherndes Prinzip"*[3] spricht. Sie untermauert den Grundsatz der datenvermeidenden und datensparsamen Technikgestaltung beim Umgang mit personenbezogenen Daten. Das Gesetz zur Einführung der Vorratsdatenspeicherung hat erhebliche Auswirkungen auf die Anonymität der Nutzer. Der Autor bildet sie rechtlich und technisch detailliert ab. Seine Kritik der Regelung führt zu den eingangs erwähnten Aussagen von Gustav Radbruch, wonach es für die Bewahrung von Rechtsstaatlichkeit auf einen inhaltlich-wertenden Schutzmechanismus für Kernbereiche der menschlichen Freiheit und Würde ankommt. Ist Politik wirklich stark, wenn sie maßlos reagiert und Grundrechte zugunsten einer (vermeintlichen) Sicherheit missachtet? Brunst gibt mit ausgeprägtem Problembewusstsein Antwort auf diese Frage in einer Zivilgesellschaft.

Anmerkungen

1 *Gustav Radbruch, Gesetzliches Unrecht und übergesetzliches Recht , Süddeutsche Juristen-Zeitung 1946, 105 (108).*

2 *Seneca, 88. Brief 36 (an Lucilius), zitiert nach Foegen, Die Enteignung der Wahrsager, 1993, 293.*

3 *Spiros Simitis, in: Kroker/Dechamps (Hg.), Information – eine dritte Wirklichkeitsart neben Materie und Geist 1995, 287f.*

Andrea Knaut

Biometrische Grenzkontrollen und nationale Identität

FIfF-Studienpreis 2010 2. Preis

Die EU-Nation und ihre Grenzen

In den letzten zwei Jahrzehnten lässt sich am Beispiel der Europäischen Union gut eine supranationale Verstaatlichung beobachten. Auch und gerade in Bezug auf die Grenzkontrollen und Einwanderungsbestimmungen wird dies deutlich. Zentrale Schritte auf dem Weg zum endgültigen Wegfall der Binnengrenzen mit dem 1993 in Kraft getretenen Maastrichter Vertrag über die Europäische Union hatten 1985 mit der Schaffung des Schengen-Raums begonnen und seiner beständigen Erweiterung ihren Lauf genommen.[1] Die „Freizügigkeit unter gleichzeitiger Gewährleistung der Sicherheit ihrer Bürger durch den Aufbau eines Raums der Freiheit, der Sicherheit und des Rechts"[2] regeln im derzeitigen EU-Vertrag Festlegungen zur gemeinschaftlichen polizeilichen und justiziellen Zusammenarbeit sowie zur gemeinsamen Politik im Bereich Grenzkontrollen, Asyl und Einwanderung. Diverse Verordnungen erweiterten und veränderten sukzessive die Zugriffsmöglichkeiten und Kompetenzen vorhandener nationalstaatlicher Exekutivorgane oder schufen neue. Institutionen wie die europäische Grenzschutzagentur FRONTEX, die Rapid Border Invention Teams oder das Visa-Informationssystem VIS wurden und werden noch aufgebaut. Für den Umgang mit illegalisierter Einwanderung und Asyl hat man dementsprechend mit dem Dublin-II-System, das an das Dubliner Übereinkommen von 1990 anschließt, die rechtlichen Grundlagen geschaffen.[3]

Nach den aktuellen Vertragswerken und Verordnungen der EU werden UnionsbürgerInnen und *Drittstaatsangehörige*, wozu auch *Staatenlose* gehören, unterschieden. Zweitere können den territorial abgegrenzten Raum nur unter bestimmten Bedingungen betreten – zum Beispiel mit legalen, meist zeitlich begrenzten Visa als TouristInnen, Geschäftsleute, Studierende oder qualifizierte Arbeitskräfte. Alle anderen Drittstaatsangehörigen sind etwa nach der Kategorisierung der Eurodac-Verordnung (European Dactylographic System) entweder „Asylbewerber", „Ausländer, die in Verbindung mit dem illegalen Überschreiten einer Außengrenze aufgegriffen werden" oder „Ausländer, die sich illegal in einem Mitgliedstaat aufhalten".[4] Doch wie erkennt ein/e PolizistIn eigentlich einen Ausländer, der sich illegal in einem Mitgliedstaat aufhält?

Eine erste Idee ist die berühmte Frage nach dem Ausweis – im Kontakt mit Behörden, in bestimmten Kontrollzonen oder bei der gewollten oder ungewollten Verwicklung in Strafdelikte liegt dies nahe. Insbesondere Kontrollen an in Polizeigesetzen speziell definierten Orten, und das sind nicht wenige, mit und ohne Verdacht, geschehen häufig mit Rückgriff auf rassistische Vorurteile.[5]

Der Ausweis als Teil des modernen Konzepts der (Staats-) Bürgerschaft sichert Zugehörigkeit zu einem geschlossenen mit bestimmten Ressourcen für seine Mitglieder ausgestatteten Raum ab. Und dabei haben Ausweise, Grenzkontrollen, Register, Empfehlungsschreiben von Fürsten, Brandmarkungen, Steckbriefe gesuchter Krimineller ihre Ursprünge weit vor der abendländischen Moderne.[6] Das Sich-Ausweisen scheint erforderlich in Situationen, in denen sich Menschen nicht mehr persönlich kennen. Hornung weist darauf hin, dass Kleinstgesellschaften ohne Ausweise auskommen, aber dass sich in mobilen, ausdifferenzierten, durch abstrakte Interaktionsprozesse geprägten Gesell-

schaftssystemen häufig die Notwendigkeit ergäbe, „die Identität des Gegenübers sicher festzustellen".[7] Bezogen auf den Grenzübertritt meint diese Notwendigkeit die Berechtigung zum Zugriff auf die Ressourcen einer (staatlichen) Gemeinschaft, die aber zunächst einseitig als ein Schuldverhältnis betrachtet wird. Es wird bereits präventiv eine Verbindlichkeit in Bezug auf die zukünftige Inanspruchnahme bestimmter abstrakt bereitgestellter Ressourcen abgesichert. Ob und wie viele davon wirklich genutzt werden, ist dabei genausowenig wichtig wie die erwartbare Gegenseitigkeit eines zu einer Gemeinschaft hinzutretenden Individuums. Dieses Sich-Absichern und Glaubwürdigkeit eines Handels schaffen geht also mit dem Sich-Identifizieren des Subjekts und seiner damit zukünftigen Verantwortbarmachung und Verbindlichkeit seines Etwas-Schuldens einher. Begriffe der Identität, Subjektivität und des sozialen Interagierens sind aber kaum so einfach abzuhandeln. Insofern ist es interessant, wenn in Studien wie der jüngsten des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu *Identitätsdiebstahl und Identitätsmissbrauch im Internet* zumindest darauf hingewiesen wird, dass Identität ein schillernder Begriff sei und in verschiedenen Disziplinen unterschiedliche Bedeutung habe. Gleich als erstes wird dann auf die Philosophie verwiesen und schließlich zwölf verschiedene Definitionen von Identität angegeben. Selbst beschränkt auf den technischen Kontext bleiben noch vier verschiedene.[8] Die Biometrie hat ebenfalls viele verschiedene Definitionen etwa als „science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person".[9] Der/die AutorInnen dieser Definition entkoppeln erstaunlicherweise *Identität* in einer Fussnote von der biologischen Beschaffenheit einer Person:

> *„The identity of an individual may be viewed as the information associated with that person in a particular identity management system [...]. For example, a bank issuing credit cards typically associates a customer with her name, password, social security number, address and date of birth. Thus, the identity of the customer in this application will be defined by these personal attributes (Le., name, address, etc.)."*[10]

In der Verordnung für das oben erwähnte Eurodac-System wird konstatiert: „Fingerabdrücke sind ein wichtiges Mittel zur genauen Identifizierung dieser Personen",[11] womit die eingangs erwähnten Personenkategorien gemeint sind. So klar ist das den Verfassern der Verordnung. Den Technikerinnen und Technikern, die Forschung für die Grundlagen biometrischer Verfahren betreiben oder diejenigen, die biometrische Anwendungen implementieren, ist dies nicht ganz so klar. Die Klassifikationen der Fehler bzw. der Ungenauigkeiten der biometrischen Systeme sind sogar widersprüchlich.[12] Viele internationale oder nationale Normen in diesem Bereich sind kein Jahrzehnt alt. Doch der Einsatz biometrischer Systeme wird im Rahmen symbolischer Sicherheitspolitik vorangetrieben. *Symbolisch* spielt dabei eher auf den Irrglauben an, die biometrischen Systeme würden dem oben zitierten Anspruch genauer Identifizierung wirklich gerecht, denn auf die durchaus wirkmächtigen Konsequenzen ihrer Nutzung. So wird etwa mit Hilfe von *Eurodac-Treffern*, also aufgrund zusammenpassender Fingerabdrücke von an den Grenzen oder in EU-Mitgliedsländern aufgegriffenen Personen, die *Rückführung* eines Asylbewerbers bzw. Illegaliserten in einen anderen Mitgliedstaat, der vermeintlich als erster die Fingerabdruckdaten ermittelt hat, beantragt. Der als verantwortlich ermittelte Staat entscheidet unterschiedlich schnell die Abschiebung oder im besten Fall positiv auch den Beginn eines Asylverfahrens. Gemäß der jährlichen Tätigkeitsberichte der EU-Kommission über die Arbeit der Eurodac-Zentraleinheit wurden weit mehr als eine Million Fingerabdruckdaten in den letzten sieben Jahren übermittelt. Auch wenn sogenannte *Treffer* durch weitere Identifikationsmethoden überprüft werden müssen, schaffen die Zahlen ein gewisse Rationalität für Entscheidungen über das Hin- und Herschieben von Menschen zwischen den EU-Mitgliedstaaten. Die Zahlen führen zu fassbareren Interpretationen von *Migrationsströmen*, zu durch plötzlich von Zahlen untermauerten Forderungen, Menschen in Haft zu nehmen, damit sie sich einer Rückführung innerhalb der EU nicht entziehen können, noch mehr Daten zu speichern, damit das System effizienter arbeiten könne und anderen neuen Begehrlichkeiten für Zugriffe zur Terrorabwehr.[13]

Auch die Staatsbürgerinnen und Staatsbürger der EU müssen mit ihren Visa-Dokumenten ohnehin biometrisch taugliche Gesichtsbilder vorhalten und sind auch, wie jetzt mit dem neuen Personalausweis, zunehmend angehalten abgenommene Fingerabdrücke aufzuzeichnen. Die kriminaltechnische Praxis der erkennungsdienstlichen Behandlung im Rahmen von Straftaten wurde in Deutschland schon 1992 gemäß §16 des damals geänderten Asylverfahrensgesetzes auf Asylbewerberinnen und Asylbewerber ausgedehnt. Nun gilt sie alsbald für alle. Dennoch bleibt die Trennung in legale und illegale Partizipation und Gruppenzugehörigkeit auch im biometrischen Kontext erhalten. Nicht nur in den Pilotprogrammen zum Biometrie-Einsatz ließ sich stets eine diskursive Trennung zwischen *Komforterhöhung durch Biometrie für Vielreisende* wie etwa bei der in meiner Diplomarbeit genau untersuchten *Automatisierten Biometriegestützten Grenzkontrolle* (ABG) am Frankfurter Flughafen und der *Verhinderung von Asylbetrug oder illegaler Einreise durch*

Andrea Knaut

Andrea Knaut ist Diplom-Informatikerin und arbeitet derzeit als wissenschaftliche Mitarbeiterin an der Arbeitsgruppe für Informatik und Gesellschaft an der Humboldt-Universität zu Berlin. Sie war lange Jahre Aktivistin der JungdemokratInnen/Junge Linke Berlin, bei der Naturfreundejugend und den Naturfreunden Berlin und der antirassistischen Arbeit. Zur Zeit ist sie eher Theoretikerin und noch am ehesten mit der Arbeit des Netzwerks für Kritische Migrationsforschung assoziiert.

Biometrie im Kontext der Ausgrenzung von Drittstaatsangehörigen ausmachen.[14] Programme wie das *BIOmetrics Data Experimented in Visas* (BIODEVII), die Planungen des elektronischen Aufenthaltstitels oder Eurodac gingen eher in diese Richtung.

Der Identitätsbegriff in der Biometrie und Fehler

Nun, also, IngenieurInnen, TechnikerInnen und ProgrammiererInnen wissen gewöhnlich um die komplexen Probleme biometrischer Systeme.

Ein zentrales, politisch extrem wirksames Missverständnis der Biometrie ist die Suggestion *eindeutiger Identifikation* einer Person durch biometrische Vermessung. Bei der biometrischen Erkennung handelt sich um einen Mustervergleich, also die Ähnlichkeit eines sogenannten *Sample* bzw. Referenzmusters mit einem *Template*. Dabei gibt es zahlreiche Fehlerquellen: Beginnend bei der Aufnahme des Merkmals durch die Sensorik, der anschließenden Signalverarbeitung, der Transmission des Signals, eventueller Verschlüsselung, seiner Segmentierung, der Erstellung von *Features* bzw. des eigentlichen digitalen Musters aus dem Sample der Messung und der Einstufung seiner Qualität, seiner Speicherung und eben seines Vergleichs mit einem Template, das natürlich selbige Prozedur über sich ergehen lassen musste, sowie der Berechnung der Ähnlichkeitswerte der Muster. Die Schwellwerte, unter denen zwei Muster als gleich gelten, sind zudem noch oft administrierbar in Hinblick auf die Sicherheitsszenarien. Dass das oben geschilderte generische System von einer großen Zahl an verschiedenen Herstellern in Einzelkomponenten implementiert ist und sowohl der hardware- als auch softwareseitigen Integration bedarf, dürfte vorstellbar sein. Dass bereits der Austausch einzelner Komponenten Kompatibilitätsprobleme mit sich bringen kann, ebenfalls. Selbstverständlich gibt es Phänomene wie die Template-Alterung. Die Schwierigkeiten und Komplexität steigen an, wenn nicht wie bei den Reisepässen oder neuen Personalausweisen eine 1:1-Verifikation von aktuell erfassten Samples mit auf dem RFID-Chip abgelegten vorgenommen wird, sondern eine 1:N-Identifikation wie eben in Eurodac.

Die Standardisierung und öffentliche Performanztests sind also mehr als notwendig, um halbwegs einen Überblick zu bewahren. Und selbst die statistisch messbaren Fehler wie die bekannte *False-Rejection-Rate* (FRR), die *False-Acceptance-Rate* (FAR) sowie die *False-Non-Match-Rate* (FNMR) und die *False-Match-Rate* (FMR) und weitere waren lange Zeit nicht einheitlich definiert und haben durch die Ausklammerung von Akzeptanzfragen und Umwelteinflüssen begrenzte Aussagekraft.

Insofern nimmt es nicht wunder, wenn hin und wieder einige versuchen, auf die Bremse zu treten:

„Biometrische Eigenschaften eignen sich in der Regel nicht, um eine Identität im Internet nachzuweisen, denn sie müssen lokal auf Seite des Clients erfasst, und dann als Datensatz über das Internet transportiert werden.“, heißt es etwa in oben zitierter Studie des BSI.[15] Ist das Problem das Internet? Ist der Transport über das für Eurodac genutzte sTESTA-Netzwerk (*secure Trans European Services for Telematics between Administrations*) weniger anfällig, da es komplett vom öffentlichen Internet isoliert ist?[16]

Der Diebstahl biometrischer Datensätze ist ein weiteres von vielen Problemen. Die Autoren der BSI-Studie aber erwähnen auch, dass Biometrie, zwar bezogen auf Identifikation im Internet, auch aus Gründen des allgemeinen persönlichkeitsrechtlichen Datenschutzes abzulehnen sei. Da sei hinsichtlich der zentralen Speicherung und der Kopplung permanenter biometrischer Datensätze an andere persönliche Daten noch erhöhter Forschungsbedarf vonnöten.

Doch schon allein die technischen Probleme genügten auf der Biosig-Konferenz in Darmstadt 2010, um einen Frontex-Vertreter warnen zu lassen, „dass sich mit der zunehmenden Sammlung biometrischer Daten ihr Nutzen auflöse.“[17]

Selbst die erfahrenste Gruppe, die kriminalistischen ForensikerInnen, warnen bezüglich der hoch gelobten Aussagekraft von Fingerabdrücken. Als einziges Beweismittel vor Gericht sind sie höchst zweifelhaft. Umfrageergebnisse der American Academy of Forensic Sciences (AAFS), die 2010 präsentiert wurden, ergaben: „(...) 75 per cent of US forensic scientists believed that innocent people may be in jail or on death row because of fingerprint errors.“[18]

Versuche auf datenschutzrechtlicher Ebene, Biometrie und deren vermeintlich Genauigkeit mit Vorsicht zu genießen, greifen die Hinweise auf die technischen Fehler auf: Wird jemand durch ein biometrisches System zurückgewiesen, sollte zunächst von einer Falschrückweisung ausgegangen werden – gewissermaßen ist das eine Unschuldsvermutung.

Doch allein die Kritik an der Biometrie anhand ihrer Fehler führt offensichtlich kaum zum Abbruch ihrer zunehmenden Nutzung. Nicht zuletzt, weil die statistisch quantifizierbaren Systemfehler erfassbarer scheinen. Die Rechenleistungen, Ausfälle usf. lassen sich konkreter beziffern als menschliches Versagen. Fehler werden zum unausschöpflichen Potential für die Verbesserungen eines Verfahrens zur Senkung eben dieser. Die Optimierung der Systeme ist der Wachstumsmotor ganzer Branchen. Und die Ideologie der Kopplung von körperlicher Disposition und Zugehörigkeit zu einem Staat, Volk und Nation stabilisiert sich damit im Grunde, wenngleich gerade der Biometrie auch das Potential eingeräumt wird, Wiedererkennung jenseits rassistischer Stereotype oder Kopplung an die soziale Identität zu ermöglichen. So sprechen einige Biometriker von der Möglichkeit der Wiedererkennung von Personen durch anonyme Biometrie, da biometrische Messdaten wie Fingerabdrücke oder Augen allein keinerlei Angaben über Namen, Altern, Geschlecht, Ethnie, Gesundheit oder Einwanderungsstatus offenbarten.[19] Eine solche Vision lässt jedoch sehr schnell vergessen, dass eine Wiedererkennung im Kontext eines Zugangskontrollszenarios nur Sinn macht, wenn an die soziale Identität bestimmte Privilegien gekoppelt sind.

Wie eingangs erwähnt wird in der Blackbox Biometrie unsichtbar, dass der Mustervergleich kein eindeutiger ist und sein kann. Woher das Missverständnis kommt, dass eine biometrische Vermessung, eine eindeutige Identifikation darstellt, ist sicherlich eine vielschichtige Untersuchung wert, die sicher eher einen soziologisch-philosophischen Charakter haben müsste. Meine These, dass sie verschleiert, dass Wiedererkennung, Identifizieren, Inkludieren, Exkludieren ein sozialer und kommunikativer

Prozess ist, und versucht wird, die Verantwortung für die mit diesem Prozess einhergehenden Konsequenzen mit der biometrischen Automatisierung auf Maschinen zu verlagern, konnte ich gerade im Bereich der Erkenntnistheorie, der Einordnung in Konzepte der Akteur-Netzwerk-Theorie von Latour und Callon bzw. das der Situierten Wissen von Donna Haraway nur begrenzt leisten.[20] Der Versuch der Verortung einer vermeintlich objektivierbaren Wiedererkennung von Menschen durch Automaten in einem rationalistischen Wissenschaftsbild, das den Forscher, Forschungsinteressen und das gesellschaftspolitische Setting bestimmter Machthierarchien der Akademien und Labore thematisiert, ist extrem schwierig. Genauso konnte ich auch die Latoursche Idee des Erhebens der Maschinen zu gleichberechtigten Akteuren innerhalb lediglich beschreibbarer Netzwerke, in denen Akteursinteressen mit Programmen und Antiprogrammen aufeinandertreffen, nur in einem oberflächlichen Verständnis berücksichtigen. Gerade die Betrachtung der Biometrie aus dem Blickwinkel der Wissenschaftsgeschichte und einem systematischen Beobachten der Methodik der wissenschaftlichen ArbeiterInnen und ihrem Interagieren mit Politik und Wirtschaft sollte viel Aufschluss über den Siegeszug technologischer Innovationen trotz ihrer Fehlerhaftigkeit bringen.

Und weiter?

Der Aufbau der Agentur für das Großmanagement von IT-Systemen in Europa zur Administration von VIS, SIS II, SIS, Eurodac[21], wovon erstere bis heute nicht wirklich funktionieren, aber auch der neue Personalausweis in Deutschland zeigen, dass trotz aller Warnungen von TechnikerInnen zu den Fehlern biometrischer Systeme deren Nutzung befördert wird und diese verstärkt eingesetzt werden. Am wenigsten in Frage stellen können das Ganze die damit benutzten MigrantInnen. Immer wieder gibt es Meldungen in den Medien von dem harschen Agieren der neuen Grenzschutzagentur.[22] Informationsverarbeitende Technologie ist Teil der Militarisierung der Grenzen, die einen euphemistischen Deckmantel erhält. Viele Firmen, in denen InformatikerInnen landen, verdienen auch irgendwo in diesen Bereichen ihr Geld. Die Fehler der Technologie sind dabei vielleicht ein Problem, das die Wirksamkeit der Systeme auf technischer Ebene diskreditiert. In Bezug auf Migration müsste allerdings eigentlich auch die politische Motivation der sicherheitstechnischen Aufrüstung zur Sprache kommen: Der Preis des Liberalismus ist die Abschottung, die im Kontext neu an Land gewinnender nationalistischer Tendenzen in den Industrieländern kumuliert, und die grundsätzlich ein recht ahistorisches Verhältnis zum Wohlstand offenbart, der auch auf der Kolonisation der Staaten beruht, deren Opfern man damals und heute nicht die Reisefreiheit gewähren mag, die UnionsstaatsbürgerInnen als wichtiges Gut betrachten. *Informatik und Gesellschaft* als Feigenblatt der informatischen Technikwissenschaft mag ein Auslaufmodell sein an deutschen Universitäten. Gewissensbisse in Form einer gelebten gesellschaftlichen Verantwortung sind nicht unbedingt en vogue. Eine staatlich nicht kontrollierbare Migration aber wird es immer geben. Das ist das Schöne: auch Biometrie ist sehr wohl zu unterlaufen und zu überlisten – seit den 1970ern ist es im wissenschaftlichen Kontext offiziell anerkannt, dass „biometric forgery and mimicry" möglich ist[23] – ein beliebtes Spielfeld nicht nur der Hacker-Community.

Quellen

Bauer, Robin: Grundlagen der Wissenschaftstheorie und Wissenschaftsforschung. In: Ebeling, Smilla und Sigrid Schmitz: Geschlechterforschung und Naturwissenschaften. Einführung in ein komplexes Wechselspiel. Wiesbaden: VS-Verlag, 2006, S. 247-280.

Borges, Georg; Schwenk, Jörg; Stuckenberg, Carl-Friedrich; Wegener, Christoph: Identitätsdiebstahl und Identitätsmissbrauch im Internet. Rechtliche und technische Aspekte. BMI und BSI, 2010.

Kritische jurist_innen der FU Berlin: „The colour of guilt and innocence" – racial profiling im Rahmen polizeilicher Personenkontrollen. aus: STREIT, Zeitschrift der Kritischen Jurist_innen 1/2010. Veröffentlicht unter gleichem Titel bei der Kampagne für Opfer rassistischer Polizeigewalt, URL: http://kop-berlin.de/2010/01/the-colour-of-guilt-and-innocence-racial-profiling-im-rahmen-polizeilicher-personenkontrollen/ (13.10.2010).

Groebner, Valentin: Der Schein der Person. Steckbrief, Ausweis und Kontrolle im Europa des Mittelalters. München: C. H. Beck-Verlag, 2004.

Hornung, Gerrit: Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren. In: Der elektronische Rechtsverkehr, Bd. 10. Baden-Baden, Nomos, 2005.

ISO/IEC JTC 1/SC 37: *Information Technology – Biometric performance testing and reporting – Part I: Principles and framework.* ISO/IEC JTC 1/SC 37: ISO/IEC 19795-1:2006(E). 01.04.2007.

Jain, Anil K./Ross, Arun A.: Introduction to Biometrics. In: Dies. et al.: Handbook of Biometrics. New York: Springer Science+Business Media, 2008, S. 1-22.

Knaut, Andrea: Die Konstruktion menschlicher Identität durch biometrische Erkennungsverfahren bei Personenkontrollen an Nationalstaatengrenzen. Diplomarbeit am Institut für Informatik, Humboldt-Universität zu Berlin, 27. 3. 2009. URL: http://waste.informatik.hu-berlin.de/knaut/texts/Diplomarbeit_v1_1.pdf

Latour, Bruno: Technik ist stabilisierte Gesellschaft. In: Belliger, Andréa/Krieger, David J.: ANThology. Ein einführendes Handbuch zur Akteur-Netzwerk-Theorie. Transcript, 2006, S. 369-396.

Parenti, Christian: The Soft Cage: Surveillance in America From Slavery to the War on Terror. New York: Basic Books, 2003.

Torpey, John: The invention of the passport: surveillance, citizenship and the state. Cambridge: Cambridge University Press, 2000.

Wayman, James L., Anil Jain, Davide Maltoni, Dario Maio (Hg.): Biometric Systems: technology, design and performance evaluation. London, Berlin, Heidelberg: Springer-Verlag, 2005.

Die erwähnten EU-Verordnungen sind alle auf dem Server http://eur-lex.europa.eu zu finden.

Anmerkungen

1 *Das Schengener Durchführungsübereinkommen (SDÜ) ist die Grundlage für die Einrichtung des polizeilichen computergestützten Schengener Informationssystems SIS zur Fahndung und dessen immer noch unfertigen und immer wieder totgesagten Folgesystem SIS II, das auch biometrische Daten für die europaweite Fahndung nutzen soll.*

2 *Lissabonner Vertrag über die Arbeitsweise der Europäischen Union, Abl. Nr. C 83 vom 30.3.2010, Präambel, S. 16.*

3 *Frontex: VO EG Nr. 2007/2004; RABIT: VO EG Nr. 863/2007; VIS: VO EG Nr. 767/2008; Dublin-II: VO EG Nr. 343/2003.*

4 *So jeweils in VO EG Nr. 2725/2000 in den Kapiteln II, III und IV benannt.*

5 *Allein das Allgemeine Sicherheits- und Ordnungsgesetz der Berliner Polizei (ASOG) zählt in § 21 verschiedene Orte auf, an denen die Polizei zu verdachtsunabhängiger „Identitätsfeststellung" berechtigt ist. Der Artikel „»The colour of guilt and innocence« – racial profiling*

im Rahmen polizeilicher Personenkontrollen" einer Kritischen Juristin von Anfang 2010 beschreibt den Alltag rassistischer Polizeikontrollen und verweist auch Stellen im Bundespolizeigesetz, die verdachtsunabhängige Kontrollen ermöglichen.

6 *Vgl. Groebner, 2004 zur Geschichte der Ausweise und Identifizierungspraktiken im europäischen Mittelalter oder Parenti, 2003, der sich in Bezug auf die amerikanische Geschichte, beginnend beim Sklavenhandel, mit Praktiken der Überwachung und Identifizierung menschlicher Individuen im Kontext von Machtverhältnissen und Kontrolle beschäftigt.*

7 *Hornung, 2005, S. 29.*

8 *Borges, Georg et al., 2010, S. 14ff.*

9 *Jain, Anil K. und Ross, Arun, 2008, S. 1.*

10 *Ebd.*

11 *VO EG Nr. 2725/2000, Absatz (4) in der Präambel, die die Gründe für die Einführung des Eurodac benennt.*

12 *Im Standardisierungsdokument für Performanstests biometrischer Systeme ISO/IEC 19795-1:2006(E) heißt es: „a short review of the technical literature on biometric device testing over the last two decades or more reveals a wide variety of conflicting and contradictory testing protocols" (S. vi) und verweist elf verschiedene Dokumente.*

13 *Zur Festschreibung von in Deutschland sowieso gängigen Praxis der Abschiebehaft in allen EU-Staaten siehe Arbeitsdokument zum Bericht der EU-Kommission 2007, S. 30. Zur Forderung nach Speicherung aller übermittelten Daten Bericht von 2007, S. 12. Eine überarbeitete Verordnung ist diesbezüglich in Arbeit. Der letzte Tätigkeitsbericht von 2010 weist darauf hin, dass damit „Strafverfolgungsbehörden der Mitgliedstaaten und Europol der Zugriff auf die Zentraldatenbank EURODAC zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten ermöglicht" werden soll. (COM (2010) 415, S. 2)*

14 *Vgl. Knaut, Andrea, 2009 zu ABG und BIODEV II. Vgl. VO (EG) Nr. 380/2008 u. a. zum elektronischen Aufenthaltstitel. Auch in Dokumenten des BSI, Bundesinnenministeriums oder des Bundesverwaltungsamts finden sich Erwähnungen dazu.*

15 *Borges et al., S. 51ff.*

16 *Vgl. den Artikel „STESTA: Secure Trans European Services for Telematics between Administrations" auf der Europa-Website der EU-Kommission, URL: http://ec.europa.eu/idabc/en/document/2097/5644.html (14.11.2010).*

17 *Heise online: Biosig 2010: Finger für Europa. 13.9.2010, URL: http://www.heise.de/newsticker/meldung/Biosig-2010-Finger-fuer-Europa-1078022.html (14. 11. 2010).*

18 *Baumgartner, Boyd: Fingerprint evidence to harden up at last. 23.3.2010, URL: http://www.clpex.com/phpBB/viewtopic.php?f=2&t=1384 (14.11.2010).*

19 *Wayman et al., 2005: S. 15. Datenschützer_innen sind bezüglich der Aussagekraft der Daten bezogen etwa auf Gesundheit allerdings anderer Ansicht.*

20 *„Technik ist stabilisierte Gesellschaft." (Latour, 2006) ist der Titel eines Aufsatzes, der inspiriert zur These der einen sozialen Prozess stabilisierenden Black Box Biometrie. Latour diskutiert das in selbigem aber recht kritisch. Haraways Begriff der Situierten Wissen ordnet dabei auch rationalistisch, wissenschaftlich objektivierte Positionen in ein Netz aus Interessen, das im wissenschaftlichen Apparat besteht, ein. Die Situierten Wissen kennzeichnen Verantwortlichkeit auch für vermeintlich bewiesene Tatsachen. Die indirekte Wiedergabe des wissenschaftstheoretischen Ansatzes von Donna Haraways Lehre verkörperter Objektivität ist angelehnt an (Bauer 2006).*

21 *Dossier 2009/0089/P (COD).*

22 *ARD-Nachrichten: Schwere Vorwürfe gegen EU-Grenzschutzagentur. 5. 10. 2010, URL: http://www.tagesschau.de/ausland/bootsfluechtlinge100.html (14.11.2010).*

23 *Wayman et al., 2005: S. 5ff.*

Michael Prinzinger

FIfF-Studienpreis 2010
2. Preis

Anonymität – Schutzschild der Bevölkerung

Protections for anonymous speech are vital to democratic discourse.
Allowing dissenters to shield their identities frees them to express critical, minority views...
Anonymity is a shield from the tyranny of the majority...
It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular:
to protect unpopular individuals from retaliation... at the hand of an intolerant society.
Urteil des U.S. Supreme Court, 1995

In einem Zeitalter, in dem Informationen wichtiger und wertvoller werden als Rohstoffe, Maschinen und Grundbesitz, stellt sich die Frage, wie man am besten mit Informationen umgeht. Der Datenschutz spielt dabei eine wichtige Rolle, schreibt er doch sowohl der Regierung als auch Firmen einen sorgfältigen Umgang mit Daten vor. Dennoch liest man immer wieder von Unfällen, bei denen persönliche Daten an falsche Hände gelangen, oder von Eingriffen in die Privatsphäre der Daten aus Gründen der nationalen Sicherheit. Wie sicher also ist unser wichtigster Besitz, unsere Informationen?

Es ist kaum mehr möglich, seine Wohnung zu verlassen ohne überall Informationen darüber zu hinterlassen, wo man gewesen ist und was man dort gemacht hat. Einige Beispiele:

- In jedem Einkaufszentrum hängen Überwachungskameras von der Decke.
- Rabattkarten zeichnen genau auf, was man gekauft hat.
- Mobiltelefone sind Peilgeräte, mit deren Hilfe die Bewegungen ihrer Besitzer genau nachvollzogen werden können.
- Am Arbeitsplatz wird genau aufgezeichnet, welche Internetseiten man mit dem Arbeitsplatzrechner ansteuert.
- Die Vermittlungsdaten der Telefongespräche, die man dort (oder auch unterwegs mit seinem Mobiltelefon) führt, werden ebenfalls gespeichert.

- Erreicht man dann seine eigene Wohnung, meldet man sich bei Facebook und MySpace an und erzählt der Welt seine Vorlieben und Charaktereigenschaften.

Die Fülle an Informationen ist also enorm. Neue Gesetze erweitern den Fundus an Informationen jeden Tag. Vorratsdatenspeicherung, LKW-Maut, Elektronische Gesundheitskarte, Biometrischer Reisepass, Bundestrojaner und Lauschangriff sind dabei nur die bekanntesten Projekte.

Aber wer hat eigentlich so viel Interesse daran, diese Informationen zu erheben, zu sammeln und zu verarbeiten?

Die Liste wird angeführt von Regierung, Polizei und Geheimdiensten: BKA, Europol und Interpol haben bereits jetzt weitreichende Befugnisse, zu überwachen, zu speichern und zu verarbeiten. Als Rechtfertigung nennen diese staatlichen Instanzen oft Terrorprävention und Verbrechensverfolgung. In Wirklichkeit bietet die Überwachungsmaschinerie dem Staatsapparat noch ganz andere Vorteile. Die Regierung hofft damit, die Bevölkerung besser kontrollieren zu können und politische Kritik zu mindern. Tatsächlich gibt es einen psychologischen Effekt, genannt *Panoptismus*, nach dem man weniger offen eine kritische unerwünschte Meinung äußert, wenn man dabei beobachtet oder aufgezeichnet wird. Auch neue Technologien hofft die Regierung mit mehr Überwachung besser kontrollieren zu können. Vergessen wir auch nicht, wie Überwachung und das Sammeln von Informationen bei der Gestapo oder der Stasi verwendet wurden.

Auch die Wirtschaft hat großes Interesse an diesen Informationen und nutzt diese, um Persönlichkeitsprofile ihrer Kunden zu erstellen. Mit diesen Profilen wiederum lässt sich dann persönliche Werbung anbieten, die Kreditwürdigkeit von Menschen überprüfen oder das Privatleben eines Arbeitsplatzbewerbers genau überprüfen.

Es wird immer deutlicher, dass es sehr wichtig für die Bevölkerung ist, sich nicht vollends bis zu einem gläsernen Menschen durchleuchten zu lassen. Dies ist offensichtlich auch dem Bundesverfassungsgericht klar, welches nun schon mehrmals richtungsweisend für einen Schutz persönlicher Informationen geurteilt hat. Aus den Paragraphen 1 und 2 des Grundgesetzes hat das Bundesverfassungsgericht eine Fülle von Schutzrechten abgeleitet. Für den Schutz von Informationen am wichtigsten sind das Recht auf informationelle Selbstbestimmung, das Recht am eigenen Bild und Wort und das Recht auf Privatsphäre. Diese Gesetze schützen die Informationen, wenn sie nicht mehr der eigenen Kontrolle unterliegen. Hinzu kommt das Recht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Dieses Recht schützt persönliche Informationen auf dem eigenen Rechner. Informationen, die sich auf dem Transportweg befinden, werden durch das Fernmeldegeheimnis (§10) geschützt.

Leider haben die Beispiele am Anfang dieses Artikels gezeigt, dass diese juristischen Schutzmechanismen noch nicht ausreichen. Das Interesse der Regierung und der Wirtschaft, einmal erhobene Informationen zu verwenden, ist einfach zu groß. Was also ist notwendig, um persönliche Informationen effektiv zu schützen? Die Antwort mag überraschend sein: Das beste ist, erst gar keine Informationen zu erzeugen. Wo keine Informationen vorliegen, können diese auch nicht missbraucht werden und stellen keine Gefahr dar. Keine Informationen zu erzeugen klingt sehr schwierig, ist aber eigentlich ganz einfach: man muss nur anonym bleiben.

In vielen Bereichen des Lebens ist die Anonymität ein wichtiger Grundpfeiler der Gesellschaft. So wäre beispielsweise keine demokratische Wahl denkbar, wenn Stimmen mit dem Namen des Wählers verbunden wären. Seelsorge und Selbsthilfegruppen basieren ihre Tätigkeit auf der Anonymität der Hilfesuchenden. Die Schweigepflicht der Ärzte schützt die Anonymität der Patienten und den Patienten dadurch vor Diskriminierung und Ausgrenzung. Die Schweigepflicht von Anwälten und der Schutz der Informationen des Angeklagten ermöglichen eine faire Gerichtsverhandlung. Aber auch im Alltag ist Anonymität mitunter so selbstverständlich, dass wir nicht über sie nachdenken. Wenn wir durch die Stadt gehen, sind wir gegenüber anderen Menschen weitgehend anonym. Wenn wir in einem Geschäft etwas einkaufen, müssen wir dazu nicht unser Geburtsdatum und unsere Adresse angeben.

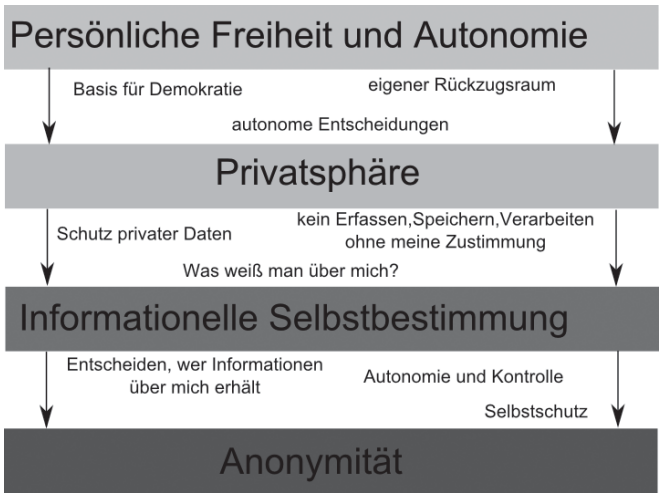
Anders im Internet. Hier ist leider momentan das Gegenteil üblich. Unter anderem durch unsere IP-Adresse hinterlassen wir eindeutige Spuren, aus denen jeder unserer Schritte nachvollzogen werden kann. Da das Internet aber eine immer größere Rolle im Leben der Menschen einnimmt, ist es gerade hier wichtig, die persönlichen Daten zu schützen. Als wie wichtig und einflussreich haben sich in den letzten Jahren kritische Blogs erwiesen? Wie viele Menschen machen vom Internet Gebrauch, um Hilfe oder Informationen zu psychischen Problemen zu finden, von denen ihre Mitmenschen möglichst nichts erfahren sollten?

Momentan ist der Schutz nicht hinreichend. Mit geringem Aufwand kann man sehr viel über einen Menschen herausfinden. Die geplante Vorratsdatenspeicherung sichert diese Informationen auch noch über eine lange Zeitspanne. Also ist es naheliegend, auch im Internet mehr auf Anonymität zu setzen, um Persönlichkeit und Privatsphäre zu schützen.

Es gibt inzwischen eine ganze Reihe von Softwareprogrammen und Diensten, die die Anonymität im Netz erhöhen. Bekannte Vertreter sind hierbei z.B. Tor, JAP und I2P. Zudem gibt es vielversprechende Neuentwicklungen, wie das *Phantom*-Protokoll, die technisch immer ausgefeiltere Methoden anwenden. Allen diesen Ansätzen ist gemein, dass sie durch geschicktes Routing versuchen, die IP-Adressen der Kommunikationspartner zu verschleiern und die übertragenen Informationen durch Verschlüsselung unlesbar zu machen. Dadurch sind die bei der Kommunikation anfallenden Informationen nicht mehr einer Person zuzuordnen und somit effektiv anonymisiert. Tor und JAP setzen dabei auf leistungsstarke Router, welche den Nutzern zur Verfügung gestellt werden. I2P und Phantom dagegen setzen auf eine durchgehende Peer-to-Peer-Infrastruktur: Jeder Nutzer des Dienstes soll gleichzeitig den anderen Teilnehmern als Router dienen.

Alle diese technischen Ansätze geben große Hoffnung; für einen umfassenden Schutz muss jedoch auch ein juristisches Fundament für ein Recht auf Anonymität geschaffen werden. So ein Recht ist keineswegs utopisch: Bereits jetzt finden sich in vielen nationalen Gesetzen (z.B. Telemediengesetz, Telekommunikati-

onsgesetz) und internationalen Abkommen (z.B. europäische Datenschutzrichtlinien, Erklärung zur Kommunikationsfreiheit im Internet, OECD guidelines for cryptography policy) Passagen über Anonymität.



Ein Recht auf Anonymität lässt sich leicht begründen. In der Aufklärung haben sich persönliche Freiheit und Autonomie als Grundpfeiler der Demokratie erwiesen. Beide benötigen eine weitreichende Privatsphäre als Voraussetzung (Recht auf Privatsphäre). Im Informationszeitalter muss diese Privatsphäre auf Informationen ausgeweitet werden, um persönliche Freiheit und Autonomie weiterhin sicherstellen zu können (informationelle Selbstbestimmung). Autonomie und effektive Kontrolle dieser Informationen jedoch benötigen heute Anonymität.

Schlussfolgernd lässt sich sagen, dass im Informationszeitalter durch zunehmende Überwachung und Datenverarbeitung mehr und mehr Informationen anfallen, an welchen Regierungen und Unternehmen großes Interesse haben. Die Verbreitung privater Informationen stellt jedoch eine große Gefahr für einige der wichtigsten Errungenschaften der Menschheit dar, darunter Meinungsfreiheit, Demokratie, das soziale Netz, kritisches Denken und Informationsfreiheit. Nur eine Anonymisierung kann diese Informationen effektiv schützen. Diese Anonymität kann jedoch nur auf soliden technischen und juristischen Grundlagen gewährleistet werden.

> *„Der letzte Zweck des Staates ist nicht, zu herrschen, die Menschen in der Furcht zu erhalten und fremder Gewalt zu unterwerfen, sondern vielmehr den Einzelnen von der Furcht zu befreien, damit er so sicher als möglich lebe, d.h. so, dass er sein natürliches Recht zum Dasein ohne seinen und Anderer Schaden am besten sich erhalte. Ich sage, es ist nicht der Zweck des Staates, die Menschen aus vernünftigen Wesen zu wilden Thieren oder Automaten zu machen; sondern ihre Seele und ihr Körper soll in Sicherheit seine Verrichtungen vollziehen, sie sollen frei ihre Vernunft gebrauchen und weder mit Hass, Zorn oder List einander bekämpfen, noch in Unbilligkeit gegen einander verfahren. Der Zweck des Staates ist in Wahrheit die Freiheit.“*
>
> Spinoza, Tractatus Theologico-Politicus (1670)

Michael Prinzinger hat an der Universität Nürnberg-Erlangen studiert. Die prämierte Arbeit entstand an der technischen Fakultät, Lehrstuhl Verteilte Systeme und Betriebssysteme.

about WebAG

Das Ziel der WebAG ist die Modernisierung der FIfF-Webseiten. Wir möchten die verschiedenen Web-Aktivitäten des FIfF auf den Webseiten integrieren sowie sie regelmäßig mit Inhalten aus der FIfF-Kommunikation aktualisieren.

In einem ersten Schritt möchten wir mit einer Vorgehensweise nach IT-Grundschutz (desBSI) die organisatorische Struktur der Webredaktion klären und uns Gedanken über die Bedürfnisse und Wünsche der FIfF-Leser für die Webseite machen. Daraus sollen dann Anforderungen an Navigation, Layout und Struktur der Webseiten abgeleitet werden.

In einem zweiten Schritt sollen dann die Ergebnisse entsprechend technisch umgesetzt werden.

Wir suchen nach Lesern, die Spaß und Freude daran haben, jetzt am Anfang konzeptionell mitzuarbeiten und dann ggf. nach Etablierung der Strukturen die Redaktion unterstützen. Einen Mail-Verteiler für Interessierte gibt es schon *web-ag@lists.fiff.de* [1]. Wir freuen uns immer über Kritik und Anregungen, die Ihr zu unserer Arbeit habt!

Viele Grüße

Raffael Rittmeier und Sebastian Jekutsch

[1] *http://lists.fiff.de/mailman/listinfo/web-ag*

Stefan Hügel

Ereignis-Log 4/2010

Immer wieder gibt es Ereignisse, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau von Bürgerrechten stehen. Wir dokumentieren hier einige davon. Die Aufzählung kann nicht vollständig sein; mit einigen besonders bedeutsamen Ereignissen wollen wir aber auf die weiterhin besorgniserregende Entwicklung hinweisen.

August 2010

19. August 2010: Die rheinland-pfälzische Landesregierung beschließt eine Novelle des Polizei- und Ordnungsbehördengesetzes. Dieses schafft umfangreiche Überwachungsbefugnisse für die Landesbehörden. Erlaubt werden damit Online-Durchsuchungen und die Überwachung verschlüsselter Internet-Telefonie. Zugelassen werden sollen auch beispielsweise Rasterfahndungen (Quelle: netzpolitik.org).

19. August 2010: Die Bundesländer kritisieren die Bundesregierung wegen ihrer Zurückhaltung bei der Einführung gesetzlicher Regelungen für *Google Street View*. Der Bundesrat hatte einen eigenen Gesetzentwurf vorgelegt; Innenminister de Maizière strebt eine Regelung an, die auch andere Dienste berücksichtigt (Quelle: Heise).

20. August 2010: Bei der *Alten Leipziger Versicherung* waren ca. 3.600 Versicherungsanträge zeitweise ungeschützt zugänglich. Die Daten wurden über einen Tarifrechner aufgenommen und enthielten unter anderem Daten wie Bankverbindung, Beruf, Fahrzeuge, allfällige Vorschäden und den bisherigen Versicherer (Quelle: Heise).

25. August 2010: Nach einem Bericht im Forbes-Blog werden in den USA mobile Röntgenscanner eingesetzt, mit denen Fahrzeuge durchleuchtet werden können. Diese wurden zunächst in Afghanistan und im Irak eingesetzt; mittlerweile sind sie auch in den USA im Einsatz (Quelle: netzpolitik.org, Forbes).

27. August 2010: Bei der Drogeriekette *Schlecker* sind ca. 150.000 Datensätze von Online-Kunden zeitweise frei über das Internet zugänglich. Die Daten enthalten Anschrift, E-Mail-Adresse und Geburtsdatum und lassen Rückschlüsse auf bestellte Waren zu (Quelle: Heise, netzpolitik.org, Bild).

27. August 2010: Aufgrund einer Klage gegen die *Bergische Krankenkasse* unter Berufung auf das informationelle Selbstbestimmungsrecht wird nun die verfassungsmäßige Unbedenklichkeit der elektronischen Gesundheitskarte geprüft. Die Richterin des Düsseldorfer Sozialgerichts will die Frage dem Bundesverfassungsgericht vorlegen. Die Klage des Wuppertalers wird durch die *Freie Ärzteschaft* unterstützt, die auf einen Stopp des Projekts „staatlicher Datengier" hofft (Quelle: Heise).

September 2010

1. September 2010: Patrick Breyer vom AK Vorrat und Wolfgang Wieland, Bundestagsabgeordneter der Grünen, reichen Verfassungsbeschwerde gegen das Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSI-Gesetz) ein. Die Regelungen ermächtigten zu einer grenzenlosen Vorratsdatensammlung, so Wieland. Breyer erläutert, „dass die dem BSI erlaubte Kommunikations- und Surfprotokollierung direkt durch den Staat erfolgen und sogar die aufgerufenen Internetseiten umfassen soll, macht die Regelung von Grund auf verfassungswidrig, wenn man die Maßstäbe des Verfassungsgerichtsurteils zur Vorratsdatenspeicherung zugrunde legt" (Quelle: Arbeitskreis Vorratsdatenspeicherung, Heise).

8. September 2010: Die automatisierte Erfassung von IP-Adressen für Massenabmahnungen in der Schweiz ist nach einem Urteil des schweizerischen Bundesgerichts rechtswidrig. Die *Logistep AG* hatte die Adressen im Auftrag der Inhaber von Urheberrechten in P2P-Tauschbörsen protokolliert, um Rechteverletzer ausfindig zu machen (Quelle: Heise).

9. September 2010: Das Finanzgericht Köln weist Klagen gegen die Steuer-ID ab. Der 2. Senat äußert zwar Zweifel an der Verfassungsmäßigkeit, sieht aber nicht, dass des Recht des Einzelnen auf informationelle Selbstbestimmung schwerer wiege als das Interesse der Allgemeinheit an gleichmäßiger Besteuerung. Das Gericht hat deswegen die Frage nicht dem Bundesverfassungsgericht vorgelegt (Quelle: Heise).

14. September 2010: Das Bundesverfassungsgericht lehnt einen Eilantrag gegen den elektronischen Entgeltnachweis ELENA ab. Der erste Senat räumt ein, dass die Datenspeicherung einen Grundrechtseingriff darstelle, hält es aber für ausreichend, die Verfassungsmäßigkeit im Hauptverfahren zu prüfen, das für 2011 erwartet wird (Quelle: Bundesverfassungsgericht, Heise).

22. September 2010: In Indien wird damit begonnen, Erfassungsgeräte für das größte Biometrieprojekt der Welt auszurollen. Ziel des Projekts ist der Aufbau einer zentralen Datenbank in der in vier bis fünf Jahren biometrische Daten der Hälfte der erwachsenen indischen Bevölkerung gespeichert werden sollen – rund 600 Millionen Datensätze. In zwei Bundesstaaten werden ab Oktober ID-Nummern vergeben, die später alle Inder erhalten sollen. Bis 31. Dezember 2011 sollen die für das Projekt erforderlichen Fingerabdruck- und Iris-Scanner installiert sein (Quelle: Heise).

24. September 2010: Bundesjustizministerin Leutheusser-Schnarrenberger plant weiterhin trotz kritischer Stimmen die Einrichtung einer „Stiftung Datenschutz". Sie will damit die Kompetenz der Bürger im Umgang mit elektronischen Spuren im Internet und im öffentlichen Leben fördern. *Edgar Wagner*, Landesdatenschutzbeauftragter von Rheinland-Pfalz kritisiert daran vor allem, dass die Stiftung mit Geld der Wirtschaft aufgebaut werde und damit ihre Unabhängigkeit gefährdet sei (Quelle: Heise).

24. September 2010: Bundesinnenminister Thomas de Maizière will Befugnisse für die innere Sicherheit erheblich erweitern. Er fordert dazu die heimliche Online-Durchsuchung mit dem Bundestrojaner und die Quellen-Telekommunikationsüberwachung, beispielsweise zum Abhören von Gesprächen über VoIP. Bundesjustizministerin Leutheusser-Schnarrenberger hatte eine ähnliche Liste, die der Vorgänger de Maizières, Schäuble, veröffentlicht hatte, seinerzeit als „Horrorliste" bezeichnet. „Wir haben uns in der Koalition darauf verabredet, mit dem Stakkato immer neuer Sicherheitsgesetze aufzuhören", so die Ministerin (Quelle: Heise, Welt, Hamburger Abendblatt).

27. September 2010: Der Nacktscanner-Probebetrieb am Hamburger Flughafen beginnt. Zwei Geräte sollen nach Angaben des Innenministeriums für sechs Monate getestet werden. Bundesinnenminister Thomas de Maizière hält dies für einen wichtigen Schritt auf dem Weg zu mehr Flugsicherheit. Die Scanner sind seit Beginn der Diskussion 2008 heftig umstritten; auch der damalige Bundesinnenminister Schäuble hatte seinerzeit erklärt, sie nicht einsetzen zu wollen: „Solange solche Bilder entstehen, ..." Die neuen Nacktscanner zeigen den Körper schematisch (Quelle: Heise).

28. September 2010: In Österreich betreibt die Polizei stationäre Kameras, die alle vorbeifahrenden Fahrzeuge photographieren. Die Kennzeichen werden dann mit der Fahndungsdatenbank EKS – Elektronisches Kriminalpolizeiliches Informationssystem – abgeglichen. Löst das System Alarm aus, wird das Photo einem Beamten vorgelegt, der ggf. eine Fahndung auslöst. Bei Fehlalarm wird nach Angaben des Innenministeriums der Datensatz sofort gelöscht (Quelle: Heise).

30. September 2010: Die EU-Kommission klagt wegen der verdeckten Tests des Online-Werbedienstleisters *Phorm* gegen Großbritannien. Zuvor hatte die Kommission ein Vertragsverletzungsverfahren bereits wegen Verstoßes gegen die EU-Richtlinien zur Vertraulichkeit der elektronischen Kommunikation eingeleitet. Bemängelt wird, dass nach britischem Recht die Protokollierung der Kommunikation zu Werbezwecken auch dann erlaubt sein kann, wenn der betroffene Nutzer nicht eingewilligt hat (Quelle: Heise).

30. September 2010: Der Deutsche Bundestag spricht sich mit den Stimmen der Regierungskoalition bei Enthaltung der SPD gegen einen Antrag der Grünen zur Aussetzung und strikten Begrenzung des Elektronischen Entgeltnachweises (ELENA) aus (Quelle: Deutscher Bundestag, Heise).

Oktober 2010

1. Oktober 2010: Das Bundesverfassungsgericht nimmt die Verfassungsbeschwerde gegen das Gesetz über den registergestützten Zensus, der von ca. 13.000 Personen unterstützt wurde, nicht zur Entscheidung an. Zur Begründung erklärte das Gericht, nicht das gesamte Gesetz könne Gegenstand einer Verfassungsbeschwerde sein; die angegriffenen Bestimmungen müssten genau bezeichnet werden. Die Beschwerdeführer hätten aber beantragt, das ganze Gesetz als unvereinbar mit ihren Grundrechten zu erklären (Quelle: Bundesverfassungsgericht, Heise).

1. Oktober 2010: Die Bezirksverordnetenversammlung Tempelhof-Schöneberg in Berlin hat das zuständige Bezirksamt beauftragt, die Legalität eines Internet-Prangers für Freier rund um den U-Bahnhof Kurfürstenstraße zu prüfen (Quelle: Heise).

4. Oktober 2010: Ein Polizeibeamter wird im Prozess zur Polizeigewalt auf der Demonstration „Freiheit statt Angst" 2009 zu einer Geldstrafe von 80 Tagessätzen zu €60 verurteilt. Das Amtsgericht Berlin-Tiergarten sah es als erwiesen an, dass der Beamte am 12. September 2009 einem Angestellten mit der Faust in den Rücken geschlagen habe (Quelle: Heise).

8. Oktober 2010: Beim Privatsender RTL2 startet die TV-Serie *Tatort Internet – schützt endlich unsere Kinder*, bei der mutmaßliche Sexualstraftäter in eine Falle gelockt und vor laufender Kamera – verpixelt – gestellt und befragt werden. Kritiker monieren, dass die Sendung keine Aufklärung biete, sondern die Bloßstellung zum Ziel habe, die „merkwürdig sadistisch" anmute. Unterstützt wird die Sendung von der Präsidentin der Organisation *Innocence in Danger*, Stephanie zu Guttenberg (Quelle: RTL2, Heise).

11. Oktober 2010: Aus dem Premiumbereich auf der Webseite der Wochenzeitung *Die Zeit* sind Kundendaten kopiert worden. Diese umfassen Namen, Adressen, E-Mail-Adressen und teilweise Kontoverbindungen. Zum Tatzeitraum und zur Frage, ob es ein interner oder externer Angriff gewesen sein, gab es keine Angaben (Quelle: Heise).

15. Oktober 2010: Mehrere EU-Parlamentarier kritisieren in einer schriftlichen Erklärung das Überwachungsprojekt INDECT – *Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment*. Die Initiatoren sehen weitgehende Einschnitte in die Privatsphäre der Bürger. Mit Fördergeldern der Union werde an einer großen „Menschensuchmaschine" geforscht, so *Alexander Alvaro*, innenpolitischer Sprecher der FDP im EU-Parlament. Diese solle „die gleichzeitige Überwachung und Abgleichung von Internetseiten, Videomaterial aus Überwachungskameras und privaten Computern ermöglichen". Gegen die Unterstützung unabhängiger Forschung sei zwar nichts einzuwenden, die Dimension der Unternehmung sei aber so groß, „dass hier keine abschließenden Tatsachen geschaffen werden dürfen" (Quelle: Heise).

20. Oktober 2010: Der Hamburgische Datenschutzbeauftragte *Johannes Caspar* hat Strafantrag gegen ein Unternehmen des EC-Kartendienstleisters *Easycash* gestellt. Easycash habe über eine Hamburger Tochter Daten aus dem EC-Zahlungsverkehr mit Kundenkartendaten abgeglichen und dem Handel Zahlungsverkehrsanalysen angeboten (Quelle: Heise).

23. Oktober 2010: Google-Manager *Alan Eustace* teilt in einem Blog-Eintrag mit, dass Street View Fahrzeuge bei ihren WLAN-Scans auch unverschlüsselte E-Mails und Passwörter aufgezeichnet haben (Quelle: The Official Google Blog – googleblog.blogspot.com, Heise).

25. Oktober 2010: Im *Rabenhof-Theater* in Wien werden die diesjährigen Preisträger der *BigBrotherAwards Österreich* ausgezeichnet. Den Preis erhielten *Gudrun Höfner* von der Firma

ITworks für das Datenabzapfen bei Langzeitarbeitslosen in der Kategorie *Business und Finanzen*, *Josef Pröll* von der ÖVP für den Aufbau einer zentralen Datenbank mit Finanzdossiers aller Bürgerinnen und Bürger in der Kategorie *Politik*, die Staatsanwaltschaft Wien für die Einvernahme österreichischer Journalisten in der Kategorie *Behörden und Verwaltung*, *T-Mobile Austria* für den Umgang mit kostenpflichtigen SMS in der Kategorie *Kommunikation und Marketing* und die „Internetabsperrer" in der Kategorie *Lebenslanges Ärgernis*. Preisträgerin der Volkswahl ist die Justizministerin *Claudia Bandion-Ortner* (ÖVP) für das Terrorismuspräventionsgesetz. Den Positivpreis *Defensor Libertatis* erhielten *John Young* u.a. für das Projekt *Cryptome.org* zur Veröffentlichung von Dokumenten – einem Vorgänger von Wikileaks. In der Kategorie Politik wurde auch *Christian Felber* von *Attac* für seine Forderung nominiert, das Bankgeheimnis in Österreich abzuschaffen. Attac hat dazu in einer umfassenden Stellungnahme begründet, warum man an der Forderung festhält (Quelle: BigBrotherAwards.at, Heise).

29. Oktober 2010: Die EU-Kommission erhebt Klage vor dem Europäischen Gerichtshof (EuGH) gegen Österreich. Österreich habe die Datenschutzrichtlinie von 1995 mangelhaft umgesetzt. Insbesondere stehe die österreichische Datenschutzkommission (DSK) unter der Aufsicht des Bundeskanzleramts und sei damit nicht unabhängig, wie in der Richtlinie gefordert. Im März hatte der EuGH bereits festgestellt, dass in Deutschland die in den Ländern für den Datenschutz zuständigen Stellen nicht unabhängig seien; auch dies verstoße gegen Europarecht (Quelle: Heise).

November 2010

2. November 2010: Der Bundesrat legt eine Reihe von Änderungsanträgen zum Regierungsentwurf des Arbeitnehmer-Datenschutzgesetzes vor. Formal kritisieren sie, dass die Bundesregierung kein eigenes Gesetz vorlegt, sondern nur einen „Unterabschnitt im Bundesdatenschutzgesetz" novellieren will. Inhaltlich fordern die Landespolitiker eine stärkere Einschränkung der Videoüberwachung – insbesondere ein Verbot der Verwendung von Aufzeichnungen zur Leistungs- und Verhaltenskontrolle – und die Einschränkung verdachtsloser Abgleiche zur Korruptionsbekämpfung (Quelle: Deutscher Bundesrat, Heise).

5. November 2010: Polizei und Verfassungsschutz wollen im Zuge der Modernisierung ihrer Informationssysteme künftig Daten per Volltextsuche erschließen, die bisher nur in den Akten vorhanden sind. Die Datenschutzbeauftragte warnen davor und fordern in einer Entschließung auf, dies nur in sehr engen verfassungsrechtlichen Grenzen zuzulassen (Quelle: Bundesdatenschutzbeauftragter, Heise).

8. November 2010: Nach einer Studie der *Hans-Böckler-Stiftung* missachten viele Betriebe die Privatsphäre ihrer Angestellten. 2000 Betriebsräte berichteten in einer repräsentativen Befragung von Datenschutzverstößen. Umfrageleiter *Martin Behrens* geht aber von einer noch höheren Dunkelziffer aus. Probleme gebe es in Betrieben jeder Größe; besonders groß sei der Anteil der Verstöße in Großbetrieben (Quelle: Hans-Böckler-Stiftung, Heise).

8. November 2010: Die US-Bürgerrechtsorganisation EPIC – *Electronic Privacy Information Center* – veröffentlicht seine Klageschrift gegen das Flughafen-Sicherheitsprogramm der Regierung. Die Durchleuchtung sei „illegal und ineffektiv" und verletze mehrere Gesetze und die Verfassung der Vereinigten Staaten (Quelle: EPIC, Heise).

8. November 2010: Nach Berichten von *Global Voices Advocacy* werden in Thailand 256.110 Webseiten durch die dortige Zensurinfrastruktur gesperrt (Quelle: netzpolitik.org).

9. November 2010: Die Homepage kernenergie.de des *Deutschen Atomforums* wird von Hackern übernommen. Zeitweise ist der Slogan „Kernenergie – so sicher wie diese Webseite" zu sehen. Die Seite wurde zunächst vom Netz genommen und ist mittlerweile wieder verfügbar (Quelle: Heise).

9. November 2010: Jeder zweite Personalchef – 49% – informiert sich im Internet über Bewerber. Dies ergibt eine Studie des Branchenverbands *Bitkom*. Genutzt würden vor allem Suchmaschinen (Quelle: Bitkom, Heise).

9. November 2010: Bereits am ersten Tag nach der Veröffentlichung der *AusweisApp*, der Software zum neuen Personalausweis, wurde durch *Jan Schejbal* von der Piratenpartei Deutschland eine Sicherheitslücke aufgedeckt. Zwar lässt sich der Ausweis dadurch nicht auslesen, man kann aber Schadsoftware auf dem Rechner einschleusen, auf dem die AusweisApp läuft. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) kündigt später eine neue Version der Software an (Quelle: Piratenpartei Deutschland, Heise, netzpolitik.org).

10. November 2010: Sachverständige haben bei einer Anhörung im Rechtsausschuss des Bundestages in ihren Stellungnahmen den Schwebezustand beim Zugangserschwerungsgesetz als rechtswidrig bezeichnet. Auch das Gesetz selbst wird als verfassungswidrig angesehen. Die Nichtanwendung des Gesetzes verstoße gegen die Pflicht der Verwaltung, geltende Rechtsnormen zu vollziehen (Quelle: Deutscher Bundestag, Heise).

12. November 2010: Bundesdatenschutzbeauftragter *Peter Schaar* schlägt eine abgeschwächte Form der Vorratsdatenspeicherung vor. Die Daten sollen anlasslos über einen Zeitraum von zwei Wochen vorgehalten werden. Damit rücken Schaar und auch der Leiter des Unabhängigen Landeszentrums für Datenschutz (ULD) Schleswig-Holstein, *Thilo Weichert*, der die Forderung unterstützt, von bisherigen Forderungen ab, auf die Vorratsdatenspeicherung vollständig zu verzichten (Quelle: Bundesdatenschutzbeauftragter, Heise, Zeit.de, taz.de).

Stefan Hügel

Stefan Hügel ist Vorsitzender des FIfF, arbeitet als IT-Berater und lebt in Frankfurt am Main

Wir trauern um

Prof. Dr. Andreas Pfitzmann

der am 23. September 2010 verstorben ist.

Andreas Pfitzmann prägte in Deutschland den wissenschaftlichen und politischen Diskurs über Datenschutz und informationelle Selbstbestimmung. Er hat dabei als Wissenschaftler immer mit Nachdruck eine fundierte unabhängige Meinung vertreten und vermochte stets, über die Grenzen seiner Disziplin hinweg die Auswirkungen von Technik verständlich zu machen. Er engagierte sich in der Forschung mit Kompetenz, Eloquenz und Courage und gewann damit ein hohes internationales Renommee.

Seit 1993 leitete Andreas Pfitzmann die Forschungsgruppe „Datenschutz und Datensicherheit" an der Fakultät Informatik der Technischen Universität Dresden. Er war Sachverständiger für das Bundesverfassungsgericht, unterschiedliche Bundesregierungen, mehrere Parteien, die EU-Kommission und die OECD.

Wir verlieren mit Andreas Pfitzmann einen herausragenden Wissenschaftler und einen einzigartigen Verteidiger des Rechts auf Anonymität und der informationellen Selbstbestimmung – den Grundvoraussetzungen für eine gelebte Demokratie. Unvergessen bleiben uns seine mitreißenden Vorträge und seine anregenden Gedankenexperimente. Mit seinem nachdrücklichen Einsatz dafür, auch unangenehme Wahrheiten auszusprechen, wird er uns stets ein Vorbild sein.

Unsere Gedanken und unser Mitgefühl sind bei seinen Angehörigen.

Vorstand und Beirat des FIfF

Andreas Pfitzmann

Biometrie

Neue Sicherheitsprobleme

Überwachbarkeit und Datenschutz müssen nicht nur innerhalb einzelner Anwendungen (wie Reise- und Zahlungsverkehr, E-Mail, Überwachungskameras, ...) ausbalanciert werden, sondern über Anwendungen hinweg. Die geplanten Pässe schaffen ernste Sicherheitsprobleme. Fingerabdrücke in Pässen fördern Kriminalität mehr, als sie sie bekämpfen, und erschweren polizeiliche Ermittlungen – also keine Fingerabdrücke in Pässen!

In der Biometrie werden Körper- oder Verhaltensmerkmale gemessen, um durch Vergleich mit Referenzwerten Menschen zu authentifizieren oder zu identifizieren. Die Fehlerrate beim Erkennen (und Zulassen) hängt reziprok mit der beim Nicht-Erkennen (Abweisen) zusammen. Heute und zumindest auch in der überschaubaren Zukunft können nicht beide Fehlerraten so weit gesenkt werden, wie wir dies von Systemen kennen, die auf Wissen (z.B. Passwort/PIN) oder Besitz (z.B. Chipkarte) der Menschen beruhen.

Sicherheitsprobleme für klassische forensische Techniken

1. Verbreitete und umfangreiche Datenbanken mit Fingerabdrücken oder generelles „Abgeben" des Fingerabdrucks erleichtern den Nachbau von „Fingern" und damit das Hinterlassen falscher Fingerabdrücke. Je mehr Fingerabdrücke mit Kontextdaten zur Auswahl stehen, desto hilfreicher für Kriminelle und fremde Geheimdienste.

2. Werden mittels Fingerabdruck-Biometrie große Werte gesichert, wird eine Finger-Nachbau-„Industrie“ entstehen.

3. Da Infrastrukturen beispielsweise für Grenzkontrollen weniger schnell zu aktualisieren sind als einzelne Maschinen zum Fingernachbau, ist insgesamt ein Sicherheitsverlust zu erwarten.

Diebstahl von Körperteilen

4. Die (vermeintliche) Verbesserung der Sicherheit durch Biometrie kann die körperliche Unversehrtheit der Betroffenen gefährden. Es wurden schon Finger abgeschnitten, um ein Auto zu stehlen.

5. Sollte biometrische Lebenderkennung funktionieren, dürften Entführung oder Erpressung den Diebstahl von Körperteilen ersetzen.

Datenschutzprobleme

Datenschutz durch Löschung funktioniert im Internet nicht, da man alle Kopien entdecken müsste: Bereits die Erhebung der Daten muss vermieden werden.

Es ist ein wesentlicher Unterschied, ob der zu vermessende Mensch explizit mitwirken muss (aktive Biometrie), so dass er sich der Messung bewusst ist, oder ob seine Mitwirkung unnötig ist (passive Biometrie), sodass eine Messung ohne sein Wissen erfolgen kann.

6. Daten lassen sich ohne Information der Betroffenen erheben und auswerten, z.B. bei der Gesichts- oder Spracherkennung.

7. Ein Netzhaut-Scan liefert Daten über den Alkoholkonsum der letzten beiden Tage, der Fingerabdruck möglicherweise über Homosexualität. Das kann Menschen erpressbar machen.

8. RFIDs in Pässen sind unsicher. Das RFID kann auslesen, wer immer Zugriff auf den Papierteil hatte (ausstellendes Land, Grenzposten bei Ein- oder Ausreise, Händler, die z.B. Mobilfunkverträge verkaufen und dabei eine Papierkopie des Passes erhalten) oder die Kooperation einer solchen Person. RFIDs in Pässen müssen deshalb entweder vermieden oder beispielsweise durch eine metallische Hülle des Passes vor unbemerktem Auslesen geschützt werden.

9. Werden mehrere biometrische Merkmale erfasst, um die Unsicherheit einzelner Merkmale zu kompensieren, vervielfacht dies das Datenschutzproblem.

Enttarnung gewünschter Mehrfachidentitäten

Staaten werden nicht nur Terroristen und Kriminelle, sondern auch fremde Geheimdienstagenten enttarnen wollen und dazu personenbezogene Biometriedatenbanken anlegen. Die organisierte Kriminalität wird Biometriedatenbanken zur Enttarnung verdeckter Ermittler oder von Personen in Zeugenschutzprogrammen anlegen.

Biometrie – wie einsetzen und wie keinesfalls?

Zwischen Menschen und ihren Geräten ist die Authentifizierung durch Besitz und/oder Wissen *und* Biometrie unproblematisch. Forensische Techniken werden nicht entwertet, es entstehen keine Datenschutzprobleme.

Es bleibt das Problem des Diebstahls von Körperteilen. Eine Abschaltmöglichkeit der Biometrie nach der Authentifizierung kann Entführungsopfern die Chance geben, durch Kooperation mit ihren Entführern unversehrt zu bleiben. Auch Kompromisse zwischen keinerlei Abschaltbarkeit und vollständiger, dauerhafter Abschaltbarkeit können sinnvoll sein, natürlich nur, wenn allgemein bekannt.

Wir sollten anderen Staaten das Anlegen von Biometrie-Datenbanken über ihre Besucher weder durch ein „Abrichten“ auf brave Mitwirkung an jedem beliebigen Lesegerät erleichtern noch durch Maschinenlesbarkeit unserer Reisepässe verbilligen. In Demokratien ist vor dem breiten Einsatz von Biometrie in Infrastrukturen, etwa in Ausweisen, eine qualifizierte, plurale Debatte nötig. Sie wird bisher von den Innen- und Sicherheitspolitikern der westlichen Industriestaaten verweigert oder – wo dies nicht möglich ist – durch unhaltbare Versprechungen oder grob einseitige Problemdarstellungen manipuliert.

Passive Biometrie durch fremde Geräte ist vom Betroffenen nicht erkennbar und darum kaum zu verhindern. Verdeckt angewandte technisch unterstützte Biometrie sollte unter Strafe gestellt werden.

Nachdruck des Beitrags von Andreas Pfitzmann aus der Sonderausgabe der FIfF-Kommunikation August 2007 „Wider den Zeitgeist“

Eva Dworschak

Wohin entwickelt sich unsere Demokratie?

Seit fast einen Jahrzehnt werden Grundrechte zunehmend eingeschränkt und dabei die Freiheitsrechte der Bürger beschnitten. Wie kam es dazu – und regt sich Widerstand?

In der letzten Zeit wird das Verfassungsgericht als letzte und rettende Instanz angerufen, es scheint fast so, als verließe sich das Volk inzwischen auf die Korrektur der politischen irrgelaufenen Schnellschüsse. Das ist eine Fatalität, die verhindert werden muss und auch zunehmend wird, da das Bundesverfassungsgericht weder alsKontrollinstanz, noch als erfolgreiches Korrektiv zu sehen ist. Nicht für jeden erkennbar, zeigt aber ein neuer Widerstand, eine Art neue Aufklärung viele Gesichter unter der Bevölkerung. Es stellt sich daher die Frage nach den Gründen der Grundrechtskorrosion und einem möglichen Wandel hin zur Sicherung unserer Demokratie.

Die Verlässlichkeit des Hohen Gerichts nicht verkennend, muss doch die Anrufung des Gerichts als *ultima ratio* und das darin immanente Risiko als solches gesehen werden. Die Gefahr eines stetig voranschreitenden Verlustes der Grundrechte und grundrechtsrelevanten Rechte liegt auf der Hand:

Zum Einen birgt das Zuwarten bis zur Beschwerdeerhebung die Gefahr, dass bereits kodifizierte Gesetze ganz oder zumindest in Teilen erhalten bleiben und auch Begleitgesetze gar nicht mehr in eine Überprüfung einbezogen werden. Es ist also vonnöten, dass bereits bei der politischen Debatte die richtige Richtung eingeschlagen wird und grundrechtsrelevante Aspekte berücksichtigt werden.

Zum Anderen ist die rigide Annahmepraxis des Verfassungsgerichts hinlänglich bekannt, die sich lediglich auf die Annahme von 2% aller Beschwerden beläuft[1]. Im Übrigen fungiert das Bundesverfassungsgericht auch als Organ, die Grundrechte anlässlich des neuen Zeiten- und Gesinnungswandels auszulegen. Nach Beendigung eines Verfahrens ist zwar noch bestenfalls auf europäischer Ebene ein Vorgehen gegen eine Verletzung möglich, aber oftmals ist zu diesem Zeitpunkt damit die gesetzliche Regelung oder das Handeln besiegelt. Die rigide Praxis, wie auch die verspätete Wahrnehmung von Abwehrmöglichkeiten und fehlende vorangehende wahrgenommene Kontrollinstanzen führen dazu, dass vermehrt grundrechtsgefährdende Handlungsweisen und Strukturregelungen der Politik Fuß fassen.

Das nunmehr 60 Jahre alte Grundgesetz leidet daher an der Dekonstruktion der darin verbürgten Freiheits- und Bürgerrechte.

Ein Gegensteuern oder korrigierendes demokratisches Eingreifen des Volkes kann aber nur mittels ausreichender Informationsgabe, Sachkenntnis und mit hinreichendem Widerstandswillen erreicht werden.

Gesellschaft und Grundrechte

Dass hiervon (noch) nicht ausreichend vorhanden ist, zeigt die zu vernehmende Entwicklung der Grundrechtskorrosion durch die Gesetzgebung seit Erfindung des so genannten Terrors bzw. dessen Neudefinition nach 2001 und dessen Bekämpfung. Während seither etliche Regelungen (Antiterrorgesetze) erlassen wurden, ist die sogenannte *„erregte Gesellschaft"* mit ablenkendem Konsum und dem neuen *„Sensationismus"*[2] beschäftigt. Sie ist weder motiviert, eigentlichen Ärgernissen auf den Grund zu gehen, noch in der Lage die wahren Ambitionen der Gesetzgebenden zu erkennen. Andere wiederum erkennen ob der Flut kaum noch die Möglichkeit, etwas zu tun. Vermehrt wird angenommen, die einschränkenden Gesetze dienten tatsächlich der eigenen Sicherheit. Dabei wird die damit einhergehende Selbstbeschränkung gerne in Kauf genommen, teilweise sogar heroisch als „ich habe ja nichts zu verbergen", und es sei doch „gut, wenn der Gefahr bereits im Vorfeld begegnet wird", unterstützt.

Durch den neuen „Sensationismus" reagieren die Bürger auf medial aufbereitete Risiken statt auf staatliche Repressionen; durch vermehrte mediale Wiedergabe werden sie mit medial erzeugten „moralischen Panikattacken" (Schweinegrippe, sexueller Missbrauch, Kindesentführungen) gefüttert und ihnen wird ein unbedingt zu sicherndes Sicherheitsbedürfnis gegen den *Terror* eingeimpft. Die Verblendung der Bürger, die sich gerne vom Staat lenken lassen, statt sich als Teilhaber zu sehen, und den Sicherheitsverfechtern Glauben schenken, entzieht dem Blick, dass die neugeschaffenen gesetzlichen Regelungen eine Kontrolle und Einsicht in das private Leben ermöglichen, welche in dieser Dimension in noch keinem totalitären Staat herrschte.

Als Folge werden Bürger, die eine kritische Auseinandersetzung wagen, Demokratie leben und schließlich öffentlich handeln, zumeist als irre Verschwörungstheoretiker, bestenfalls als linke Chaoten abgestempelt. Sie wehren sich dagegen, dass ein Staat

sich plötzlich selbst gegen Bürger schützen will und sein Volk unter *Generalverdacht* stellt. Der einhergehende Verschleiß unabdingbarer Grundrechte und die damit korrumpierte Demokratie werden vom Volk in Kauf genommen. Bei der letztendlich als Rechtfertigung für das staatliche Handeln geäußerten Feststellung: „Wir leben doch in einer Demokratie, da kann uns doch nichts passieren!", wird ausnahmslos verkannt, dass eben jene unbedingt weiter verfochten und deren Erhalt erkämpft werden muss. Die Rettung eines Basismodells der Demokratie erfordert die unbedingte Verfechtung unserer grundrechtlich verankerten Freiheitsrechte.

Dem kann auch nicht entgegen gehalten werden, dass die *medialen Zeiten* sich geändert haben und eine Selbstaufgabe des privaten Schutzes durch Bekanntgabe privater Daten in sozialen Netzwerken die Berufung auf Schutz ad absurdum führe. Ganz im Gegenteil, die Bekanntgabe von persönlichen Daten im Internet und andernorts erfolgt freiwillig und zumeist nicht umfassend. Insbesondere ist ein bestimmtes Klientel von Menschen erkennbar, die sich so weitgehend outen, dass von Ihnen sicherlich nicht auf die Allgemeinheit geschlossen werden kann. Eine Rechtfertigung beriefe sich somit nicht nur auf eine Minderheit, sondern auch auf ein nicht vergleichbares privates Phänomen. Währenddessen verläuft die staatliche Beschränkung faktisch heimlich und unfreiwillig unentwegt weiter, während sie sich vor allem nicht mehr nur auf das Ausspähen und Überwachen von persönlichen Daten beschränkt. Das zunehmend öffentlich geführte Leben kann nicht als Rechtfertigungsgrund für generelles, ungeprüftes und unkontrollierbares staatliches Handeln gelten. Grundrechte und daraus ergehende Abwehrrechte dürfen aufgrund dessen nicht per se ausgehebelt werden.

Stattdessen wird der Rechtsstaat umgebaut, der *Terror* ist nunmehr die Rechtfertigung des Vorgehens eines Staates gegen einzelne, bei dem der Staat vor einzelnen (z.T. grundlos unter Verdacht gestellte Bürgern) *geschützt* werden müsse. Dies stellt eine schleichende Abkehr vom bisher geltenden System dar, in dem der Staat (mittels Staatsgewalt) vor dem einzelnen Kriminellen (in der Mehrzahl allenfalls vor Banden und organisierter Kriminalität) schützte.

Die Abkehr vom Rechtsstaat stellt gleichfalls eine *Abkehr von der Demokratie* dar. Unsere Grundrechte erlitten seit 2001 eine Unmenge an Korrosionen durch gesetzliche Neuerungen oder einfach vollzogenen oder angeordneten Maßnahmen, die vermeintlich zum Erhalt einer vermeintlich bedrohten Sicherheit notwendig seien.

Wir sprechen hier alleine von rund 70 Gesetzesänderungen bis 2007 – sie wurden teilweise später durch das Bundesverfassungsgericht zwar revidiert wurden; der *freiheitsschädigende Trend* wurde dadurch jedoch nicht aufgehalten. Schließlich ging damit, begleitet durch das mediale Aufheizen, auch der Meinungswandel einher und das Abstumpfen einer Empfindsamkeit gegenüber dem notwendigen und unabdingbaren Erhalt der verfassungsrechtlich verankerten Rechte sowie die dazugehörende Geisteshaltung.

Gesetzliche Regelungen führen nach und nach zur Grundrechtskorrosion

Schon im Jahr 2001 wurde das erste der folgenden *Terrorismusbekämpfungsgesetze/Antiterrorgesetze* erlassen, die staatliche Kontrolldichte und Informationszugriff auf persönliche Daten erhöhen.

Obwohl es bereits das *Verbrechensbekämpfungsgesetz* gab, startete neu die Verschärfung rechtlicher Regelungen im Luftverkehr. Eingeführt wurden u.a. der Einsatz bewaffneter *Sky Marshalls*, die verschärfte Kontrolle von Personen und Gepäck. Das BKA kann seither leichter auf Flugdaten und Telefonverbindungen zugreifen, die Verfassungsschützer erhielten die Erlaubnis, bei Banken, Postdienstleistern und Luftverkehrsunternehmen Informationen abzufragen.

Die so genannten *Otto-Kataloge* im Jahre 2002 brachten eine Befugniserweiterung des BKA und der Polizei mit sich. Das *Sicherheitspaket II* umfasst dabei die Vereinfachung der Telekommunikationsüberwachung, die Vereinfachung von Rasterfahndungen, die Vereinfachung von Ausländerkontrollen sowie neue Bestimmungen für die Sicherheitsüberprüfung von Beschäftigten an sicherheitsempfindlichen Stellen.

Zu den vollzogenen Maßnahmen gehörte auch die zunächst zur Bekämpfung der RAF eingeführte *Rasterfahndung*, die elektronische Personenselektion, die vor allem Migranten ein gesteigertes Sicherheitsrisiko unterstellte, da nach „Schläfern" gesucht wurde. Zur Weltmeisterschaft im Jahre 2006 führte der bislang wohl umfangreichste Sicherheitscheck zu absurden Ablehnungen, wenn auch nur eine entfernte Kontaktmöglichkeit zu bestimmten Gruppen festgestellt (nicht nachgewiesen) wurde.

Die *Antiterrorgesetze* sind die umfangreichsten Sicherheitsgesetze, die jemals erlassen wurden, und trotz fragwürdiger Er-

Eva Dworschak

Eva Dworschak, Rechtsanwältin

folge wurden sie mit dem *Terrorismusbekämpfungsergänzungsgesetz* Anfang 2007 nochmals um fünf Jahre verlängert und in Teilen weiter verschärft.

So begann 2006/2008 der Aufbau einer *Antiterrordatei auf Grundlage des Antiterrordateigesetzes von 2006*[3], auf die der Zugriff von BKA und Bundesamt für Verfassungsschutz zugelassen wurde. Dies stellt eine unzulässige Aufhebung der gebotenen Trennung von Polizeibehörden und Geheimdiensten dar. Noch im Jahr 2010 erfuhr das Gesetz weitere Verschärfungen.

Ein beliebtes Mittel, um die staatliche Kontrolldichte zu erhöhen, stellt die verdachtslose *Videoüberwachung* dar, die zwar in den 90er Jahren ihre Entstehung, aber erst nach 9/11 einen explodierenden Einsatz fand. Dabei stellt die Videoüberwachung ebenfalls einen erheblichen Eingriff in das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht der informationellen Selbstbestimmung dar. Eine gesetzliche Ermächtigungsgrundlage war zunächst nicht greifbar, auf das Bundesdatenschutzgesetz oder andere hierfür zu unbestimmte Rechtsnormen darf das Handeln nicht gestützt werden. So befand das Bundesverfassungsgericht[4] dann im Jahr 2007, dass die entsprechenden Normen keine hinreichenden Vorgaben für Anlass und Grenzen der erfassten datenbezogenen Maßnahmen enthielten, um als Ermächtigungsgrundlage für den beabsichtigten Grundrechtseingriff in Betracht zu kommen.

Beachtenswert ist hier jedoch die Einschränkung durch das Bundesverfassungsgericht, indem es einräumt, dass eine Überwachungsmaßnahme mittels einer bestimmten und normenklaren Rechtsgrundlage verfassungsgemäß sei. Voraussetzung sei ein hinreichender Anlass für die Überwachung, aber grundsätzlich sei diese unter Beachtung der erforderlichen Voraussetzungen dann zulässig. So müssten Überwachung sowie Aufzeichnung insbesondere in räumlicher und zeitlicher Hinsicht und im Hinblick auf die Möglichkeit der Auswertung der Daten das Übermaßverbot wahren. Hier zeigt sich, dass auch das Hohe Gericht mit der allgemeinen Gesinnungsänderung selbstverständlich Schritt hält.

Folglich findet sich beispielsweise für eine konkrete Strafverfolgung (und nicht bloße Gefahrenabwehr) mittels polizeilicher Videoaufnahmen eine Rechtsgrundlage in §100c StPO. Nach und nach wurden aber die polizeilichen Instrumente in den landesgesetzlichen Polizeigesetzen verschärft, so dass wiederum eine verdachtsbezogene Überwachung möglich ist. Da die Überwachung viele Rechtsgebiete tangiert, wird hier auf eine Darstellung relevanter Urteile[5] verwiesen. Es zeigt sich eine zunehmende generelle Akzeptanz gegenüber diesem Verfahren. Und es eröffnet sich die bange Frage, wie unser zukünftiges Leben mit Mitbürgern aussehen mag, die als Kind stets von Staat und Eltern auf Schritt und Tritt überwacht wurden.

Auch hier kann nicht das Phänomen herangezogen werden, dass *freiwillige Selbstdarstellungen* in Youtube oder Einrichtungen von dauerhaft verfolgbaren Webcams oder die Einrichtung einer App, das anderen die eigene Standortverfolgung erlaubt, eine ebenso tiefgreifende Überwachungsmöglichkeit darstellt. Dies ist und bleibt jedes Mal eine einzelne individuelle Entscheidung, die jeder für sich selbst fällt und deren Konsequenzen sich nur gegen die eigene Person richten. *Die staatlich organisierten Maßnahmen, wie die Videoüberwachung, sind hingegen hoheitliche Maßnahmen.*

Diese scheinen mittlerweile in ihrer ideenreichen Gestaltung keine Grenzen zu finden: Vorratsdatenspeicherung aller Art im Internet, Onlinedurchsuchungen, Chipeinbauten, Nacktscanner, umfassende Geldtransferüberwachung[6] , Handy-Ortung auch im Stand-By-Betrieb etc. veranlassen die Politik zu Gesetzeserlassen im Schnellschussverfahren, die weder grundrechtlich austariert noch sinnvoll sind.[7]

Der EU liegen bereits *Fingerabdruckdateien*[8] vor, die sicher Ergänzungen begehren. Wer kann schon nachvollziehen, welche Datenabgleiche vollzogen werden, um bei der internationalen Bekämpfung des sogenannten Terrors einen Erfolg zu ermöglichen? Zumal die supranational angelegten Befugnisse stets weiter ausgeweitet werden (Kontodatenabgleich, Geldtransferüberwachungen). Zu Hilfe eilt bei der Erfassung persönlicher Daten die nunmehr eingeräumte Möglichkeit der *biometrischen Vollerfassung* und die Einbeziehung dieser Daten in Reisepässe, Identitätskarten und jegliche Form von Ausweispapieren (auch bei der elektronischen Gesundheitskarte). Die biometrische Datenerfassung im Reisepass sollte aufgrund der Kritik eine freiwillige bzw. wahlweise Abgabe des digitalen Fingerabdrucks enthalten. Diese Möglichkeit endet in der Behördenstarre, die nur einen Weg der Passbestellung anbietet, eben „nur mit Fingerabdruck möglich“ (so in Bremen). Über weitere Gefahren berichtet der Chaos Computer Club eingehend.[9]

Durchführung der Volkszählung zur supranationalen Vollerfassung

Derzeit zeigt sich eine weitere grundrechtsfeindliche Maßnahme, ohne wirklich in die Öffentlichkeit zu gelangen und dem Anspruch des Bürgers auf Information gerecht zu werden, in der Durchführung des *Zensus*. Die Daten der Volkszählung werden auf eine völlig neue Art erhoben. Es wird ein registergestütztes Verfahren verwendet, das das elektronische Aufnehmen aller relevanten Daten ermöglicht, die den betreffenden Behörden vorliegen. Die Datenerhebung wird durch Stichprobenverfahren und (nicht im ZensG legitimiert) auch durch den weiterhin stattfindenden Mikrozensus[10] ergänzt. Die Erhebung der sich in Deutschland befindlichen Personen (nicht nur deutsche oder angemeldete Bürger) ist damit insgesamt auch umfangreicher als in der EU-Vorgabe zunächst vorgesehen. Des Weiteren ist die verfassungsrechtlich vorgegebene Anonymisierung der Daten faktisch ungeklärt, da sich auch mit wenigen Daten noch Deanonymisierungen durchführen lassen und die Löschung direkt personenbezogener Merkmale sogar auf bis zu vier Jahre hinausgezögert werden kann. Die Durchführung wird irreführend meist auf den Stichtag im Mai 2011 datiert, die relevanten Daten werden aber bereits seit Sommer 2010 von Behörden oder anderen Auskunftspflichtigen eingezogen.[11]

Die Zusammenschau zeigt, wenn sie auch nicht annähernd abschließend die Instrumente und Gefahren darstellen kann, die Aushöhlung unseres einst fest im Handeln und Geiste verankerten Grundrechtsschutzes.

Gründe für den Übergang in postdemokratische Zeiten

Dabei weisen die meisten Maßnahmen geringe Erfolge auf. Eklatant ist die vielseitig getroffene Feststellung der schlichten *Ineffizienz*. Weisen sie doch darüber hinaus erhebliche Grundrechtseinschränkungen auf, unter anderem durch fehlende Normenklarheit, Verstöße gegen das Verhältnismäßigkeitsprinzip oder das Übermaßverbot.

Es scheint, als kämen die Verantwortlichen der Politik und damit der Gesetzgeber mit auftretenden Zeitphänomenen und den vermeintlichen Gefahren nicht mehr zurande, da sie sie schlicht nicht mehr inhaltlich und logisch durchdringen. Der heutige Politiker ist von dem aktuellen Geschehen inhaltlich generationenweit entfernt und folgt bei der Bewältigung von Krisen untauglichen alten Pfaden. Diese „*Pfadabhängigkeiten*“[12] verhindern Lerneffekte, da einmal Gelerntes in Standardverfahren wieder angewendet wird. Darüber hinaus maßt die Politik sich an, Zeitphänomene falsch zu deuten und daraus eine Sicherheitspolitik zu entwickeln, die dem eigenen Volk mehr schadet als nutzt, statt mittels fachübergreifender Netzwerke, eigenen Kompetenzausbaus und institutioneller Fantasie neue Ansichten und Wege zu finden, die auf einem Vertrauensverhältnis mit dem Volk aufbauen und verfassungskonforme Lösungen darstellen, die somit die noch vorhandene Demokratie sichern.

Denn es bleibt nach wie vor anzumahnen, dass *Grundrechte*, insbesondere Freiheitsrechte und das Recht auf ein faires Verfahren *immer wieder neu erkämpft und verteidigt* werden müssen. Sie werden nicht Demokratie-immanent zur Verfügung gestellt, wie manche glauben mögen. Nein, vielmehr sind sie die Voraussetzung einer lebendigen Demokratie, Voraussetzung für eine freie Willensbildung ohne Angst und durch die sich bildenden Kritikfähigkeit somit Grundlage eines gesunden Systems nach demokratischem Verständnis.

Dabei umfasst die Staatsform Demokratie weltweit nur einen Anteil von 50%-Anteil und zeigt sehr unterschiedliche Ausprägungen und eine geringer werdende Tendenz. In der Historie erweist sich, dass gerade ein hochtechnologisch und geisteswissenschaftlich entwickeltes Volk im Zenit seines kulturellen oder technischen Erfolges und/oder beim Aufstreben einer Elite sodann dem Untergang geweiht ist. Die Demokratie wird nicht mehr als unabdingbares Gut bedingungslos beschützt. Auch das Beispiel China zeigt, dass ein wirtschaftlich aufstrebendes Land seine Genugtuung dann in der Wirtschaft und dem höheren Lebensstandard findet und die Staatsform einer Demokratie hierzu keinesfalls benötigt. Im Gegenteil ist ein erfolgreicher Kapitalismus ohne Demokratie wahrscheinlich viel leichter möglich. In der derzeitigen Situation unserer Demokratie wird bei steigender Einflussnahme wirtschaftlicher Eliten eine (Rück-)Entwicklung in „*postdemokratische Zeiten*“[13] befürchtet.

Politikverdrossenheit, ein Irrtum

Vertrauensverlust in die Demokratie führt zu Stagnation. Sollen Politiker aber derzeit noch von Politikverdrossenheit sprechen, sollen sie sich deutlich machen, dass die politische Regung der Bevölkerung keineswegs erloschen ist. Sie hat sich nur in andere Kanäle verlagert, sie unterliegt einem völlig anderen Lebenskonzept und kommuniziert auf andere Weise und auf anderen Plattformen. Daher rührt auch die flächendeckende Divergenz der beiden Lager. Dass „WIR“ für die Politik nicht mehr „das Volk sind“ oder als mitbestimmend angesehen werden, wurde inzwischen verstanden. Es regt sich *braver, aber intelligenter Widerstand* auf die eine oder andere Weise. Soziales Engagement ehrenamtlicher Helfer versucht den sozialen Misstand aufzufangen, während an anderer Stelle verschiedenste Gruppen neue Lebensmodelle basteln und leben. Der Versuch der Politiker, das Volk emotional ausbluten zu lassen, welches sich zunehmend ehrenamtlichem Engagement widmet und dabei Nachteile in Kauf nimmt (Arbeitslosigkeit im rechtlichen Sinne, fehlende Rentenansprüche), zeigt die Hilflosigkeit und Kälte unserer Regierenden.

Andere Gruppierungen haben jedoch längst andere Wege aufgezeigt, man darf gespannt sein und mitmachen mit den nächsten „Superhelden“[14], die um die Ecke kommen.

Anmerkungen

1 *Hans-Jürgen Papier: „Verfassungsrecht“; Michael Sachs: „Verfassungsrecht II, Grundrechte“; Uwe Kranenphohl, „Wie entscheidet das Bundesverfassungsgericht?“, 2009.*
2 *Christoph Türcke: „Erregte Gesellschaft, Philosophie der Sensation“, C.H. Beck, München 2002*
3 *Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern, Antiterrordateigesetz ATDG, vom 22. Dezember 2006, in Kraft ab 2008*
4 *nur beispielhaft: Bundesverfassungsgericht, Beschluss vom 23.02.2007, 1 BvR 2368/06*
5 *http://de.wikipedia.org/wiki/Liste_der_deutschen_Urteile_zu_Video%C3%BCberwachungen*
6 *U.a. Anti-Terrorismusfinanzierungs-Richtlinie, RL 2005/60/EG*
7 *Weitere umfassende Information unter http://www.vorratsdatenspeicherung.de und http://wiki.vorratsdatenspeicherung.de/Hauptseite*
8 *EURODAC, http://de.wikipedia.org/wiki/EURODAC*
9 *www.ccc.de*
10 *https://wiki.vorratsdatenspeicherung.de/Mikrozensus#MZG_versus_Zensusgesetz*
11 *Weitere Informationen zum Zensus, bzw. zur Volkszählung finden sich unter http://zensus11.de/*
12 *Paul Pierson: „Politics in Time – History, Institutions and Social Analysis“, Princeton, 2004*
13 *Colin Crouch: „Die Schamlosen“, Spiegel 8/2009*
14 *Neue Superhelden gehen auf die Straße: http://www.swr.de/dokumentarfilm/junger-dokumentarfilm/comic-hamburg-robin-hood-romero/-/id=100850/nid=100850/did=4607030/17bdk8e/index.html*

Michael Ebeling

Die Volkszählung 2011

Den Jüngeren unter uns sagt der Begriff „Volkszählung" nicht viel. Vielen anderen fallen bei diesem Wort die großen Protestbewegungen der 1980er Jahre ein, Boykottbewegungen, Demonstrationen, Gerichtsverfahren und Hausdurchsuchungen. Doch bei der nächsten Volkszählung wird alles anders: Keine Vollbefragung mehr und (deswegen?) auch kein öffentlicher Aufschrei über die neuen staatlichen Datenerhebungen, keine Massenboykotte und keine Demonstrationen. Wird deswegen auch alles besser? Um beurteilen zu können, „ob alles besser wird", muss man zunächst wissen, worum es geht.

Gesetzliche Grundlagen

Die nächste Volkszählung heißt nicht mehr Volkszählung sondern *Zensus*. Und deswegen heißen die wesentlichen Bundesgesetze, die den Vor- und den Ablauf der Datenerhebung regeln sollen, *Zensusvorbereitungsgesetz* und *Zensusgesetz*. Der Inhalt dieser Gesetze und die Dimension der darin enthaltenen Regelungen erschließen sich nicht auf den ersten Blick, aufgrund der Komplexität und Verzweigtheit der Texte manchmal auch nicht auf den zweiten.

Kerndaten der Volkszählung 2011

Es handelt sich um eine EU-weite Volkszählung, was bedeutet, dass jedes Mitglied der Europäischen Union gemäß einer EG-Verordnung dazu verpflichtet ist, für das Jahr 2011 eine solche Erhebung durchzuführen und eine im europäischen Regelwerk definierte Art und Menge von Daten an die europäische Statistikbehörde *Eurostat* zu liefern.

Wie die einzelnen Länder zu ihren Ergebnissen gelangen, ist ihnen freigestellt, solange die Qualität und Güte der Daten gewährleistet sind. Auch den Stichtag darf jedes betroffene Land selber festlegen – für Deutschland wurde der 9. Mai 2011 zum zentralen Bezugsdatum ausgewählt, ein Montag.

Grundsätzliches zur Art der Zählung und zu ihrem Ablauf

Anders als bei den letzten Maßnahmen dieser Art in Deutschland wird nun ein „registergestützter Zensus" durchgeführt. Das bedeutet, dass nicht alle Menschen mit Fragebögen konfrontiert werden und dass es zudem unterschiedliche Formen der Befragungen gibt.

Bei der registergestützten Zählung handelt es sich um einen Zwitter zwischen einer Vollbefragung und einer Datengewinnung durch die ausschließliche Zusammenführung, Verknüpfung und Auswertung bestehender Datenbanken. So wird es sowohl Befragungen von Teilen der Bevölkerung als auch die Abfrage von Datensätzen aller Einwohner Deutschlands aus verschiedenen staatlichen Datensammlungen geben.

Wie wir später sehen werden, ist der Wechsel zu dieser für Deutschland neuartigen statistischen Erhebung mit verschiedenen datenschutzrechtlichen Bedenken verknüpft.

Warum also wird von der bisherigen Vollzählung abgewichen? Weil es billiger ist und die Menschen weniger belastet. So jedenfalls argumentieren Bundesregierung und Behörden. Kritische Stimmen vermuten vielmehr die staatliche Besorgnis, dass eine Vollerhebung ein größeres Potenzial für Boykottbewegungen bieten würde und deswegen unerwünscht sei. So wird in vielen Informationsangeboten der statistischen Behörden davon geschwärmt, dass doch nur jeder Zehnte befragt werde. Die Wahrheit sieht aber ein wenig anders aus.

Wer ist betroffen?

Jeder Einwohner Deutschland ist betroffen, weil über jeden von uns ein personenbezogener Datensatz erzeugt wird. Der Inhalt dieses Registers ergibt sich zum einen aus der Zusammenführung von Daten aus allen Meldeämtern/Bürgerbüros, von der Bundesagentur für Arbeit und von den Behörden, die für Finanz- und Personalangelegenheiten von Beamten und Leuten aus dem öffentlichen Dienst zuständig sind. Zum anderen werden bei Befragungen von Vermietern ebenfalls personenbezogene Daten erfasst, die dort einfließen.

Die Mehrzahl der deutschen Bevölkerung wird weder mit einem Fragebogen noch mit einem Volkszähler, also einem Interviewer, konfrontiert. Trotzdem wird sie datentechnisch voll erfasst und geht in die Statistik ein. Ein System, das man – sollte es mit etwaigen Hintergedanken absichtlich so eingerichtet worden sein – als genau so „entlastend" wie in seiner Wirkung perfide bewerten könnte.

Wer wird befragt?

- Alle Besitzer von Wohnungen oder Wohngebäuden sowie alle Wohnungsunternehmen (auch Wohnungsbaugenossenschaften).

- Alle Menschen, die so genannten „Sonderbereichen" zugehörig sind oder zugeordnet werden (dazu zählen z. B.: Senioren- und Studentenwohnheime, psychiatrische Anstalten und Krankenhäuser, Kliniken mit Langzeit-Patienten, als Notunterkünfte bezeichnete Schlafgelegenheiten für Obdachlose, Gefängnisse, Kasernen usw.)

- Bis zu 10% der Bevölkerung über eine stichprobenartige Befragung von Haushalten.

Für alle Fälle gilt die Auskunftspflicht (mit Ausnahme einer einzigen Frage im Haushalte-Fragebogen). Es ist somit untersagt, die einem vorgelegten Fragen nicht, nur teilweise oder absichtlich fehlerhaft zu beantworten. Für den Fall des Nichtbefolgens dieser Pflicht kann ein Bußgeld angeordnet werden, dessen Höchstgrenze auf 5.000 Euro festgelegt ist, das wahrscheinlich aber sehr viel niedriger ausfallen wird (200 bis 300 Euro?), sofern man als „einfacher Boykotteur" das Ausfüllen der Fragebögen verweigert.

Die Befragungen werden zum Teil durch per Post versendete Fragebögen durchgeführt (Gebäude- und Wohnerhebung) und zum anderen Teil durch Volkszähler (von offizieller Seite als „Interviewer" bezeichnet), die die Haushalte und die Sonderbereiche aufsuchen.

Wer im Rahmen der Haushalte-Stichprobe an der Volkszählung teilnehmen muss, bei dem meldet sich der Volkszähler zuvor briefpostalisch an. Die Befragten sind nicht dazu gezwungen, die Fragen sofort und zusammen mit dem Volkszähler zu beantworten (letzter muss auch nicht in die Wohnung gelassen werden, wenn man das nicht möchte). Die Fragebögen kann man auch selbst und in aller Ruhe ausfüllen und die Antworten anschließend per Briefpost versenden oder mit Hilfe einer bereitgestellten Software per Internetverbindung übertragen.

Zählt man die Anzahl der von den drei großen Befragten-Gruppen erfassten Menschen zusammen, so stellt man fest, dass etwa ein Drittel der Bevölkerung von den Befragungen zur Volkszählung 2011 betroffen sein werden. Tatsächlich wird sich dieser Wert aufgrund von Mengen-Überschneidungen vermutlich zwischen einem Viertel und einem Drittel bewegen. Auf jeden Fall aber deutlich mehr als die oftmals propagierten 10%.

Das Kleingedruckte

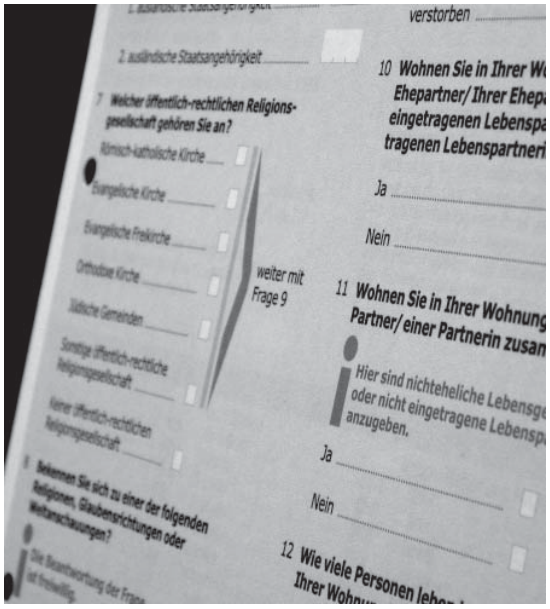
Zu dem eben Geschriebenen sind einige Einschränkungen und Ergänzungen zu machen, damit hier kein falsches Bild entsteht:

Bei den Sonderbereichen wird zwischen „sensiblen" und „nichtsensiblen" Sonderbereichen unterschieden. Zu den sensiblen Bereichen zählen Gefängnisse, psychiatrische Anstalten, Behindertenwohnheime und Notunterkünfte. Dort wird nicht jeder Betroffene direkt befragt; die notwendigen Informationen werden durch eine Zusammenarbeit mit dem Leiter des „Sonderbereichs" und dem Volkszähler ermittelt und erfasst.

Haushaltebefragungen werden hauptsächlich nur in Gemeinden mit mehr als 10.000 Einwohnern durchgeführt, weil diese die größeren Fehler in den Daten der Meldeamtsbehörden aufweisen und weil die Durchführung von Befragungen in den kleineren Kommunen mit besonderen Durchführungsschwierigkeiten behaftet wären.

Für den Fall, dass beim Abgleich der Ergebnisse der Befragungen mit den Daten aus den Behördenregistern Unstimmigkeiten auftauchen, werden in einer zweiten Welle weitere Befragungen zur deren Klärung durchgeführt. Dieses kann die Einwohner kleinerer Gemeinden genau so betreffen wie die so genannte „ergänzende Haushaltebefragung", bei der ein in seinem Umfang reduzierter Fragenkatalog zum Einsatz kommt.

Weiterhin wird es zu „Mehrfachfallprüfungen" kommen, bei denen man Unstimmigkeiten der Art nachgeht, dass eine Person an mehreren Stellen bzw. bei mehreren Meldeämtern mit seinem Hauptwohnsitz gemeldet ist.



Diese unter Umständen notwendigen Nachfragen sind durch die gewählte Methode des registergestützten Zensus zwangsläufig bedingt. Denn um ein möglichst genaues (und gerichtsfestes!) Abbild einer Gesamtheit zu erzeugen, ist es von großer Bedeutung, dass die Ergebnisse der Stichprobe hochzuverlässig sind. Darum werden alle per Befragungen eingetragenen Ergebnisse nicht anonymisiert, sondern mit Hilfe einer Ordnungsnummer personalisiert und den Auskunftsgebern zugeordnet. Laut Zensusgesetz darf diese Verknüpfung bis zu vier Jahre nach der Befragung Bestand haben.

Statistikgeheimnis und Rückspielverbot

Alle Befragungen sollen ausschließlich unter Berücksichtigung der Wahrung des statistischen Amtsgeheimnisses durchgeführt werden. Damit verbunden ist das durch das Volkszählungsurteil

vom 15.12.1983 definierte Rückspielverbot. Das bedeutet, das die Erkenntnisse, die im Rahmen der Befragungen der Volkszählung gewonnen werden, nicht als Informationen in die Meldeämter oder in andere Behörden zurückfließen dürfen. Damit soll das Vertrauen in die Anonymität der statistischen Erhebung gesichert werden. Ohne das Erlangen eines breiten Vertrauens und der damit verbundenen Qualität der Befragungsergebnisse würde eine Volkszählung wenig Nutzen bringen.

Was wird gefragt? – Welche Daten werden zusammengezogen?

Der Umfang der Befragungen ist zwar im Vergleich zur letzten westdeuschen Volkszählung von 1987 etwas geringer, in seiner Detailiertheit und seiner Ausprägung jedoch trotzdem sehr weit gehend.

In der Haushaltebefragung wird u.a. nach der Staatsangehörigkeit, dem Migrationshintergrund, nach Religion, Art der Lebenspartnerschaft, beruflichem Werdegang und Status sowie danach gefragt, ob man als Arbeitsloser ernsthaft nach neuer Arbeit sucht oder nicht.

Wohnungs- und Gebäudebesitzer müssen detaillierte Angaben zur Art und Ausstattung des Hauses bzw. der einzelnen Wohnungen machen. Fragen nach Heizungsart, dem Vorhandensein von WC oder Badewanne bzw. Dusche kommen genau so vor wie Befragungen zu Eigentumsverhältnissen, Anzahl und bis zu zwei Namen von Bewohnern und Nutzern der Wohnung.

Die vollständigen Formulare lassen sich auf den Informationsseiten des Statistischen Bundesamtes [1] einsehen.

Wann wird erhoben, befragt und gezählt?

Die zur Volkszählung in Deutschland erhobenen und zu erhebenden Daten werden sich auf den Stichtag 9. Mai 2011 beziehen. Erste Vorbefragungen für Wohnungsgesellschaften und -genossenschaften sind – abhängig vom Bundesland – bereits im August 2010 versandt worden, die Fragebögen für Wohnraumbesitzende werden ca. zwei Wochen vor dem Stichtag versandt. Die Volkszähler selber werden erst ab dem 9. Mai losziehen. Ihre Befragungen werden sich voraussichtlich über vier bis acht Wochen hinziehen. Nachbefragungen und die Klärungen von Unstimmigkeiten sollen im Herbst 2011 erfolgen und im Frühjahr 2013 soll das ganze Projekt abgeschlossen sein – so die derzeitigen offiziellen Planungen.

Mit dem Abruf von Daten wurde allerdings schon viel früher begonnen: Schon zum 1. November 2010 wurde bereits die erste von drei vollständigen Datensatzabfragen aller gemeldeten Einwohner von allen Meldeämtern Deutschlands durchgeführt. Dieser Vorgang wiederholt sich am 9. Mai und am 9. August 2011.

Und bereits von 2007 bis 2010 waren die statistischen Ämter damit beschäftigt, dem Zensusvorbereitungsgesetz Genüge zu tun und das „Anschriften- und Gebäuderegister (AGR)“ zu erstellen, in dem durch die Zusammenziehung von Daten aus einer Reihe von amtlichen Daten und öffentlichen Quellen eine vermutlich bislang einzigartige Datenbank mit allen erfassbaren Adressen, Wohnungen und Unterkunftsmöglichkeiten Deutschlands entstanden ist. Diese dient als Grundlage für die Durchführung der Befragungen von Wohnungs- und Gebäudebesitzern.

Die Umsetzung der Vorschriften

Für die praktische Durchführung sind neben dem Statistischen Bundesamt Wiesbaden die Landes-Statistikämter zuständig. Ihnen obliegt die Umsetzung der „Ausführungsgesetze“, die jedes Bundesland als Ausführungsgrundlage für die Volkszählung erlassen musste bzw. noch muss.

Im Rahmen der dort definierten Regeln werden in jedem Bundesland „Erhebungsstellen“ eingerichtet, die für ihre Kommune bzw. ihre Stadt die Organisation der Befragungen, die Schulung und Betreuung der Volkszähler sowie weitere verwaltungstechnische Aufgaben übernehmen.

Die Ausführungsgesetze sind von Bundesland zu Bundesland zum Teil sehr unterschiedlich umgesetzt worden und verlangen besondere Beachtung.

Fast alle Landesgesetze greifen die im Zensusgesetz als freiwillig angebotene Regelung an, wonach (unter Berücksichtigung einzelner Ausnahmeregelungen) theoretisch jeder Bürger zum „Ehrenamt als Volkszähler verpflichtet“ werden kann. In der Praxis wird es allerdings höchstwahrscheinlich nicht oder in nicht allzugroßem Umfang dazu kommen, weil es an Freiwilligen für eine mit steuerfreien Aufwandsentschädigungen belohnte Arbeit vermutlich nicht fehlen wird.

Volkszähler sollten nicht in der „unmittelbaren Nähe“ ihrer Wohnung eingesetzt werden, sie sind dem Statistikgeheimnis schriftlich zu verpflichten, und es wird zu beobachten sein, mit welcher Sorgfalt die Auswahl der Volkszähler und deren Arbeitsweise in der Praxis umgesetzt wird.

Auf welche weiteren Anforderungen bei der Umsetzung möglicherweise zu achten ist, wurde vom AK Zensus in einer Wiki-Seite des AK Vorrat im Rahmen einer tabellarischen Vergleichsübersicht aller Ausführungsgesetze beschrieben [2].

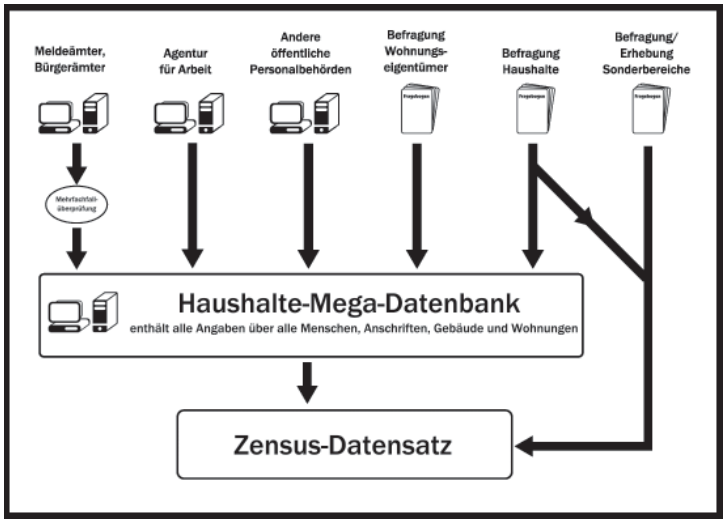
Der Sinn der Volkszählung – wofür das Ganze?

Grundsätzlich ist unbestreitbar, dass Zahlen, Daten und Informationen wichtig dafür sind, um planen, leiten, lenken und forschen zu können. Die Organisation von Infrastrukturen benötigt Zahlenmaterial: Kindergärten, Krankenhäuser, Personen- und Güterverkehr, Strom-, Wasser- und Kommunikationsleitungen müssen geplant und dimensioniert werden. In unserem derzeitigen politischen System hängen außerdem die Zuschnitte der Wahlkreise und die Höhe von Finanzausgleichszahlungen davon ab, wie viele Menschen wo leben. Und auch andere wissenschaftliche Zweige, wie beispielsweise die Sozialforschung, profitieren enorm von aktuellem und historischem Zahlenmaterial.

Dennoch bleiben angesichts realer Bundes- und Landespolitik erhebliche Bedenken, ob der Aufwand wirklich sinnvoll ist. Eine gute Zahlenbasis garantiert auf keinen Fall eine gute politische

Führung, auch wenn so in für die Volkszählung werbenden Texten immer wieder implizit argumentiert wird. Und es geht auch um viel mehr als nur die häufig simplifizierte Darstellung der Volkszählung als eine Abzählung von Menschen.

Ziel und Ergebnis soll eine möglichst fehlerfreie und lückenlose Erfassung aller Einwohner und aller Wohn- und Unterkunftsmöglichkeiten in Deutschland sein, die in eine am Merkmal *Haushalt* ausgerichteten Datenbank mündet. Aus diesem Datenpool können dann diejenigen statistischen Grunddaten erzeugt werden, die die europäische Statistikbehörde Eurostat gemäß EG-Verordnung verlangt.



Bedenken und Kritik an der Volkszählung?

Ohne eine grundsätzliche „Anti-Haltung" einnehmen zu wollen, werden von Kritikern folgende Bedenken gegen die tatsächliche Gestaltung der Volkszählung 2011 angeführt:

- *Fehlende Anonymisierung*. Durch so genannte „Ordnungsnummern" lässt sich noch bis zu vier Jahre später zurückverfolgen, welche Angaben jeder einzelne Befragte im Detail gemacht hat.

- *Zweckentfremdung von Daten*. Obwohl die Daten bei den Meldeämtern und bei der Bundesagentur für Arbeit zu ganz anderen Zwecken angegeben worden sind, werden diese Informationen nun (ohne dass man die Menschen darüber ausreichend informiert hat) der Volkszählung zugeleitet und zentral gespeichert.

- *Zwang statt Freiwilligkeit*. Einerseits wird man zwangsverpflichtet, Auskunft über sich und seine Familie zu erteilen. Bei Nichtbefolgen droht ein Bußgeld. Andererseits ist es auch möglich, dass die Anweisung erteilt wird, als „Volkszähler" arbeiten zu müssen und damit dazu beizutragen, Informationen über andere Menschen einzuholen.

- *Ungleichbehandlung von Minderheiten*. Die zwangsweise Erfassung von aller Obdachlosen, psychisch Kranken, alten Menschen und Gefängnisinsassen, die sehr weitgehenden Fragen nach Migrationshintergrund und Religionszugehörigkeit und nicht zuletzt die Befragung zur Weltanschauung wirken ausgrenzend und werden in diesem Umfang von der europäischen Richtlinie zum Teil gar nicht verlangt. Warum wird danach gefragt, welcher genauen islamischen Glaubensrichtung man angehört, wenn gleichzeitig jedoch auf eine Unterscheidung der zahlreichen christlichen Kirchen verzichtet wird?

- *Überschießende Regelungen statt Datensparsamkeit*. Statt sich auf die per EG-Verordnung zwingend geforderten Angaben zu beschränken, werden in Deutschland tiefer gehende Fragen zu dem Migrationshintergrund einer Person selbst und ihrer beiden Elternteile sowie Fragen zu Glauben, Religion und Weltanschauung gestellt.

- *Risiko von Datenskandalen*. Nur nicht vorhandene Daten sind sicher. Alles andere ist eine Illusion. Die zentrale Speicherung sensibler Persönlichkeitsdaten weckt Begehrlichkeiten und birgt die Gefahr des Datendiebstahls, der Datenverfälschungen und -manipulationen. Deren Auswirkungen können kaum hoch genug eingeschätzt werden. Zusammen mit anderen Informationen entsteht eine ausgeprägte Profilbildung von Menschen, die nur sie selber etwas angeht. Erstmalig wird in Deutschland eine zentrale Datenbank aller Wohn- und Unterkunftsmöglichkeiten erstellt, in der jeder einzelne Einwohner mit seinen Daten verknüpft wird (Anschriften- und Gebäuderegister).

- *Gefahr der Re-Identifikation anonymer Angaben*. Die nach Angaben des Statistischen Bundesamtes wertvolle „anonyme Auswertung auf kleinster Ebene" birgt bei ständig fortschreitender Mächtigkeit von IT-Systemen die steigende Gefahr von Re-Identifikationen und damit der Aufhebung nur scheinbarer Anonymität.

- *Eklatanter Mangel an aufklärender Information*. Obwohl die Pflicht zur Aufklärung der Bevölkerung im Zensusgesetz festgeschrieben und auch im Volkszählungsurteil ausdrücklich betont wurde, gab es bisher keine ernsthafte Öffentlichkeitsarbeit von Seiten der zuständigen Behörden. Das führt zu Verunsicherung und Verdruss.

- Kosten-Wahnsinn. Sprach man anfangs noch davon, dass die gesamte Volkszählung in Deutschland 315 Mio. Euro kosten würde, wird jetzt bereits von 750 Mio. Euro geredet. Zahlreiche Kommunen, Städte und Länder klagen darüber, dass die ihnen zugeteilten Gelder alles andere als kostendeckend seien. Und die Kosten, die befragten Bürgern und Wirtschaftsunternehmen entstehen, wurden in den Berechnungen gar nicht erst berücksichtigt.

- *Mangelhafte Ausführungsgesetze*. Die von jedem Bundesland in Eigenregie erlassenen Ausführungsgesetze weisen im Detail große Regelungslücken auf und lassen befürchten, dass die Umsetzung der Volkszählung zu einem operativen Desaster wird.

- *Fehlende Transparenz*. Das Zensusgesetz ist äußerst komplex und so gut wie undurchschaubar. Das Statistische Bundesamt weigert sich darüber hinaus beharrlich, Kosten für teure PR-Konzepte transparent zu machen, obwohl es sich um öffentliche Gelder handelt, die dort ausgegeben worden sind.

- *Eile statt Vernunft*. Sowohl Zensus- als auch Ausführungsgesetze wurden in großer Eile geschrieben und erlassen. Es gibt Bedenken, dass die hektische Arbeitsweise und Umsetzung der Gesetze zu fehlerhaften Rechensystemen und mangelhafter Umsetzung der Volkszählung und des gepredigten Datenschutzes führen werden.

Wie sollte man sich verhalten?

Hierfür sollten keine pauschalen Handlungsanweisungen gegeben werden.

Ich werbe dafür, dass sich jede/r eine eigene, kritische und möglichst unabhängige Meinung bilden sollte und Handeln und Verhalten an eigenen Erkenntnissen ausrichtet. Sachlich und friedlich, aber auch aktiv, stringent und beharrlich.

Es gibt wirksame Möglichkeiten des Widerstands auf juristischer wie auf praktischer Ebene. Konkrete Maßnahmen beginnen bei zivilem Ungehorsam unter Ertragung einer etwaigen Bußgeldauferlegung, über Solidaritäts-Pakte, bohrende Nachfragen bei Behörden und Beobachten der praktischen Umsetzung bis hin zum juristischen Angehen von Ausführungsgesetzen.

Diese und weitere Möglichkeiten zählen sowohl der AK Zensus [3] als auch andere Initiativen [4] auf.

Der AK Zensus

Nachdem die Volkszählung 2011 für lange Zeit kein Thema für die allermeisten Menschen gewesen ist, haben sich auf dem CCC-Kongress SIGINT in Köln im Mai 2010 einige Interessierte zum AK Zensus zusammengetan.

Organisatorisch in den Arbeitskreis Vorratsdatenspeicherung eingebettet und mit Unterstützung von FoeBuD und FIfF wurde innerhalb weniger Wochen eine Verfassungsbeschwerde gegen das Zensusgesetz erarbeitet und am letztmöglichen Tag, am 16. Juli 2010 in Karlsruhe eingereicht [5].

Leider hat das Bundesverfassungsgericht diese Beschwerde nicht zur Entscheidung angenommen, weil es einige Bedingungen dafür nicht erfüllt gesehen hat [6], womit dieser Rechtsweg nun ausgeschlossen ist.

Der AK Zensus versteht sich als zentrale Plattform für die Kritiker des *Zensus 2011* und versucht, als offene und parteiunabhängige Gruppe Aufklärung zu betreiben, Menschen zu vernetzen, Vorträge zu diesem Thema zu vermitteln, weitere juristische Vorgehen zu koordinieren und etwaige Widerstandsformen zu entwickeln.

Neben einer umfangreichen Informationssammlung zur Volkszählung [7], zu den Ausführungsgesetzen [8], den Statistikbehörden [9], zum Mikrozensus [10] und zu der Geschichte der Volkszählungen im Nationalsozialismus [11] bietet der AK Zensus auf einem eigenen Informationsportal Informationen zur Volkszählung: **www.zensus11.de**

Persönliches Fazit

Zwar ist allen im AK Zensus Engagierten klar, das die Volkszählung 2011 nicht *das* große Thema für bürger- und datenschutzrechtlich ausgerichtete Menschen ist und sein wird – entsprechend halbherzig wird der Zensus 2011 in der Medienöffentlichkeit antizipiert – und die Nicht-Annahme der Verfassungsbeschwerde war für alle Beteiligten ein herber Rückschlag. Trotzdem halte ich die sachlich-kritische Auseinandersetzung für unerlässlich und die kritische Begleitung der Umsetzung sowie eine starke Aufklärungsarbeit für enorm wichtig.

Dabei sollte stets zwischen den ausführenden statistischen Ämtern und den Urhebern der Zensusgesetze unterschieden und nie vergessen werden, dass wir uns mit aller Kritik und bei allem „Nachbohren“ nicht gegen die ausführenden Menschen in den Ämtern und Behörden richten, sondern gegen die im Zensusgesetz manifestierten Regeln und die zugrunde liegenden Absichten der Gesetzgeber.

Anmerkungen

[1] http://www.zensus2011.de

[2] http://wiki.vorratsdatenspeicherung.de/images/Vergleich_ausf%C3%BChrungsgesetze.pdf

[3] http://www.zensus11.de

[4] http://vobo11.de

[5] http://www.vorratsdatenspeicherung.de/content/view/373/135/lang,de/

[6] http://www.bundesverfassungsgericht.de/entscheidungen/rk20100921_1bvr186510.html

[7] http://wiki.vorratsdatenspeicherung.de/Volkszählung

[8] http://wiki.vorratsdatenspeicherung.de/Ausfuehrungsgesetze

[9] http://wiki.vorratsdatenspeicherung.de/Volkszaehlung-Statistikbehoerden-Fragen

[10] http://wiki.vorratsdatenspeicherung.de/Mikrozensus

[11] http://wiki.vorratsdatenspeicherung.de/NS-Volkszaehlung

Michael Ebeling

Michael Ebeling, 40 Jahre alt, ist Diplom-Ingenieur aus Hannover und engagiert sich im AK Vorrat und im AK Zensus.

Thilo Weichert

Zensus 2011 und der Datenschutz – eine unendliche Geschichte?

Die Volkszählung 2011 heißt offiziell nicht „Volkszählung", sondern Zensus. Der ursprüngliche deutsche Begriff ist belastet mit Assoziationen zum Widerstand der damals bundesrepublikanischen Bevölkerung gegen die Zählungen in den 1980er Jahren – geplant und gescheitert 1983, mit mäßigem Erfolg durchgeführt 1987. Weiter assoziiert ist der Begriff mit dem berühmten Urteil des Bundesverfassungsgerichtes (BVerfG) 1983, mit dem das Recht auf informationelle Selbstbestimmung, kurz das Grundrecht auf Datenschutz, aus der Taufe gehoben wurde. Dieser Sieg einer außerparlamentarischen Bürgerbewegung und des Datenschutzanliegens war mit einer Niederlage der etablierten Politik und der Statistiker verbunden. Mit dem Begriff „Zensus" soll die Erinnerung hieran umgangen werden.

Dennoch: Beim Zensus 2011 wurde von den Volkszählungen aus den 80ern gelernt. Waren Verfassungsbeschwerden gegen den damaligen Zensus nicht nur erfolgreich, sondern für die weitere juristische und öffentliche Diskussion zum Datenschutz stilbildend, so erhofften sich Gegner des heutigen Zensus vergeblich Entsprechendes: Eine Verfassungsbeschwerde wurde zwar von 13.000 Personen unterstützt, aber mit Beschluss vom 21.09.2010 vom höchsten deutschen Gericht nicht einmal zur Entscheidung angenommen. Die „undifferenzierte" Nennung der Zensusgesetz-Regelungen und der möglicherweise betroffenen Grundrechte reiche, so das BVerfG, angesichts des „umfangreichen und detaillierten Regelungsgehaltes für eine hinreichende Bezeichnung des angegriffenen Hoheitsakts nicht aus".

Selbst wenn die Beschwerdeschrift detaillierter gewesen wäre, hätte sie wohl beim BVerfG keinen Erfolg gehabt. Denn die Statistiker von Bund und Ländern haben aus der Schlappe in den 1980ern gelernt und viele Fehler vermieden, nicht nur den Fehler einer arroganten und autoritären Öffentlichkeitsarbeit, sondern auch die vielen rechtlichen und technischen Fehler, die zum juristischen Scheitern beitrugen: Es erfolgt keine Vollerhebung der Bevölkerung, sondern nur eine 10%-Stichprobe, gekoppelt mit mehreren Registerzählungen aus den Meldebehörden, der Bundesagentur für Arbeit, sowie aus der Personal- und Finanzverwaltung sowie eine Befragung sämtlicher Gebäude- und Wohnungseigentümer.

Zentral für die verfassungsrechtliche Beurteilung ist weiter, dass die Daten streng dem Statistikgeheimnis unterliegen sollen, also auch nicht über Umwege an den Verwaltungsvollzug zurückfließen dürfen. Die technischen und organisatorischen Abschottungen bei den Erhebungsstellen und in den Statistikämtern sollen auch ein ungeplantes Abfließen oder Herauslecken der Daten verhindern. So soll beispielsweise sichergestellt werden, dass bei den 80.000 Erhebungsbeauftragten keine Polizisten, Sozialarbeiter oder sonstige Personen eingesetzt werden, bei denen es zu Interessenkonflikten kommen könnte.

Für die von der Stichprobe und der Eigentümererfassung betroffenen Menschen ändert sich gegenüber der alten Volkszählung insofern nichts, als sie auskunftspflichtig sind und diese Pflicht per Buß- und Zwangsgeld durchgesetzt werden kann. Unbestreitbar ist weiterhin, dass die erbetenen Auskünfte teilweise sehr sensibel sind, etwa die zur Religionszugehörigkeit oder zum Migrationshintergrund. Die Frage nach dem religiösen Bekenntnis ist jedoch freiwillig; hierauf wird ausdrücklich hingewiesen.

Wenn nun BVerfG und Datenschutzbeauftragte keine grundsätzlichen Bedenken haben, so bedeutet dies nicht, dass der Zensus unproblematisch wäre. Bei der konkreten Umsetzung kann vieles falsch gemacht werden, insbesondere bei den Erhebungsbeauftragten und den kommunalen Erhebungsstellen. Aber auch beim Registerabgleich kann es zu Fehlern kommen. Bürgerrechtsbewegte werden – schon aus Nostalgie – die Durchführung des Zensus mit Argusaugen beobachten. Und das ist auch gut so, weil diese zwangsweise Sammlung sensibler Daten auch im neuen Gewand zum Missbrauch einlädt.

Spätestens seit *Stuttgart 21* stellt sich für die Bevölkerung verstärkt die Frage: Was kostet uns das als Steuerzahler? Der Zensus ist mit voraussichtlichen Kosten von über 0,7 Mrd. Euro nicht gerade billig. Zweifellos gibt es eine europäische Verpflichtung zum Zensus. Deren Sinn kann man aber angesichts des Umstandes hinterfragen, dass statistische Daten zunehmend auch anderweit verfügbar sind. Aus Datenschützersicht jedenfalls wäre es zu wünschen, dass es sich beim Zensus um eine endliche Geschichte handelt.

Thilo Weichert

Dr. **Thilo Weichert** ist Landesbeauftragter für Datenschutz Schleswig-Holstein und Leiter des Unabhängigen Landeszentrums für Datenschutz, Kiel.

Werner Hülsmann

Ein kurzer Auszug aus der Geschichte der Volkszählung

Die Volkszählung im national-sozialistischen Unrechtsregime

„Es begab sich aber zu der Zeit, dass ein Gebot von dem Kaiser Augustus ausging, dass alle Welt geschätzt würde. Und diese Schätzung war die aller erste und geschah zur Zeit, da Quirinius Statthalter in Syrien war. Und jedermann ging, dass er sich schätzen ließe, ein jeder in seine Stadt." (Lukasevangelium 2, 1-14)

Diese aus der biblischen Weihnachtsgeschichte bekannte Volkszählung hat mit den späteren Volkszählungen zu statistischen Zwecken gar nichts zu tun. Denn die Schätzung des Kaiser Augustus diente in erster Linie dem Zweck, Steuern für das römische Reich einzutreiben. Die erste anhand von Tonscherben belegbare Volkzählung fand etwa 3800 v. Chr. im antiken Babylon statt. Im Römischen Reich fanden seit dem 6. Jahrhundert vor Christus alle fünf Jahre Volkszählungen für die römischen BürgerInnen statt.

Die zwischen 1834 und 1867 vom Deutschen Zollverein alle drei Jahre durchgeführten Volkszählungen in den Mitgliedsländern dienten dazu, die Einnahmen des Zollvereins im Verhältnis zur Einwohnerzahl zu verteilen. Im Deutschen Reich fanden Volkszählungen 1871 und zwischen 1875 und 1910 im fünfjährigen Turnus statt. Danach wurde kriegsbedingt nur noch in unregelmäßigen Abständen gezählt. So gab es Zählungen 1916 und 1917 zum Zweck der Lebensmittelverteilung, 1919 und 1925 wurden wieder reguläre Volkszählungen durchgeführt.[1]

Die Volkszählungen in der NS-Zeit

„Bedeutende Statistiken während des ‚Dritten Reiches' waren insbesondere die beiden Volkszählungen – 1933 kurz nach der Machtübernahme der Nationalsozialisten und 1939 kurz vor Ausbruch des Zweiten Weltkrieges"[2]

Die Volkszählungen 1933 und 1939 waren gleichzeitig Volks-, Berufs- und Betriebszählungen und wurden wie die von 1925 von dem Bevölkerungswissenschaftler *Friedrich Burgdörfer* geleitet. Mit diesen Volkszählungen hat das nationalsozialistische Deutschland vorgeführt, wozu Volkszählungen missbraucht werden können, wohin die Reduktion von Menschen auf eine Summe von Zahlen, Daten und Ordnungsnummern führt. Die Wissenschaft der Statistik erlebte während des Nationalsozialismus eine ungeahnte Förderung von politischer Seite. Dabei ist zu bemerken, dass der Missbrauch der Statistik durch entsprechende Gesetzesänderungen legalisiert wurde, der Bruch des Statistikgeheimnisses kein Gesetzesverstoß mehr war.

Zusammen mit dem von den Nationalsozialisten eingeführten Arbeitsbuch (1935), dem Gesundheitsstammbuch (1936), der Meldepflicht (1938), der Volkskartei (1939) und zuletzt der Personenkennziffer (1944) waren die Ergebnisse der Volkszählung sowie ihre konsequent sachlich wissenschaftliche Auswertung die bürokratischen Voraussetzungen für ein abgestuftes System von Lohn und Strafe, für „Auslese" und „Ausmerze". Deportationen erfolgten nicht willkürlich, sondern fein differenziert und organisiert – eben mit „deutscher Gründlichkeit". So waren die statistischen Ämter, die Kirchen- und Gemeindeverzeichnisse die allerersten Ziele der deutschen Invasions- und Besatzertruppen. Daran zeigt sich, dass einmal vorhandene, aus gänzlich anderen Gründen gesammelte Daten und Informationen zweckentfremdet werden und höchst gefährlich sein können.

„Die Ergebnisse beider Volkszählungen bildeten die wichtigste Voraussetzung zur Festlegung der zur späteren Deportation vorgesehenen Bevölkerung. Bereits in der Zählung vom 16. Juni 1933 wurden etwa eine halbe Million „Glaubensjuden" erfasst. Mit der Zählung 1939 wurde für alle Juden, „Mischlinge" und Ausländer eine „Ergänzungskarte" ausgefüllt, die als Grundlage für die Reichskartei der Juden und „jüdischen Mischlinge" im Sinne der NS-Rassengesetzgebung diente. Diese enthielt Namen, Geburtsnamen, Wohnung, Geschlecht, Geburtstag, Religion, Muttersprache, Volkszugehörigkeit, Beruf und Kinderzahl unter 14 Jahren des jeweiligen Haushalts."[3]

Nachforschungen haben gezeigt, dass diejenigen Menschen jüdischen Glaubens die besten Überlebenschancen hatten, die der Erfassung der Volkszählungen aus den 1930er Jahren entgangen waren. In einer vom statistischen Bundesamt beauftragten Studie wird festgestellt:

„Grundsätzlich machte der Präsident des Statistischen Reichsamtes gegen die Auswertung der Ergänzungskarten der Juden jedoch keine Bedenken geltend, zögerte sie aber hinaus. Er wolle ‚rechtzeitig Vorschläge machen', wie und wann den Gemeinden ‚die Abstammungsangaben der Zählung für die Volkskartei zur Verfügung gestellt werden können.' Und er bat in seinem Schreiben, das er auch den Statistischen Landesämtern zur Kenntnis brachte, darum, ‚auf die Möglichkeit der späteren Verwendung der Ergänzungskarten für Zwecke der Gemeinden vorerst öffentlich noch nicht hinzuweisen, da sonst der Zweck der Abgabe im verschlossenen Umschlage hinfällig würde.' Damit war allen mit der

Volkszählung befassten leitenden Statistikern bekannt, dass die Ergänzungskarten auch zur vollständigen Erfassung von Juden und jüdischen „Mischlingen" bei den Meldebehörden herangezogen werden sollten."[4]

Volkszählungen in den beiden Deutschen Staaten

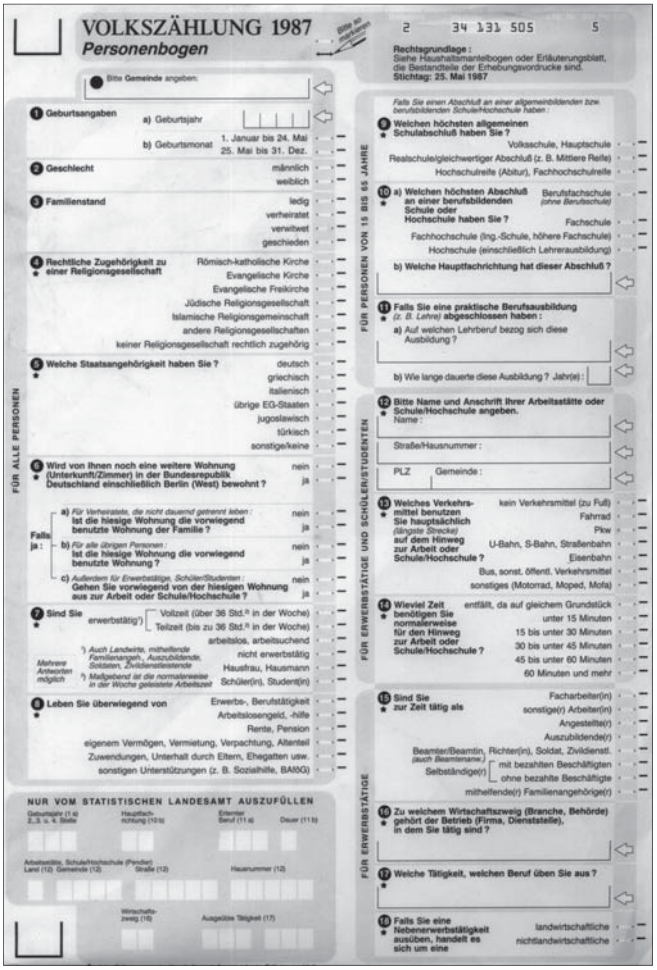
Das Statistische Bundesamt als Nachfolger des Reichsstatistikamts

Trotz seiner unrühmlichen Vergangenheit in der NS-Zeit durfte *Siegfried Koller* von 1953 bis 1962 als Leiter der Abteilung Bevölkerungs- und Kulturstatistik am Aufbau des Statistischen Bundesamts wesentlich mitwirken. So lieferte er als Sozialmediziner und Biostatistiker im „Dritten Reich" u.a. scheinwissenschaftliche Begründungen für die von den Nazis begangenen Verbrechen wie Mord, Zwangssterilisation und Eheverbot und war maßgeblich an Begriffsbildungen wie „Arbeitsscheuer" und „Gemeinschaftsunfähiger" und deren statistischer Behandlung beteiligt[5]. Koller war es auch, der 1957 den „Mikrozensus" in Westdeutschland einführte und die Volkszählung 1961 vorbereitete.

In der Bundesrepublik wurden 1950 und 1987 Volks-, Berufs-, Gebäude-, Wohnungs- und Arbeitsstättenzählungen sowie 1961 und 1970 Volks-, Berufs- und Arbeitsstättenzählungen durchgeführt. Ergänzend gab es während der Gebäude- und Wohnungszählung von 1956 eine Wohnbevölkerungszählung („kleine Volkszählung"). Die 1987 durchgeführte Volkszählung war ursprünglich für 1983 geplant. Durch eine Verfassungsbeschwerde wurde die Volkszählung vom Bundesverfassungsgericht zuerst ausgesetzt und dann durch Nichtigerklärung des zugrundeliegenden Volkszählungsgesetzes im sogenannten *Volkszählungsurteil* gekippt. Erst Jahre später ist es dem Gesetzgeber gelungen, ein neues Volkszählungsgesetz vorzulegen und dann 1987 die Volkszählung durchzuführen. Im Volkszählungsurteil hat das Bundesverfassungsgericht am 15.12.1983 das *Recht auf informationelle Selbstbestimmung* begründet.

Volkszählungsboykott 1987

Gegen die Volkszählung 1987 hatte sich – wie bereits 1983 – ein breiter Widerstand gebildet. Anders als 1983 wurde das Volkszählungsgesetz 1987 nicht vor dem Bundesverfassungsgericht angegriffen. Überall bildeten sich Volkszählungs-Boykottinitiativen (VoBo-Inis), die u.a. auch von FIfF-Mitgliedern kräftig unterstützt wurden. Es wurde zu unterschiedlichsten Protestformen aufgerufen. Diese reichten von der Verweigerung, den Bogen auszufüllen über den Widerspruch gegen die Auskunftserteilung (mit gleichzeitiger Beantragung der Wiederherstellung der aufschiebenden Wirkung vor dem Verwaltungsgericht), Ausfüllen mit Kugelschreiber statt Bleistift (verhinderte damals die Maschinenlesbarkeit), Beantwortung der Fragen in Erzählform statt auf den Bogen, falschen Angaben bis hin zu alternativen Sammelstellen, die die leeren Bögen sammelten und nach Entfernen der Ordnungsnummern auf den Bögen auf Wäscheleinen, Wänden etc. präsentierten. Inwieweit der Protest zu einer deutlichen Verschlechterung der statistischen Ergebnisse geführt hat, ist wissenschaftlich nicht endgültig entschieden. Tatsache ist aber, dass die Maueröffnung 1989, die Wiedervereinigung


VOLKSZÄHLUNG 1987
Personenbogen

Quelle: http://de.wikipedia.org/w/index.php?title=Datei:Volkszaehlung.JPG

Werner Hülsmann

Werner Hülsmann, Dipl. Informatiker, selbstständiger Datenschutzberater und Datenschutzsachverständiger, Konstanz, Beiratsmitglied des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V., ist im AK Zensus aktiv.

1990 und die damit verbundenen „Völkerwanderungen“ zwischen den beiden deutschen Staaten bzw. den alten und neuen Bundesländern dazu geführt haben, dass die 1987 erhobenen und bis 1989 ausgewerteten Daten mit der Wirklichkeit nicht mehr übereinstimmten.

1950 und 1964 erfolgten in der DDR Volks- und Berufszählungen. Allerdings wurden die Ergebnisse von 1950 aus politischen Gründen nicht veröffentlicht. Die Ergebnisse von 1964 wurden von der Staatlichen Zentralverwaltung für Statistik umfassend veröffentlich. 1971 und 1981 fanden in der DDR Volks-, Berufs-, Wohnraum- und Gebäudezählungen statt, deren Ergebnisse nur in Teilen veröffentlicht wurden

Volkszählungen nach 1990

Eigentlich wäre 1997 eine Volkszählung im wiedervereinten Deutschland fällig gewesen. Diese wurde allerdings nicht durchgeführt. Das hatte verschiedene Gründe. Zum einen schreckten die enormen Kosten die Politiker ab, und zum anderen war es offensichtlich, dass sich die Politik mit einer Volkszählung der bisherigen Art bei der Bevölkerung nicht gerade beliebt machen würde.

Aufgrund einer EG-Richtlinie ist die nächste Volkszählung mit Stichtag 9. Mai 2011 bereits beschlossene Sache und auch im vollen Gange. Mehr Informationen hierzu im Artikel von Michael Ebeling (ab Seite 28).

Anmerkungen

1 vgl. http://de.wikipedia.org/wiki/Volksz%C3%A4hlung
2 http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Navigation/Service/UeberUns/Geschichte
3 http://de.wikipedia.org/wiki/Volksz%C3%A4hlung
4 M. A. Jutta Wietog: Bevölkerungsstatistik im Dritten Reich in: Wirtschaft und Statistik Heft 7/2001, S.593
5 vgl. http://de.wikipedia.org/wiki/Siegfried_Koller)

Herbert Kubicek

Auf dem falschen Pfad

Warum der neue Personalausweis das Internet nicht sicherer machen kann – Schlussfolgerungen aus einer internationalen Vergleichsstudie

Seit dem 1. November 2010 wird in Deutschland ein neuer, elektronischer Personalausweis ausgestellt. Er hat die Größe einer Kreditkarte und ist mit einem RFID-Chip ausgestattet, auf dem auf Antrag digitale Fingerabdrücke und eine digitale Signatur gespeichert werden können. Darüber hinaus ermöglicht er einen so genannten elektronischen Identitätsnachweis (eIDN), mit dem Transaktionen im Internet sicherer werden sollen, indem eine auf dem Chip gespeicherte elektronische Identität auf technisch sichere Art überprüft werden kann. Andere europäische Länder haben bereits früher solche elektronischen Identitäten (eIDs) zum Zwecke der Online-Authentisierung eingeführt. Die Nutzung ist dort weit hinter den Erwartungen zurückgeblieben. Der deutsche eIDN beansprucht, im Hinblick auf Sicherheit, Datenschutz und Komfort besser zu sein als die anderen Lösungen. Trifft dies zu und wird es von den Anbietern und Nutzern auch honoriert? Ein kürzlich abgeschlossener Vergleich der eID-Einführung in sieben anderen europäischen Ländern lässt einige begründete Antworten auf diese Fragen zu.

Ein beträchtlicher Teil der Internetnutzer zögert noch, Waren online zu bestellen oder Verwaltungsvorgänge elektronisch abzuwickeln, weil das Netz als nicht sicher genug angesehen wird. Meldungen über das Ausspähen persönlicher Daten inklusive Kontonummer und Passwörter, den so genannten Identitätsdiebstahl, verstärken diese Bedenken. Als ein Schwachpunkt gelten die derzeitigen Verfahren der Identifizierung bei Online-Transaktionen, die so genannte Authentisierung, in Form der Eingabe von Benutzername und Passwort. Höhere Sicherheit bieten Verfahren, in denen zwei voneinander getrennte Komponenten, in der Regel Besitz eines Mediums, wie z. B. einer Chipkarte, und Wissen, in der Regel eine PIN, zusammen eingesetzt werden müssen. Im Falle landesweiter staatlich legitimierter eIDN enthält der Chip Daten, die die Identität einer Person eindeutig und verlässlich definieren und in der Regel aus den nationalen Melderegistern stammen. Die Chipkarten werden von staatlichen oder staatlich autorisierten Stellen herausgegeben. Die Überprüfung der Echtheit der eID-Daten durch die Dienstanbieter erfolgt ebenfalls bei staatlichen oder staatlich autorisierten Zertifizierungsstellen.

Die Regierungen der EU-Mitgliedstaaten hatten sich schon 2005 darauf verständigt, solche sichereren eIDN in ihren Ländern bis 2010 einzuführen, die auch den Datenschutz respektieren und den Nutzungskomfort maximieren. In Deutschland wurde wie in einigen anderen, aber keineswegs allen EU-Ländern ein solcher eIDN auf dem neuen Personalausweis implementiert und mit dem „Gesetz über Personalausweise und den elektronischen Identitätsnachweis“ vom 18. Juni 2009 gesetzlich geregelt. Danach kann seit dem 1. November 2010 jeder deutsche Staatsbürger ab 16 Jahren bei der Beantragung des neuen Personalausweises wählen, ob die eID-Funktion freigeschaltet werden soll oder nicht. Um diese Funktion nutzen zu können, muss man einen RFID-Kartenleser an den eigenen Rechner anschließen sowie einen so genannten Bürger-Client in den Internet-Browser integrieren.

Anbieter von Online-Diensten, die eine eID-basierte Authentisierung anbieten wollen, müssen beim Bundesverwaltungsamt eine Zugriffsberechtigung auf die für ihren jeweiligen Dienst erforderlichen ID-Daten beantragen und ein darauf bezogenes Berechtigungszertifikat bei einem akkreditierten Zertifizierungs-

Dienstanbieter erwerben. Und sie müssen entweder eID-Middleware auf ihren Servern installieren oder einen Vertrag mit einem eID-Provider schließen. Für die Berechtigungszertifikate ist eine einmalige Gebühr von 1.000 Euro zu entrichten sowie laufend 2.500 Euro pro Jahr für das Zertifikat für den ersten angebotenen Dienst und 500 Euro pro Jahr für jeden weiteren Dienst. Wenn man keinen eigenen eID-Server einsetzt, sondern diesen Dienst von einem eID-Provider bezieht und in das eigene Online-Angebot integriert, kostet dies neben der einmaligen Anpassung des CMS oder Shop-Systems ca. 5.000 Euro pro Jahr.

Damit zur Ausgabe der neuen Ausweise entsprechende Angebote existieren und funktionieren, hatte das BMI einen betreuten Anwendungstest mit rund 30 Unternehmen unterstützt. Von den für den Startzeitpunkt erhofften 1.000 bis 1.500 ausgegebenen Zertifikaten war man im September 2010 nach einem Bericht von heise online vom 15. 9. 2010 allerdings noch weit entfernt. Anfang November 2010 waren auf der Web-Seite zum Personalausweis knapp 30 ausgegebene Zertifikate angegeben *(http://www.personalausweisportal.de/cln_102/sid_9A870429C6C3FE2E754A7D48EFE82A8D/DE/Neue-Moeglichkeiten/neue-moeglichkeiten_node.html).* Es gab am 1. November jedoch nicht ein einziges nutzbares Angebot.

Sind das die üblichen Anlaufprobleme von Innovationen oder wird der eIDN ein ähnliches Schicksal erleiden wie die elektronischen Signaturen? Werden die höhere Sicherheit und die datenschutzfreundliche Gestaltung von den Verbrauchern honoriert oder setzen sie ganz andere Prioritäten? Über solche Fragen kann man zu Beginn von grundlegenden Innovationen zumeist nur spekulieren. Weil andere EU-Länder jedoch bereits früher mit der Einführung von eIDs begonnen und dabei unterschiedliche Wege beschritten haben, kann man in diesem Fall aus den dortigen Erfahrungen Schlussfolgerungen für die wahrscheinliche Entwicklung in Deutschland ziehen.

Das Institut für Informationsmanagement Bremen (ifib, *www.ifib.de*) hat die Einführungsprozesse nationaler eID-Management-Systeme (eIDMS) in Belgien, Dänemark, Deutschland, Estland, Finnland, Österreich, Spanien und Schweden untersucht. Ein eIDMS umfasst nicht nur die technischen Komponenten für den eIDN auf Seiten der Nutzer und Dienstanbieter, sondern auch die Institutionen und Prozesse der Registrierung, der Distribution und des Supports. Diese Forschung wurde von der VolkswagenStiftung im Rahmen des Förderprogramms „Innovationsprozesse in Wirtschaft und Gesellschaft" finanziell gefördert. Der Schwerpunkt der in Kooperation mit jeweils nationalen Partnern durchgeführten Untersuchung lag auf der Entstehung dieser Systeme und des Einflusses unterschiedlicher Akteure auf das letztlich eingeführte System. Die Forschungsergebnisse wurden zunächst veröffentlicht in einer Special Issue der Online-Zeitschrift „Identity in the Information Society" in Form von acht Länderfallstudien der jeweiligen Forschungspartner sowie einer Einführung und ersten Vergleichen in englischer Sprache *(http://www.springer.com/computer/journal/12394)*. Im November 2010 ist eine Zusammenfassung der Länderberichte mit ausführlichen vergleichenden Analysen in deutscher Sprache erschienen (Kubicek/Noack 2010).

Große technische und organisatorische Unterschiede

Die acht untersuchten eIDMS unterscheiden sich in nahezu jeder denkbaren Hinsicht. Dies beginnt bei dem Trägermedium, dem so genannten Token, und geht bis hin zu den Herausgeberinstitutionen. In Dänemark gibt es nur Softwarezertifikate, in Schweden kann man zwischen einer eID auf einer Chipkarte und einem Softwarezertifikat wählen, Belgien, Spanien und Estland haben Chipkarten mit kontaktbehafteten Chips gewählt, Deutschland hat sich am elektronischen Reisepass orientiert und einen RFID-Chip gewählt. Österreich verfolgt für die virtuelle Bürgerkarte eine Multi-Karten-Strategie. Sie kann alternativ auf die Sozialversicherungskarte (e-card) oder Bankkarten heruntergeladen werden. In Schweden wird die staatliche eID komplett von lizensierten Banken auf ihren Chipkarten herausgegeben. Daraus folgt: Alle eID-Systeme enthalten einen elektronischen Identitätsnachweis und eine elektronische Signatur. Aber nur in einigen Ländern kann das Trägermedium auch als nationales Ausweisdokument und Reisedokument dienen. In Österreich und Schweden geht das schon deswegen nicht, weil auf der Chipkarte kein Foto aufgedruckt ist (Abbildung 1).

Abb. 1: Trägermedien für eIDs und deren Funktionen in vier Ländern

Die Wahl des Trägermediums hat weit reichende Folgen. Wenn man einen Personalausweis mit einer zehnjährigen Gültigkeit wählt, dauert es auch zehn Jahre, bis jeder Berechtigte oder Verpflichtete ein solches Token besitzt und im Internet einsetzen kann - ein relativ langer Zeitraum, um Transaktionen im Internet sicherer zu machen und Vorbehalte abzubauen. Wahrscheinlich ist es auch etwas anmaßend zu glauben, man könne heute Tools und Verfahren bereitstellen, die auch in zehn Jahren noch Transaktionen im Internet sicherer machen. Wählt man hingegen eine Sozialversicherungskarte oder eine Bankkarte als Trägermedium, so kann ein kompletter Austausch gegen eine neue Version mit eID innerhalb der deutlich kürzeren Gültigkeitsdauer oder sogar innerhalb eines Jahres erfolgen.

Das Beispiel Österreich zeigt allerdings, dass diese theoretische Möglichkeit nicht automatisch von den Berechtigten genutzt wird. Jeder Österreicher muss von Geburt an eine e-card erwerben und kann sich ab dem Alter von 14 Jahren darauf unentgeltlich eine virtuelle Bürgerkarte laden. Aber nur ein Prozent hat von dieser Option Gebrauch gemacht (Aichholzer/Strauss 2010).

Um die Akzeptanz der eIDs zu vergleichen, kann man zum einen den Aktivierungsgrad betrachten und zum anderen die Nutzung bei bestimmten Transaktionen. Außer in Spanien gibt es in den betrachteten Ländern entweder eine Opt-In- oder eine Opt-Out-Lösung für die eID. In Belgien haben 80 % der Erwerber eines neuen Personalausweises die eID-Funktion aktiviert, in Estland 50%, in Finnland nur 1%. Dies hängt u. a. mit den Kosten zusammen. In Belgien kostet die Zusatzfunktion nichts und auch den Verzeichnisdienst für die elektronische Signatur finanziert der Staat. In Finnland muss dafür zusätzlich bezahlt werden. Entscheidend dürfte letztlich der erzielbare Nutzen aus Sicht der Bürgerinnen und Bürger sein.

Wem nutzt die eID?

Als Nutzen durch den Einsatz einer eID gegenüber der bisherigen Authentisierung durch Benutzername und Passwort werden die höhere Sicherheit gegen Identitätsdiebstahl und der Komfort genannt, der dadurch entsteht, dass man sich für alle Transaktionen im E-Government und E-Commerce nur noch die eine PIN für den eIDN merken müsse. Diese in der Marketingliteratur als Nutzenversprechen (value proposition) bezeichneten Effekte können die Herausgeber der eIDs jedoch nicht einlösen, da sie die Anbieter von Online-Transaktionen nicht verpflichten können, die bisherigen, weniger sicheren Verfahren der Authentisierung gegen das eID-basierte Verfahren auszutauschen. Dagegen spricht die lange Roll-Out-Zeit, wenn der Personalausweis als Token eingesetzt wird. Dann muss der Dienstanbieter die alten Verfahren so lange weiter anbieten. Auch in den Ländern wie Belgien, in denen die eID durch Regierungsbeschluss ausdrücklich zur Verbesserung der Sicherheit im E-Government eingeführt worden ist, ist es nicht gelungen, eine nennenswert große Zahl von E-Government-Dienstleistungen online anzubieten, die man bisher aus Sicherheitsgründen nicht anbieten konnte. Eine Ausnahme ist Estland, wo man nur mit der eID auf dem Personalausweis am i-voting auf lokaler und nationaler Ebene teilnehmen kann (Martens 2010).

Die strukturelle Bruchstelle sind die zersplitterten Zuständigkeiten für E-Government. In allen betrachteten Ländern haben Stellen innerhalb der nationalen Regierung die eID-Funktionalität, die Trägermedien und den gesamten institutionellen Rahmen bestimmt. Die Kommunen, die die überwiegende Mehrzahl von Verwaltungsleistungen für Bürgerinnen und Bürger anbieten, wurden daran kaum beteiligt. Sie können aber nicht zu bestimmten Authentisierungsverfahren gezwungen werden. Und selbst auf der nationalen Ebene wird die ID von den übrigen Regierungsstellen keineswegs als Authentisierungsverfahren bevorzugt (ausführlicher Kubicek/Noack 2010, S. 204 ff. und 314 ff.). Dies kann man gut an der Authentisierung für elektronische Steuererklärungen erkennen: Die eID-basierte Authentisierung erreicht nur einen Anteil zwischen 0,2 und 24,4 % (Tabelle 1).

Eine bemerkenswerte Erkenntnis aus diesem Vergleich besteht darin, dass diese Unterschiede nicht mit unterschiedlichen Sicherheitgraden der Authentisierungsverfahren erklärt werden können, sondern dass sogar das Gegenteil der Fall ist. Die Stärke von Authentisierungsverfahren wird, wie eingangs erwähnt, nach der Anzahl der erforderlichen Komponenten beurteilt. Das EU-Projekt STORK hat aufbauend auf früheren Konzepten der OECD eine Unterscheidung von vier Vergewisserungsstufen (Authentication Assurance Level) entwickelt, die von Eigenschaften der Registrierung und der Vergabe der eID einerseits sowie Eigenschaften der Authentisierungsprozesse andererseits abhängen. Verfahren, die bei der Registrierung auf einer Überprüfung von Person und Lichtbild sowie eines amtlichen Dokuments beruhen, haben einen höheren Vergewisserungsgrad als solche, wo man sich mit Angabe von Name, Geburtsdatum und Postleitzahl ein Zertifikat herunterladen kann, wie dies in Dänemark der Fall ist. Wenn bei der Authentisierung eine Karte und eine PIN erforderlich sind, ist die Vergewisserung höher als bei Softwarezertifikaten. Danach erreichen sechs der acht Länder die Vergewisserungsstufe 4, Schweden die Stufe 3 und Dänemark nur die Stufe 2.

2009	**BE** BelPIC	**ES** DNIe	**AT** Bürgerkarte	**DK** OCES	**FI** FINEID	**SE** Bank-ID u. a.	**EE** ID-Card
Nutzung elektron. Steuererklärung (% aller Erklärungen)	56%	21%	25,7%	87%	Keine Angaben	53%	87%
eID-Nutzung (% der elektron. Erklärungen)	14,2%	0,2%	1,0%	18,8%	Geschätzt 1%	24,4%	ca. 14%
Rangplatz Nutzung 2009	**3**	**7**	**5**	**2**	**5**	**1**	**3**

*Tabelle 1: eID-Authentisierung bei Online-Steuererklärungen in sieben Ländern (*Belgien, Spanien, Österreich, Dänemark, Finnland, Schweden und Estland*)*

2009	BE BelPIC	ES DNIe	AT Bürgerkarte	DK OCES	FI FINEID	SE Bank-ID u. a.	EE ID-Card
Stärke der Authentisierung (Vergewisserungsgrad)	4	4	4	2	4	3	4
Relative Stärke (Rangplatz)	1	1	1	7	1	6	1
Aktivierte eID-Funktion (Rangplatz)	1	3	7	5	6	4	2
eID-Nutzung (% der elektron. Erklärungen) (Rangplatz)	3	7	5	2	5	1	3

Tabelle 2: Stärke der Authentisierung sowie Verbreitung und Nutzung der eID in sieben Ländern

Tabelle 2 zeigt in der ersten Zeile diesen Rangplatz für den Vergewisserungsgrad der eIDMS und in den beiden Zeilen darunter die Rangplätze für die aktivierten eID-Funktionen und die Nutzung bei der elektronischen Steuererklärung. Die drei Spitzenreiter beim Aktivierungsgrad (Belgien, Estland und Spanien) weisen, wie zu erwarten ist, auch die höchste Vergewisserungsstufe auf. Aber dieser Zusammenhang ist nicht durchgehend. Denn Österreich und Finnland erreichen mit demselben Vergewisserungsgrad nur die beiden letzten Plätze beim Aktivierungsgrad. In Bezug auf die Nutzungsquote wird der Einfluss der Stärke der Authentisierungsverfahren noch schwächer und kippt sogar in das Gegenteil: Schweden und Dänemark liegen an der Spitze der Nutzungsquoten, obwohl sie wegen ihrer Softwarezertifikate die schwächsten Authentisierungsverfahren anbieten.

Diese Befunde erscheinen weniger verwunderlich, wenn man berücksichtigt, wem der höhere Vergewisserungsgrad dient. Die meisten Verfahren erhöhen die Gewissheit des Dienstanbieters über die Identität seiner Nutzerinnen und Nutzer. Er kann nun sicher sein, dass sich diese mit ihrer amtlichen Identität registrieren und einloggen. Die Nutzerinnen und Nutzer erfahren hingegen durch die eID in den meisten Fällen nichts über die Identität des Dienstanbieters. So kommt es bei diesen einseitigen Authentisierungsverfahren zu einer asymmetrischen Verteilung von Kosten und Nutzen: Die Bürgerinnen und Bürger sollen investieren, um die Gewissheit der Dienstanbieter über ihre Identität zu erhöhen. In dieser Hinsicht unterscheidet sich das deutsche Verfahren allerdings von allen anderen. Es wird als zwei- oder wechselseitiges Verfahren der Authentisierung gelobt. In einem Flyer des BMI heißt es sogar: *mit dem eIDN wissen Sie immer, mit wem Sie es im Internet zu tun haben*. Tatsächlich gibt das erwähnte Berechtigungszertifikat jedoch keine Auskunft über die Zuverlässigkeit oder Vertrauenswürdigkeit des Dienstanbieters. Für das Berechtigungszertifikat wird, wie der Name sagt, lediglich datenschutzrechtlich die Erforderlichkeit der für den Zugriff beantragten ID-Daten für den jeweiligen Dienst geprüft. Ob es Beschwerden bei den Verbraucherorganisationen oder datenschutzrechtliche Verstöße gab, wird nicht geprüft.

Einfachheit hat die höchste Priorität

Die Nutzungspräferenzen werden noch deutlicher, wenn man die Anteile der unterschiedlichen Authentisierungsverfahren bei der Abgabe elektronischer Steuererklärungen vergleicht (Tabelle 3): Die Chipkarten-basierten Verfahren erreichen nur einen Anteil zwischen einem und maximal 14 Prozent, während Softwarezertifikate, One-Time-Passwörter (TAN-Verfahren) und das viel kritisierte Benutzername-Passwort-Verfahren dominieren.

Das Haupthindernis dürfte, wie schon bei den elektronischen Signaturen, der Kartenleser sein. Er muss nicht nur beschafft und bezahlt, sondern auch installiert werden. Die Forschungspartner in Belgien und Spanien hatten erhebliche Probleme, die Clientsoftware und den Treiber für den Kartenleser in ihren Browser zu integrieren. Eine vom BMI in Auftrag gegebene Akzeptanz- und Usability-Studie äußert sich kritisch zu einer Installationsdauer von bis zu 36 Minuten (Grote u.a. 2010). Im Oktober 2010 erschienene Medienberichte über Sicherheitslücken, die der Chaos Computer Club öffentlich gemacht hat, haben die in der Akzeptanzstudie festgestellten Zweifel vieler Bürgerinnen und Bürger noch verstärkt. Zwar handelt es sich um bekannte Sicherheitslü-

Authentisierungsverfahren	Stärke des Verfahrens	BE	AT	ES	DK	FI	SE	EE
eID-Card	4	20%*	1%	1%		1%	2%	14%
SW-Zertifikat	3			99%	19%		22,5%	
Papier-basiert OTP-Code	2-3	80%			81%		37,3%	Ca. 80%
Username + Password	1		99%					
Telefon	2						23,2%	
SMS	2						15,1%	

* Davon die Hälfte über Mitarbeiter der Verwaltung oder Steuerberater

Tabelle 3: Alternative Authentisierungsverfahren bei Online-Steuererklärungen in sieben Ländern

cken von PCs, die vor allem dann zum Tragen kommen, wenn man den einfachen Basisleser ohne eigene Tastatur für die Eingabe der PIN benutzt. BMI und BSI verweisen daher auf die sichereren Standard- und Komfortleser, die allerdings auch deutlich teurer sind, und erwarten im Übrigen, dass alle Nutzerinnen und Nutzer ihre PCs vor Angriffen schützen, eine Firewall installiert haben, ihre Antivirenprogramme ständig aktualisieren, die Karte nicht auf dem Kartenleser liegen lassen u. a. m. In dieser Argumentationslinie werden die Bürgerinnen und Bürger, denen ein sichereres Verfahren der Authentisierung angeboten werden soll, letztlich zum Sicherheitsrisiko erklärt: Wenn sie nicht all das tun und ihre eID von anderen missbraucht wird, sind sie danach wohl selber schuld und müssen für den Schaden haften.

Das Missverständnis von dem „Einen für zwei Welten"

Zu einer solchen paradoxen Argumentation kommt es aufgrund eines Missverständnisses bei der Auswahl der Personalausweise als Token für die eID. In Belgien, Spanien und Deutschland stand in erster Linie die Entwicklung eines neuen chipbasierten Ausweises für Grenz- und Polizeikontrollen an. Dieser sollte noch fälschungssicherer sein und in Deutschland durch das biometrische Foto und die ursprünglich verpflichtende Speicherung von Fingerabdrücken auch die Sicherheit der Authentifizierung der Besitzer erhöhen. Als gleichzeitig das Thema Identitätsdiebstahl im Internet hochkam und als Barriere für die intensivere Nutzung der wirtschaftlichen und gesellschaftlichen Potenziale dieses neuen Mediums eingeschätzt wurde, verfielen die für den Personalausweis Verantwortlichen auf die Idee, man sollte sich mit demselben Token nicht nur in der realen Welt, sondern auch im Internet ausweisen können. Das Leitbild des Sich-Ausweisens prägt dementsprechend die eID-Funktion auf den Personalausweisen. So wird für den neuen deutschen Personalausweis auch mit dem Slogan geworben „Der eine für zwei Welten". Dieses falsche Leitbild führt zu dem schon erwähnten Problem der asymmetrischen Verteilung von Kosten und Nutzen. Denn es werden die fundamentalen Unterschiede in Bezug auf die Herstellbarkeit von mehr Sicherheit übersehen. Die beiden „Welten" unterscheiden sich in nahezu jeder Hinsicht. Bei den hoheitlichen Anwendungen handelt es sich um einige wenige geschlossene, zentral gestaltete, im Zeitablauf stabile und zentral steuerbare Systeme mit einheitlichen Endgeräten und wenigen, vollständig definierten Prozessen, die von geschulten Beamten bedient werden. Demgegenüber ist die eID-Funktion nur ein kleines Element in der Gesamtheit aller Online-Transaktionen, das dort mit funktional ähnlichen Verfahren konkurriert. Die Gesamtmenge der Transaktionen im Internet und die dafür eingesetzte Hard- und Software bilden ein heterogenes, sich permanent veränderndes offenes System, dessen Technikeinsatz und Nutzung niemand steuern kann. Die Entwickler und Herausgeber der eID haben sich enorm überschätzt, als sie das Nutzenversprechen abgegeben haben, diese chaotische Welt durch die eID sicherer zu machen.

Authentisierung oder Autorisierung

Mit der Fixierung auf das Sich-Ausweisen wurde noch ein weiterer Unterschied übersehen. Die meisten Nutzerinnen und Nutzer wickeln online einen großen Teil ihrer Transaktionen mit immer denselben Dienstanbietern ab. Sie machen Online-Banking, buchen Fahrkarten, kaufen Bücher und MP3 Files und bewegen sich in einem Social Network. Der Nachweis der amtlichen Identität ist bei der Erstregistrierung akzeptabel und im beiderseitigen Interesse. Aber warum soll man sich mit demselben Aufwand bei jeder Banküberweisung authentisieren? Betrachtet man das Online-Banking genauer, dann stellt man fest, dass die Banken in den vergangenen Jahren nicht an der Verbesserung der Sicherheit des Log-Ins gearbeitet haben, sondern an der der TAN. Nach einer Liste auf Papier, von der man selbst eine TAN wählen konnte, kam die Aufforderung, eine bestimmte TAN mit einer vorgegebenen laufenden Nummer einzusetzen. Dieses Verfahren wird in jüngster Zeit durch das mTAN- oder iTAN-Verfahren ersetzt. Die mTAN wird über einen zweiten Kanal auf ein zuvor registriertes Mobiltelefon geschickt und muss per Hand zur Autorisierung einer Überweisung eingegeben werden. Ein Angreifer müsste also nicht nur die Kontrolle über den PC errungen haben, sondern genau in dem Moment auch die Mobilkommunikation abfangen. Noch sicherer ist das iTAN-Verfahren, bei dem eine Ausgangs-TAN im Online-Banking-Dialog gesendet wird, die man in einen Offline-TAN-Generator eingeben muss. Dieser nicht an das Netz angeschlossene Kartenleser errechnet dann in Abhängigkeit von der eingesteckten Bankkarte die eigentliche TAN, die man per Hand eingibt. Die meisten Banken scheuen zur Zeit noch die Kosten für diesen Kartenleser. In Belgien und Österreich ziehen zumindest einige Banken diese Lösung jedoch der eID vor, weil sie deutlich geringere Hotline-Kosten verursacht. In Österreich ziehen sich die Banken von dem Angebot der Bürgerkarte zurück, weil es nach Browser- und Betriebssystemwechseln immer wieder Kompatibilitätsprobleme mit dem Client und dem Kartenleser gab und die Anrufe bei der Hotline des Online-Banking sprunghaft angestiegen sind.

In Deutschland stehen die Banken der eID skeptisch gegenüber. An dem Anwendungstest hat nur eine Bank, die DKB, teilgenommen. Die DKB ist eine reine Online-Bank. Bei der Kontoeröffnung erfolgt die Authentifizierung bisher über das Post-Ident-Verfahren. Im Vergleich dazu ist die eID einfacher und günstiger. Aber das Online-Banking erfolgt auch bei der DKB weiterhin nur mit dem PIN/TAN-Verfahren. Auch wenn es nicht

Herbert Kubicek

Prof. Dr. **Herbert Kubicek**, Institut für Informationsmanagement Bremen (ifib).
Beiratsmiglied des FIfF.

in das Weltbild der IT-Sicherheitsexperten mit ihrem kryptologischen Hintergrund passt: Die m- und iTAN-Verfahren sind sicherer als die eID mit PIN, weil die Wissenskomponente dynamisch ist. Man braucht für jede Transaktion eine neue, dynamisch generierte TAN, während die eID-PIN statisch ist und daher leichter kompromittiert werden kann.

Prognose und strategische Optionen

Das sind keine guten Voraussetzungen für die Akzeptanz des eIDN auf dem neuen Personalausweis. Ganz so schlimm wie in Finnland, wo nur ein Prozent der Antragsteller eines neuen Personalausweises die zusätzlich zu bezahlende eID-Funktion gewählt haben, wird es nicht kommen. Aber die 80% Aktivierung in Belgien werden auch nicht zu erreichen sein, weil dort eine Alles-aus-einer-Hand-Strategie verfolgt wurde und der Staat auch den Verzeichnisdienst für die elektronische Signatur bezahlt. Der in Estland erreichte Aktivierungsgrad von 50% dürfte die in Deutschland in drei bis fünf Jahren erreichbare Obergrenze darstellen. Dort gibt es, wie erwähnt, einige exklusive Anwendungen für die eID, die in Deutschland bisher nicht erkennbar, für die Zukunft aber auch nicht auszuschließen sind. Doch der Aktivierungsgrad sagt noch nichts über die Nutzung. Nicht jeder, der den eIDN beantragt, wird sich nachher auch den Kartenleser besorgen und den Client installieren. Bei der elektronischen Steuererklärung ELSTER wird der eIDN neben den bisherigen Verfahren der Authentisierung angeboten und wie in den anderen Ländern einen Anteil zwischen 10 und 20% erreichen.

Damit wird das Ziel, die Transaktionen im Internet sicherer zu machen, deutlich verfehlt. Will man dennoch etwas zur Erreichung dieses Zieles tun, gibt es vor allem zwei strategische Optionen: Man kann versuchen, es den Esten nachzumachen, und wenn das nicht gelingt, wie die Finnen reagieren.

Die einzige erfolgreiche Implementierung der eIDN auf einem Personalausweis ist in Estland zu finden. Dort wird sie von einem Konsortium aus Banken und einem Telekommunikationsunternehmen ausgegeben, das ein wirtschaftliches Interesse am Verkauf dieses Zusatzprodukts hat. Das Konsortium hat nach einer wenig erfolgreichen Startphase erkannt, dass es sich intensiv um exklusive und sichtbare Anwendungen bemühen muss und hat dies auch geschafft. Exklusiv ist das erwähnte i-voting, das insbesondere Erstwähler motiviert, sich die eID zuzulegen. Sichtbar ist die Anwendung an Fahrkartenautomaten in Tallin und anderen großen Städten. Man kann sich mit der eID auch für das Online-Banking einloggen und mit der Signaturfunktion Überweisungen tätigen. Das PIN-TAN-Verfahren wird zwar weiterhin angeboten. Aber kürzlich haben die Banken das Limit für Online-Überweisungen beim PIN-TAN-Verfahren gegenüber dem eID-Verfahren gesenkt (Martens 2010). Für Deutschland bedeutet dies, dass die Banken überzeugt werden müssten, das eID-Verfahren plus elektronische Signatur nicht nur auch anzubieten, sondern es zu bevorzugen.

Wahrscheinlich wird dies nicht gelingen. Dann hat es der eIDN deutlich schwerer als in Estland, und es bleibt nur die finnische Strategie: Nachdem nur ein Prozent der Personen, die einen neuen Personalausweis erwerben mussten, diesen mit eID-Funktion beantragt haben, hat die Regierung zur Verbesserung der Online-Sicherheit im E-Government mit den finnischen Banken vereinbart, deren TAN-Lösung auch für E-Government-Dienste einzusetzen. Über das nationale Portal VETUMA kann man mit demselben Benutzernamen und Passwort auf das Online-Banking und auf E-Government-Dienste zugreifen und die jeweiligen Transaktionen mit einer TAN autorisieren (Rissanen 2010 sowie Kubicek und Noack 2010).

Mit anderen Worten: Wenn der Innenminister die Banken nicht von den Vorteilen seiner Lösung überzeugen kann, soll er sich von den Vorzügen der Bankenlösung für die Mehrzahl der Transaktionen im Internet überzeugen lassen. Diese ist millionenfach bewährt, wird ständig technisch verbessert, ist alltagstauglich und fehlertolerant, erfordert keine Investitionen und Rüstkosten auf Seiten der Nutzer und ist auch für die Anbieter wirtschaftlich günstiger. Aber bevor es dazu kommt, müssten die Verantwortlichen erst einmal einsehen, dass sie auf dem falschen Pfad sind. Und das wird wohl erst geschehen, wenn die obige Prognose in drei Jahren bestätigt wird.

Literatur

Aichholzer, G., Strauß, S. (2010): The Austrian Case: Multi-card concept and the relationship between citizen ID and social security cards. Identity in the Information Society, Vol. 3, No. 1, Juli 2010, S. 65-85.

Grote, J. H., Keizer, D., Kenzler, D., Kenzler, P., Meinel, Ch., Schnjakin, M., Zoth, L. (2010): Vom Client zur App. Ideenkatalog zur Gestaltung der Software zum Einsatz des neuen Personalausweises. Hasso Plattner Institut (http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Studie_Usability_Volltext.pdf?__blob=publicationFile)

Kubicek, H., Noack, T. (2010): Mehr Sicherheit im Internet durch elektronischen Identitätsnachweis? Der neue Personalausweis im europäischen Vergleich. Münster: LIT Verlag

Mariën, I., Van Audenhove, L. (2010): The Belgian e-ID and its complex path to implementation and innovational change. Identity in the Information Society, Vol. 3, No. 1, Juli 2010, S. 27-41.

Martens, T. (2010): Electronic identity management in Estonia between market and state governance. Identity in the Information Society, Vol. 3, No. 1, Juli 2010, S. 213-233.

Rissanen, T. (2010): Electronic identity in Finland: ID cards vs. bank IDs. Identity in the Information Society, Vol. 3, No. 1, Juli 2010, S. 175-194.

STORK (2009): Quality Authentication Scheme. Deliverable D 2.3. STORK eID Consortium.

Lew Palm

Praxisüberwachung – ein Recherche- und Erfahrungsbericht

Ärztliche und psychotherapeutische Praxen müssen bis zum Jahr 2011 einen Spionage-Router in ihren Computernetzwerken einsetzen

Zur Zeit werden die meisten Praxen in Deutschland von den Kassenärztlichen Vereinigungen zu einer Anbindung an ein Netzwerk namens KV-SafeNet *über das Internet gezwungen. Ich bin Informatiker und betreue die Computersysteme einer psychotherapeutischen Praxis. Mir sind grobe Sicherheitsmängel in Konzeption und Ausführung dieser Umstellung aufgefallen, jedoch kein Nutzen für Ärzte, Therapeuten oder Patienten. Des Weiteren sehe ich gesellschaftliche und politische Gefahren und die Möglichkeit, dass die eingesetzte Technik sich sehr einfach zum Überwachen des gesamten internen Datenverkehrs jedes lokalen Praxis-Computernetzwerks verwenden lässt.*

Die niedergelassenen Ärzte und Psychotherapeuten in Deutschland rechnen ihre Leistungen nicht direkt mit den gesetzlichen Krankenkassen ab, sondern sie tun dies über Mittlerinnen, die Kassenärztlichen Vereinigungen (KVen). In jedem Bundesland gibt es eine KV, und gemeinsam sind sie in der Kassenärztlichen Bundesvereinigung (KBV) organisiert, die vom Gesundheitsministerium kontrolliert wird. Vereinfacht gesagt, haben die KVen auch den öffentlichen Auftrag, die knapp 150.000 Praxen so zu organisieren, dass sie im Interesse der etwa 72 Millionen gesetzlich Krankenversicherten wirken können[1].

In der von mir betreuten Praxis wurde bislang das Versenden der KV-Abrechnung, welches quartalsweise ansteht, durch das persönliche Überbringen von feststofflichen Datenträgern bewerkstelligt. Dazu wurden eine CD, Diskette oder Papiere direkt zur Geschäftsstelle der Kassenärztlichen Vereinigung gebracht. Dem Praxispersonal war das recht, der Aufwand ist nicht sehr groß. Mir als IT-Verantwortlichem gefiel es auch, denn so musste kein Praxisrechner am Internet hängen (und die Sicherheit der persönlichen Datenübertragung ist ungeschlagen hoch). Die für Abrechnungen in dieser Praxis verwendbare und auf dem Markt existierende Software setzt zwingend ein Microsoft Windows als Betriebssystem voraus. Es wird mit sehr schützenswerten Daten der Patienten umgegangen, aber eine Vielzahl nachlässig betreuter Windows-Computer ist mit Backdoors bzw. Rootkits verseucht. Deswegen wollte ich eine Anbindung der Praxis an das Internet vermeiden, da sie einen unverhältnismäßig hohen Aufwand an Sicherheitsmaßnahmen erforderlich gemacht hätte. Alle mir bekannten psychotherapeutischen Praxen der Umgebung lieferten die Abrechnungsdaten persönlich bei der KV ab; es ist aber zu vermuten, dass viele andere (bei größerer räumlicher Entfernung zum nächsten KV-Büro) ihre Abrechnung per Einschreiben über den Postweg versendeten.

Zwang zur Internet-Abrechnung

Doch nun hat sich die Situation geändert. Die KVen haben die bisherige Vorgehensweise verboten und zwingen die niedergelassenen Ärzte und Psychotherapeuten ab dem Jahr 2011 zur Online-Abrechnung[2]. Der Sinn des Zwangs erschloss sich mir zunächst nicht. Dem minimal höheren Aufwand des manuellen Einlesens eines Datenträgers pro Arzt bzw. Therapeuten und Quartal bei den KVen steht ein erhöhtes Sicherheitsrisiko durch IT-unkundige Praxismitarbeiter gegenüber, die ihre Computer mit dem Internet verbinden müssen. Mir schien eher ein sukzessiver und zwangfreier Umstieg von persönlicher oder postalischer zur Online-Übertragung sinnvoll, falls dieser von den Betroffenen überhaupt gewünscht ist.

Auch ging ich davon aus, dass ein *einfaches* und *sicheres* Verfahren gewählt würde. Eine Grundregel beim Entwerfen eines jeden technischen Systems ist, das System so einfach wie möglich (und nötig) zu halten, da jedes zusätzliche Element Risiken birgt. Es würde sich anbieten, die Abrechnungs-Datei auf dem Arzt-Computer mit dem öffentlichen PGP-Schlüssel der KV zu verschlüsseln (z.B. mit GnuPG[3]), und sie dann über eine beliebige Dateiübertragungs-Technik (z.B. Secure CoPy) auf den KV-Server zu transportieren. Dafür sind alle Programme vorhanden und ausgiebig erprobt; die Einbindung in jede bestehende Arzt-Abrechnungs-Software wäre trivial. Der größte Vorteil läge in der *Überprüfbarkeit* der Sicherheit der technischen Vorgänge durch die Öffentlichkeit (bzw. durch unterschiedliche Experten, die für keine oder zumindest unterschiedliche Lobbys arbeiten), denn der Quellcode der genannten – im Sicherheitsbereich wichtigen und populären – Programme liegt offen vor.

Es kam aber ganz anders. Die KVen entschieden sich, mit Kanonen auf kleine, niedliche Vögel zu schießen. Sie bildeten ein Computernetzwerk namens *KV-SafeNet*, wobei die Rechner der Bundesländer-KVen und der KBV-Zentrale über dicke Datenleitungen (Backbones) verbunden sind. Den Anschluss dieser Server an das (bzw. die Schnittstelle zum) Internet organisieren momentan 25 privatwirtschaftliche Firmen[4]. Von der Praxis aus wird durch einen Tunnel über einen DSL-Anschluss und das Internet ein Virtuelles Privates Netzwerk zu einem Server dieser Firmen aufgebaut. Aus der Sicht der auf einem Praxis-Rechner laufenden Software wirkt das so, als sei der Computer in einem lokalen Netzwerk mit den anderen Praxen, den KV-Servern und den Servern der eben genannten Firmen.

Das Konzept ist nicht schlecht – wenn man von einer Zentrale aus eine permanente Verbindung zu allen Praxiscomputern haben möchte. Für die KV-Abrechnung und so gut wie alle anderen Datenverarbeitungs-Bedürfnisse der Ärzte, Psychotherapeuten und Patienten ist es völlig unnötig.

Geheimkasten 007 in undurchsichtiger Mission

Es geht noch weiter: Die KVen haben angeordnet, dass der Aufbau des Tunnels nicht durch einen Praxiscomputer selbst ge-

schieht (was problemlos möglich wäre), sondern durch einen speziellen Router. Dieser Router muss von den Praxisbetreibern bei einer der 25 *Provider*-Firmen gekauft werden. Von den KVen wird er offiziell treffenderweise *Blackbox* genannt, denn *in seine Funktionsweise darf von den Ärzten und Psychotherapeuten bzw. ihren IT-Betreuern keine Einsicht genommen werden*. Als Router ist er meistens das Zentrum auch des internen Netzwerk-Datenverkehrs in der Praxis. Er darf aber vom Praxisbetreiber weder konfiguriert werden, noch kann dieser nachvollziehen, zu welchen Servern im Internet der Router Verbindungen aufnimmt und welche Daten er überträgt. Eine Überwachung und Protokollierung der gesamten lokalen Netzwerkdaten durch die entsprechende KV-SafeNet-Provider-Firma ist problemlos möglich, da diese den Router ohne das Wissen des Arztes bzw. Therapeuten fernsteuern und einrichten kann. Kein zurechnungsfähiger IT-Administrator würde eine Blackbox mit einer verschlüsselten Schnittstelle nach außen in das Zentrum seines Netzwerks einbauen und danach noch einen Pfifferling auf die Sicherheit des Systems wetten – denke ich. Die KVen scheinen das anders zu sehen; sie haben ja auch keine Hemmungen, die Praxen zu einer Installation einer solchen Box zu zwingen.

Man muss also als Arzt, Psychotherapeut (und als deren Patient) seiner SafeNet-Anbieter-Firma (zu denen auch die Telekom gehört) vollkommen vertrauen. Ebenso muss man darauf vertrauen, dass, sollte die *Blackbox* immerhin ordnungsgemäß funktionieren, allen anderen am Gesamtnetzwerk Beteiligten keine sicherheitstechnischen Schnitzer passieren. Dies sind immerhin 25 Provider-Firmen, 17 KVen, die KBV und mehrere zehntausend Praxen. Allein die Größe des Netzwerks und seine vielen Schnittstellen zum Internet machen klar, dass eine Abschottung gegen ernsthafte Angreifer von außen eher Minuten als Tage hält. Man muss davon ausgehen, dass Datendiebe oder -manipulateure sich sehr schnell zumindest einen Praxis-Account bei einem der Provider besorgen können und damit Teil des Netzes werden.

Der Begriff *Blackbox* ist auch nur aus Sicht der Praxis und Patienten treffend – für die verkaufende *Provider*-Firma handelt es sich um eine White Box, denn ihre interne Funktionsweise ist dort vollständig bekannt. Zumindest muss man hoffen, dass dies zutrifft und keiner der Firmen relevante Fehler oder unerwünschte sicherheitskritische Funktionen in ihrer Box übersieht. Wie gut die Firmen in diesem zentralen Punkt ihre Arbeit machen, ist aber prinzipiell nicht überprüfbar, denn für ihre Kunden ist die Box ja *black*.

Security by Obscurity

Die Übertragung der Patientendaten im *SafeNet* wird allerdings noch einmal verschlüsselt – per PaDok bzw. D2D, der gleichen Technik, die auch auf der elektronischen Gesundheitskarte zum Einsatz kommen soll (der CCC hat sich in der Datenschleuder Nr. 85 damit beschäftigt[5]). Diese Technik hat mit dem *Blackbox*-Router im Praxis-Netzwerk eines gemeinsam: Die Hersteller verraten nicht, wie sie funktioniert[6]. Das soll vermeintlich die Sicherheit des Systems erhöhen, da angreifende Kriminelle etwas Zeit zur Analyse brauchen. Diese Vorgehensweise nennt man *security by obscurity*. Sie ist kontraproduktiv, da eine Analyse wohlmeinender Sicherheitsexperten unterbunden wird, die Kriminellen auf Dauer aber selten am Verstehen des Systems gehindert werden. So ließen sich die gesamten geheimen Einstellungen der *Blackbox* meiner Praxis mit wenigen Stunden Arbeit auslesen, wenn man das Gerät in den Händen und die Motivation zu einer kriminellen Handlung hat. Die *Blackboxerei* stellt also keineswegs einen ernstzunehmenden Schutz gegen Kriminelle und bösartige Datendiebe dar, sondern sie hindert einzig die Betreiber der Praxen an der Kontrolle über ihre eigene IT-Infrastruktur.

Claude Shannon, der Begründer der Informationstheorie, äußerte sich schon in den 40er Jahren zu diesem Thema: *„The enemy knows the system"*. Auguste Kerckhoffs schrieb 1883 in seinen Grundsätzen der modernen Kryptographie: *„The system must not require secrecy and can be stolen by the enemy without causing trouble"*[7]. Mit *system* bezog er sich auf den technischen Verschlüsselungsapparat. Damit meinte er, dass die Kenntnis vom Verschlüsselungsalgorithmus, die ein Spion durch das Stehlen des Apparats erlangt, diesem beim Entschlüsseln der geheimen Nachrichten nicht helfen dürfe. Seit über einhundert Jahren ist es allen Kryptographen bekannt, dass man Sicherheit durch die hohe Qualität der Kodierverfahren und nicht durch die Geheimhaltung derselben herstellen sollte. Eine Verschleierung der Verfahren selbst spricht immer für ihre mindere Qualität – und hält nie lange.

Zur Kasse bitte

Ein weiterer Nachteil des *SafeNets* sind die hohen Kosten für die Praxen. Ein Blackbox-Router kostet zwischen 190 und 500 Euro. Die Provider-Firmen verlangen von jeder Praxis eine monatliche Gebühr von mindestens 17 Euro (zusätzlich zum DSL-Anschluss). Bei einem Übertragungsvolumen von oft weniger als

Lew Palm

Lew Palm ist verheiratet und lebt mit Frau und Hund in Berlin-Neukölln. Zur Zeit schreibt er an der Universität Bremen seine Diplomarbeit in der Biologie und der Informatik, bei der es nicht um Gesundheitspolitik, sondern um die Computersimulation von Evolution geht. Er gehört keiner politischen oder wirtschaftlichen Organisation an, beschäftigte sich jedoch innerhalb wie außerhalb des Studiums auf technischer und auf gesellschaftlicher Ebene mit Themen wie der informationellen Selbstbestimmung und der politischen Macht, die mit dem Besitz, der Verbreitung oder der Geheimhaltung von Informationen einhergehen kann. Zu erreichen ist er unter *lew@informatik.uni-bremen.de*.

einem Megabyte (so zumindest in der von mir betreuten Praxis) pro Quartal sind die jährlichen Kosten von über 200 Euro unverhältnismäßig hoch. Hier könnte man darüber nachdenken, ob die Preisgestaltung nicht nach § 138 Abs. 2 BGB als sittenwidrig einzuschätzen ist.

Die Entwickler bzw. Entscheider hinter dem *SafeNet* bauen also ein System, das nicht mal den Sicherheitskonzepten von 1883 entspricht. Es ist für die KVen wie auch für die Ärzte sehr teuer, dabei für die Abrechnung unnötig. Allein die Größe und Menge der involvierten Parteien (u. a. 25 Privatfirmen) macht das Netz angreifbar. Die Abrechnungen wären über bestehende Techniken (PGP) einfacher, billiger und sicherer zu übertragen. Jeder Netzwerk-Administrator wird auf die Barrikaden gehen, wenn er eine ferngesteuerte Blackbox in das Zentrum seines Netzes einsetzen soll, wie dies nun in den Praxen geschehen muss. Hier drängt sich nach Marcus Cicero die Frage auf: *„Wem nützt es?"* Die erste Antwort darauf ist merkwürdig. Auf den ersten Blick scheint es nur den 25 Provider-Firmen zu nutzen, die daran kräftig verdienen. Diese sind aber nicht die Initiatoren. Alle anderen haben mit dem *SafeNet* erst mal nur Ärger.

Doch vor Spekulationen über die Interessen hinter *SafeNet* möchte ich über die Erfahrungen berichten, die ich als IT-Administrator meiner Praxis in den letzten Tagen gemacht habe.

Zur Zeit bekommen die Ärzte und Psychotherapeuten vieler Bundesländer von den KVen eine motivationsfördernde *Prämie* von mehreren hundert Euro, wenn sie innerhalb von kurzer Zeit die ferngesteuerte *Blackbox* für ihr Praxis-Netzwerk anschaffen[8]. Wohlgemerkt müssen die Praxen dies sowieso tun, denn andere Arten der Abrechnungen werden nicht mehr akzeptiert. Wieso für eine verpflichtende Handlung noch eine *Prämie*? Es soll wohl der passive Widerstand vieler Ärzte und Psychotherapeuten gebrochen werden, die durch ein Verschleppen der Anschaffung die Einführung des neuen Systems verzögern oder behindern.

Blick auf eine real existierende „Blackbox"

Die Bestechung funktionierte auch bei meiner Praxis. Ich schaute mich um nach dem billigsten Angebot und stieß auf die Deutsches Gesundheitsnetz Service GmbH[9]. Dort kostet der Router „nur" 190 Euro, die jährlichen Gebühren für die Berechtigung zur Verbindungsaufnahme zum VPN-Server belaufen sich auf 204 Euro.

Die mysteriöse *Blackbox* interessierte mich besonders. Sie entpuppte sich als *Fritz!Box Fon WLAN 7170*[10], hergestellt von der AVM GmbH aus Berlin. Ein nachträglich angebrachter Aufkleber etikettierte sie um in einen *DGN Safenet-Konnektor*. Dieses Gerät (ohne den Konnektor-Aufkleber) bekommt man nicht nur bei Media Markt und ähnlichen Geschäften, sondern auch im Versandhandel ab 120 Euro[11]. Der mit 70 Euro bezahlte *Mehrwert* des an meine Praxis gelieferten Routers gegenüber dem Versandhandel-Modell liegt in der Konfiguration: Durch die DGN GmbH wurde die Verbindung zu ihrem Virtuellen Privaten Netzwerk (und vielleicht noch andere Funktionalitäten) eingestellt, sowie ein dem Käufer unbekanntes Login-Passwort gesetzt. Eben jenes geheime Passwort macht für die Praxis dann aus der Fritz!Box eine Black!Box.

Eine Untersuchung des Routers im Netzwerk (genauer gesagt: ein Portscan) ergab dann, dass diverse Server auf dem Gerät laufen und auf Verbindung warten, d.h. verschiedene Ports offen waren[12]. Dies ist für die angedachte Funktionalität des VPN-Routers unnötig; es stellt mindestens ein erhöhtes Sicherheitsrisiko dar. Beispielsweise der laufende Dienst für Telefonie (SIP) ist überflüssig, da das Gerät weder für diesen Zweck angeschafft wurde noch mangels Passwort dafür konfigurierbar wäre.

Unter Anderem lief auch ein Webserver. Die dort angezeigte Seite ist die übliche Fritz!Box-Login-Page. Unter dem Passwort-Feld steht die freundliche Aufforderung *„Wenn Sie Ihr Kennwort vergessen haben, klicken Sie hier"*. Da konnte ich mich nicht zurückhalten und habe es getan. Das Ergebnis war wie erwartet, dass die Fritz!Box ihre Konfiguration löschte und sich damit in den Zustand versetzte, den sie auch hat, wenn man sie frisch aus dem Media Markt trägt.

Auf die Anfrage an die DGN GmbH nach den Konfigurationsdaten wurde ebenfalls wie zu vermuten reagiert: Ich solle das Teil einschicken und eine Gebühr von 30 Euro entrichten, damit die Firma den Router neu konfiguriert.

Bei der ganzen Geschichte gibt es mehrere Hässlichkeiten. Die Firmen verlangen sehr viel Geld für sehr wenig Leistung – besonders die monatlichen 17 Euro für die üblicherweise nur einmal im Quartal genutzte Berechtigung zur Teilnahme am VPN sind unverschämt. Ein happiger Aufschlag von 70 Euro für die Vorkonfiguration eines Routers ist auch nicht wenig. Das ganze Konzept des fremdkontrollierten Routers im Praxis-LAN ist unsicher. Aber wieso laufen auf dem Gerät auch noch unnötige Dienste? Wieso hat die DGN eine Fritz!Box mit WLAN- und Telefonie-Hardware verwendet, wenn solche Funktionalitäten gar nicht genutzt werden dürfen? Es stellt sich auch die Frage, ob ein solches Konsumenten-Endgerät den an eine ärztliche Praxis gestellten Sicherheitsanforderungen genügt. Offenbar hat die DGN mit den überflüssigen Serverdiensten in der Konfiguration geschlampt. Bei einem solch groben Patzer, einem Fehler, durch den jeder Auszubildende in den entsprechenden Lehrberufen durch eine Prüfung fallen würde, drängt sich die Frage auf, wie denn die restliche Konfiguration aussieht. Leider ist das nicht auf legalem Weg überprüfbar, denn die Firma rückt – auf Weisung der KV, es muss ja eine Blackbox sein – mit dem Passwort nicht heraus.

Von Seiten des *SafeNets* bzw. der Provider-Firma aus ist der Router ebenso erreichbar wie aus dem lokalen Netzwerk (dank VPN). Deswegen können sich die Angestellten der DGN in unsere Fritz!Box jederzeit einloggen, sie haben ja auch das Passwort. Beworben wird das auf deren Homepage mit *„Kostenlose und komfortable Fernwartung durch unsere Hotline-Mitarbeiter"*[13]. Das bedeutet schlicht, dass jede ärztliche und psychotherapeutische Praxis in Deutschland die Kontrolle über ihren herausgehenden und *internen* Datenverkehr an eines der privatwirtschaftlichen *SafeNet*-Unternehmen *outsourcen muss*!

Im Fall der DGN hat die Sache noch ein Sahnehäubchen: Die Fritz!Box hat eine Funktion zum Mitschneiden des gesamten Datenverkehrs schon eingebaut. Auf der Seite http://router-adresse/html/capture.html – wobei Router-Adresse durch die IP-Adresse der jeweiligen Praxis-Fritz!Box zu ersetzen ist – kann

ein DGN-Angestellter bequem und ohne besondere Computerkenntnisse über den Webbrowser das Mitschneiden des gesamten internen Netzwerk-Datenverkehrs in der jeweiligen Praxis ein- und ausschalten und die Daten zu sich herunterladen[14].

Wozu sich das „SafeNet" gebrauchen ließe?

Aber warum sollte das jemand tun? Weiter gefasst, führt das zu der weiter oben gestellten und noch nicht beantworteten Frage: Warum das alles? Wem nützt es? Hier kann nur spekuliert werden. Es ist jedoch offensichtlich, dass die vorgegebenen Argumente für das *SafeNet* nicht mit den echten Interessen übereinstimmen. Wollte man wirklich ein gutes System für die Online-Übertragung der Abrechnung über das Internet, so hätte man das einfacher, schneller, besser, sicherer und deutlich billiger haben können.

Die Praxen sollen offensichtlich mit aller Gewalt dazu gebracht werden, dass ihre Informationstechnik permanent verbunden ist mit dem Zentralserver der KVen bzw. der KBV, und dass sie durch diese besser überwachbar sind. Die zentrale Anbindung und Vernetzung der Praxen ist für sich allein nicht zweckmäßig; Sinn ergibt das Ganze erst, wenn noch weitere Schritte folgen. Man kann also vermuten, dass die KBV oder das Gesundheitsministerium Erweiterungen des Systems plant, für die die momentan aufgebaute Vernetzung Voraussetzung ist. Was könnte das sein? Es wäre möglich die Abrechnungsdaten, d.h. Daten über Patientenbesuche, Medikamente, Therapien, schon zum Zeitpunkt der Erzeugung zentral bei der KV zu speichern; keine Abrechnung pro Quartal ist dann mehr notwendig, sondern alles geht online und *on-the-fly*. Die Auslagerung der Informationstechnik aus der Praxis in den KV-Server im *SafeNet* lässt sich noch deutlich weiter treiben. Warum nicht alle Patientendaten in die Zentrale wie Diagnosen, chronische Krankheiten, Arztnotizen ...? Die Datenhaltung wird viel effizienter und die Praxen müssen sich kaum noch mehr um die Wartung von irgendwelchem Computerkram kümmern. Alle Gesundheitsdaten fast der gesamten Bevölkerung (mit Ausnahme der Privatversicherten) wären an einer Stelle und in einer Hand. Daten sind Macht und eine Datenbank ist mehr als die Summe ihrer Einzelteile. Besonders bei der Pharmaindustrie dürfte eine solche, technisch leicht auszuwertende Datensammlung Begehrlichkeiten wecken.

Endnoten

1 *http://www.kbv.de/wir_ueber_uns/83.html*
2 *Pressemitteilung der KBV dazu: http://www.kbv.de/presse/36724.html*
3 *http://www.gnupg.org/*
4 *Eine Liste ist unter http://www.kbv.de/13815.html einsehbar.*
5 *http://chaosradio.ccc.de/media/ds/ds085.pdf*
6 *Im Falle des Routers stimmt das nicht ganz: Die Funktionsweise ist bekannt – IPsec-VPN – aber die Konfiguration und Zusatzfunktionen sind es nicht.*
7 *http://www.petitcolas.net/fabien/kerckhoffs/*
8 *Z.B. in Bremen gibt es 600 Euro: http://www.aerzteblatt.de/v4/archiv/artikel.asp?id=67269*
9 *http://www.dgn.de/*
10 *Technische Details zum dem Gerät sind unter http://www.wehavemorefun.de/fritzbox/index.php/FRITZ!Box_Fon_WLAN_7170 zu finden.*
11 *Einen Überblick bezüglich der Endkundenpreise kann man sich unter http://www.heise.de/preisvergleich/a178963.html verschaffen.*
12 *Der benannte „SafeNet-Router" der Firma DGN hat folgende offene tcp-Ports: 80, 2049, 5060, 8080, 49000 und 49443*
13 *http://www.dgn.de/50produkte_tarife/05kvsafenet/10easy/index.html*
14 *http://www.wehavemorefun.de/fritzbox/Versteckte_Features*

Jochen Topf

OpenStreetMap: Wir spielen mit offenen Karten

OpenStreetMap hat sich zum Ziel gesetzt, in einem gemeinschaftlich über das Internet organisierten Projekt eine freie Karte unserer Welt zu schaffen. Mehrere zehntausend „Mapper" sind weltweit regelmäßig unterwegs, um die Karte Stück für Stück zu ergänzen. In vielen Regionen ist OpenStreetMap heute schon eine Alternative zu proprietären Karten und Navigationsgeräten.

Kostenlose Karten gibt es im Internet wie Sand am Meer. Fast jeder scheint heute ein Navigationsgerät im Auto zu haben. Wir nutzen Google Street View, um eine neue Wohnung zu suchen, und Google Earth, um den Urlaub zu planen. Jede Firma, die etwas auf sich hält, hat eine Anfahrtsskizze auf ihrer Webseite und Karten zeigen uns, wer auf der Welt gerade was getwittert hat.

Woher die Karten kommen, die man überall sieht und nutzt, darüber machen sich die meisten keine Gedanken. Die Gedanken kommen erst, wenn einem eine kostenpflichtige Abmahnung ins Haus flattert, weil man eine Karte von irgendwoher unerlaubt kopiert und auf seiner Homepage eingebunden hat. Oder wenn man sich fragt, warum auf einer Karte das Neubaugebiet am Stadtrand Jahre nach Fertigstellung immer noch nicht erscheint. Schaut man dahinter, stellt man fest, dass fast alle Karten (genauer: die Geodaten, aus denen diese Karten erstellt werden) entweder von den dafür zuständigen öffentlichen Stellen kommen (in Deutschland zum Beispiel von den Kommunen und Landesvermessungsämtern) oder von zwei Firmen, NAVTEQ und TeleAtlas, die weltweit mit Abstand die wichtigsten Anbieter sind. In letzter Zeit kommt dazu noch Google, das erst nur Geodaten dieser beiden Firmen in ihren Karten wiedergegeben hat, aber inzwischen auch selbst in großem Stil Geodaten sammelt.

Karten, schon immer auch ein Weg, um das Bild der Welt im eigenen Sinne zu prägen, sind heute vor allem ein kommerzielles Gut. Standard-Karten gibt es häufig kostenlos im Internet. Reichen einem die vorgefertigten Karten nicht, will man selbst „Hand anlegen", selbst entscheiden, was wie auf der Karte erscheinen soll, dann braucht man Zugriff auf die den Karten zu

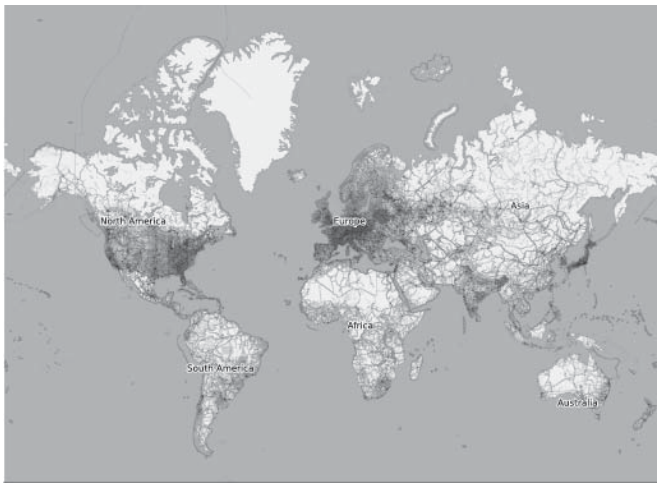


Abb. 1: OpenStreetMap ist ein weltweites Projekt, naturgemäß ist aber die Datendichte und Vollständigkeit sehr unterschiedlich

Grunde liegenden Geodaten, die dann aber viel Geld kosten. Selbst die Vermessungsämter verkaufen die mit Steuergeldern im öffentlichen Auftrag erhobenen Geodaten an ihre Bürger, in der Hoffnung, die Kosten wenigstens teilweise wieder einzuspielen. Schlimmer als die Kosten ist aber das damit verbundene Lizenz-Regime. Geodaten dürfen nicht weitergegeben werden, nicht korrigiert oder ergänzt werden. Das ist der Generation, die mit Open-Source-Software und Wikipedia aufgewachsen ist, nicht mehr genug.

Das Projekt

2004 wurde daher in England das Projekt „OpenStreetMap" (OSM, www.openstreetmap.org/de) gegründet. Ähnlich wie bei Wikipedia liegt dem Projekt die Idee zu Grunde, dass eine Community gemeinsam Daten sammelt und das Ergebnis dann unter einer freien Lizenz zur Verfügung gestellt wird. Jedem soll es möglich sein, die Daten und Karten kostenlos zu nutzen. Die Projektseite fasst das sehr gut in einem Satz zusammen: „The project was started because most maps you think of as free actually have legal or technical restrictions on their use, holding back people from using them in creative, productive, or unexpected ways." (Das Projekt wurde gegründet, weil die meisten Karten, von denen man annimmt, sie seien frei, in Wirklichkeit rechtliche oder technische Beschränkungen in der Nutzung haben, die verhindern, dass sie in kreativer, produktiver oder auf unerwartete Weise genutzt werden.)

Möglich wurde das alles durch zwei neue Technologien, die in den letzten 10 Jahren auch für den Normalbürger nutzbar und erschwinglich geworden sind: Das Internet und das satellitengestützte Ortungssystem GPS. Übrigens beides Technologien, die ihren Ursprung in der *Defense Advanced Research Project Agency* des amerikanischen Verteidigungsministeriums haben.

Erst das Internet ermöglicht die weltweite Zusammenarbeit, die in so einem Projekt nötig ist. Nur wenn es überall Leute *vor Ort* gibt, kann man eine so detailreiche Karte aufbauen, und nur wenn man sich international zusammenfindet, wird daraus eine mehr oder weniger konsistente Karte. Die Zusammenarbeit findet im Projekt hauptsächlich über das Projektwiki (*wiki.openstreetmap.org*) und diverse Mailing-Listen und Foren statt. Es gibt internationale Mailing-Listen, aber auch länderspezifische Listen. Jeder kann dabei mitreden. Einmal jährlich sammelt sich die Gemeinde auf der Konferenz „State of the Map". Etwa 300.000 Leute haben sich bei OpenStreetMap einen Account eingerichtet, aber nur etwa ein Drittel davon haben auch wirklich etwas beigetragen.

Daneben gibt es auch viele lokale Gruppen, die sich mehr oder weniger regelmäßig treffen. Deutschland ist in OSM besonders aktiv, was man auch der Karte ansieht. Hier gibt es solche lokalen Gruppen in über 50 Städten. Aber nicht nur die westliche Welt findet man bei OSM. Von Kibera, Nairobi, dem größten Slum Afrikas, gab es nie eine Karte bis OpenStreetMap-Aktivisten zusammen mit lokalen Bewohnern die Daten für OSM erfaßten.

Gelegentlich trifft man sich zu sogenannten „Mapping Parties": Typischerweise ein Wochenende lang geht man gemeinsam ein Gebiet an, tagsüber werden Daten erfasst, abends trinkt man noch gemeinsam ein Bier. Dieser soziale Aspekt gibt dem Projekt einen ganz anderen Charakter als es viele Datensammelprojekte Einzelner vorher hatten.

Zur Beteiligung am Projekt ist es dabei nicht erforderlich, Mitglied in einem Verein oder dergleichen zu sein. Es gibt die OpenStreetMap Foundation (*www.osmfoundation.org*), die sich um die Verwaltung von Spendengeldern kümmert und den Betrieb der Server organisiert, und den FOSSGIS e.V. (*www.fossgis.de*), der diese Rolle in Deutschland wahrnimmt, aber das sind eher Fördervereine, die auf die allermeisten Aktivitäten im Projekt wenig Einfluss haben.

Geodaten sammeln

Da Karten dem Urheberrecht unterliegen und es rechtlich unklar ist, in wie weit man aus vorhandenen Karten oder Luft- und Satellitenbildern Informationen übernehmen kann, hat sich das Projekt vorgenommen, Geodaten selbst zu erheben oder nur mit ausdrücklicher Erlaubnis des Rechteinhabers zur verwerten. Dazu laufen und fahren die *Mapper* (wie sich die Aktiven im Projekt selbst bezeichnen) durch die Gegend, notieren sich Straßennamen, fotografieren Briefkästen oder murmeln Informationen über Spiel-, Sport- und Parkplätze in ein Diktiergerät. Verbunden mit den Daten aus einem GPS-Gerät, das ermittelt hat, wo man sich jeweils genau befindet, kann man daraus am heimischen Rechner die Karte *zusammenbasteln*. Inzwischen gibt es natürlich auch Möglichkeiten, direkt am Handy oder PDA Daten einzugeben. Und wenn das Wetter schlecht ist, dann kann man vielleicht ein Luftbild abzeichnen, auf dem man zwar keine Straßennamen sehen kann, aber doch die Straßen selbst. Auch Flußläufe, Gebäude und viele andere Details lassen sich auf einem Luftbild sehr gut erkennen. Das geht aber, wie gesagt, nur mit der Genehmigung des Rechteinhabers, die zum Beispiel von Yahoo für deren Satellitenbilder vorliegt.

Die Geodaten werden in einer zentralen Datenbank gesammelt. Jeder stellt dort seine Ergänzungen und Änderungen ein, und jeder hat auch direkt Zugriff auf die aktuellen Daten. Es gibt keine Beschränkungen, wer was eintragen, ändern oder löschen darf. Das ist ein ganz wichtiger Teil des Konzeptes. Es soll so einfach wie möglich sein, am Projekt teilzunehmen. Die Motivation der Mapper ergibt sich auch ganz wesentlich dadurch, dass man

das Ergebnis seiner Arbeit sofort sehen kann. Natürlich schleichen sich so immer wieder auch Fehler ein, aber dafür können sie auch um so schneller wieder beseitigt werden. Das ist sehr anders als bei den proprietären Kartenanbietern, die oft Monate, wenn nicht Jahre, brauchen, um fehlerhafte Daten zu korrigieren. OSM ist daher heute vielfach aktueller als alle anderen Karten.

Um bei absichtlichen oder unabsichtlichen unerwünschten Änderungen den vorherigen Zustand wiederherstellen zu können, wird jede Änderung mit Zeitstempel und Benutzernamen gespeichert. So ist es jederzeit möglich, die Datenbank (oder Teile davon) auf einen früheren Zustand zurückzusetzen. Das wird auch gelegentlich benötigt, um Vandalismus zu beseitigen, meist sind es aber einfach Bedienerfehler bei der Nutzung eines der speziellen OpenStreetMap-Editoren.

Wenn ein Rechteinhaber das erlaubt, werden Geodaten manchmal auch aus bestehenden Datensätzen übernommen. Zum Beispiel wurden Straßendaten für die gesamten USA importiert, die dort von der Behörde für Volkszählung zur Verfügung gestellt wurden. Anders als in Deutschland sind Daten, die von amerikanischen Bundesbehörden gesammelt werden, in aller Regel gemeinfrei (Public Domain) und daher problemlos nutzbar. Auch in Deutschland gab es kleinere solche Aktionen, so hat zum Beispiel die Stadt Rostock die Umrisse aller Gebäude zur Verfügung gestellt und von StraßenNRW hat OSM Informationen über alle überregionalen Straßen in Nordrhein-Westfalen bekommen. Das hilft nicht nur, die OSM-Karte zu verbessern, sondern kommt auch dem „Datenspender" zugute. Er kann anhand der Rückmeldungen und Änderungen durch die Community sehen, wo seine Daten vielleicht Fehler enthalten oder nicht aktuell sind.

Tagging

Jedes Objekt in der OpenStreetMap-Datenbank kann mit beliebigen Attributen (bei OSM *Tags* genannt) versehen werden, die ein Objekt als Straße eines bestimmten Typs, als Briefkasten oder als Bushaltestelle kennzeichnen. Eine Bundesstraße wird zum Beispiel mit dem Tag „highway=primary", ein Restaurant mit „amenity=restaurant" eingetragen. Früher musste man diese Tags noch alle kennen, um sie in die Datenbank einzutragen, heute gibt es dafür menügeführte Programme.

Eine der wesentlichen Stärken von OSM ist, dass jeder Mapper neue Tags erfinden und selbst einfach einführen kann, wenn er keinen passenden bestehenden Tag findet. Es gibt keine abschließende Liste aller Tags und es gibt auch keine klare Begrenzung, welche Daten überhaupt bei OSM erfasst werden sollen. Der Name „OpenStreetMap" ist daher etwas irreführend, es geht um

Abb. 2: Die Stadt Lauf an der Pegnitz hat OpenStreetMap Luftbilder zur Verfügung gestellt und benutzt nun OpenStreetMap auf ihrer Webseite.

viel mehr als nur eine Straßenkarte. Radfahrer können so mit speziellen Tags Informationen erfassen, die für sie wichtig sind (*opencyclemap.org*). Andere arbeiten an Navigation für Blinde (*www.blind.accessiblemaps.org*) oder Rollstuhlfahrer (*wheelmap.org*). Wieder andere an ÖPNV-Karten (*öpnvkarte.de*). So konnte zum Beispiel auch eine Karte mit Skigebieten (*www.openpistemap.org*) entstehen, die spezielle Tags über Skilifte, Seilbahnen und Abfahrtsstrecken mit Schwierigkeitsgrad darstellt.

Nachteil des offenen Taggings ist, dass es manchmal schwierig wird, herauszufinden, wie etwas am besten eingetragen wird. Gelegentlich gibt es konkurrierende Schemata und Durcheinander. Durch die Diskussion innerhalb der Community und die Zusammenarbeit zwischen dem Mapper, der die Daten erfasst, und dem „Kartographen", der die Daten nutzt, ergibt sich so aber mittelfristig ein Community-Konsens. Und auch wenn das in der Praxis nicht immer ganz leicht ist, hat sich gezeigt, dass auf diese Weise die über die Welt verteilten Mapper in der Lage sind, an einem gemeinsamen Projekt zu arbeiten.

Haiti

Mit welcher Geschwindigkeit die Mapper arbeiten können und wie nützlich das flexible Tagging-System ist, hat sich im Januar 2010 nach dem verheerenden Erdbeben in Haiti eindrucksvoll gezeigt. Karten von Haiti gab es schon vor dem Erdbeben kaum und was es gab, war nach den Zerstörungen nicht sehr nützlich. Innerhalb weniger Tage standen aber ausgezeichnete Satellitenbilder zur Verfügung, die von einigen Firmen gespendet wurden, und die Mapper machten sich an die Arbeit. Ohne zentrale

Jochen Topf

Jochen Topf ist seit 2006 im OpenStreetMap-Projekt aktiv, er ist Co-Autor des ersten Buches über OpenStreetMap. Beruflich arbeitet er als selbständiger IT-Berater und Entwickler im Internet-Umfeld und im Bereich GIS und OpenStreetMap.

Weisungen, nur durch selbstorganisierte Koordination über das Wiki und Mailinglisten entstand innerhalb von zwei oder drei Wochen eine detaillierte Karte des betroffenen Gebietes. Zerstörte Gebäude, Krankenhäuser und Flüchtlingscamps erschienen auf der Karte. Die Mapper konnten einfach die speziellen Tags erfinden, die bis dahin keiner gebraucht hatte, die sich jetzt aber plötzlich als notwendig erwiesen. Helfer vor Ort, Behörden, Militär, NGOs, alle nutzten die OpenStreetMap-Karte. Inzwischen hat sich das Humanitarian OpenStreetMap Team (HOT) etabliert, das diese anfänglich unorganisierten Aktivitäten fortführt und erweitert.

OpenStreetMap nutzen

Das Ziel des OpenStreetMap-Projektes ist es in erster Linie, Geodaten zu sammeln und allgemein zur Verfügung zu stellen. Natürlich werden darauf aufbauend vom Projekt selbst auch Karten zur Verfügung gestellt, aber das Projekt kann und will nicht alle Nutzungsmöglichkeiten selbst abdecken. Viele Hobbyisten nutzen OSM-Daten für eigene Projekte, ein paar davon wurden in diesem Artikel ja schon erwähnt. In letzter Zeit setzen aber auch immer mehr Firmen auf OSM. MapQuest (*open.mapquest.de*) bietet OSM als Alternative an, Flickr (*flickr.com*) verwendet teilweise OSM-Karten, selbst das Weiße Haus (*www.whitehouse.gov/change*). Auch in Deutschland ist OSM *angekommen*. Das Bundesverfassungsgericht hat schon sehr früh eine OSM-Karte für seinen Anfahrtsplan verwendet, die Firma Skobbler (*skobbler.de*) bietet seit einiger Zeit Navigation auf OSM-Karten für Mobilgeräte an, Montabaur nutzt OSM in seinem Webstadtplan (montabaur.de). Die Liste ließe sich fortsetzen ...

Alle diese Nutzer mussten nicht um Erlaubnis fragen, sie konnten sich die OSM-Daten und -Karten einfach nehmen und in der gewünschten Art bei sich einbinden. Die bei OSM verwendete Lizenz *Creative Commons Attribution Share-Alike* (*creativecommons.org*) schreibt nur vor, dass ein Nutzer OpenStreetMap als Quelle nennen muss und dass die mit OSM-Daten erzeugte Karte ihrerseits wieder der gleichen Lizenz unterliegt. Ähnlich wie bei Open-Source-Software und Wikipedia liegt die lizenzrechtliche Hürde so niedrig wie möglich. Sie soll nur verhindern, dass sich jemand die Daten „unter den Nagel reißt“ und als seine eigenen ausgibt.

Die Nutzung kann auf ganz verschiedene Art erfolgen. Vielleicht reicht schon ein Screenshot einer OpenStreetMap-Karte für einen Anfahrtsplan. Wollen Sie eine dynamische Karte auf Ihrer Webseite, lässt sich das zum Beispiel mit der Open-Source-Software OpenLayers einfach umsetzen. Das eigentliche Kartenbild liegt auf einem OpenStreetMap-Server in *Kacheln* aufgeteilt parat und kann direkt von dort angefordert werden. Passt Ihnen das Kartenbild nicht, oder ist Ihnen der von der Community betriebene Kachelserver zu unzuverlässig, können Sie inzwischen auch auf die Dienste von Firmen zurückgreifen, die solche Server anbieten. Oder Sie können die Kartenbilder selbst aus den Daten erzeugen und haben damit alle Freiräume bei der Gestaltung.

Die OSM-Daten für den ganzen Planeten werden wöchentlich als Komplettabzug zum Download zur Verfügung gestellt. Wem ein Auszug reicht, der findet auch regionale Ausschnitte. Wer immer aktuelle Daten braucht, bekommt auch Dateien mit den Änderungen des letzten Tages, der letzten Stunde oder der letzten Minute. Auch die Software, um die OSM-Daten in Datenbanken einzulesen oder sie in andere Formate zu transformieren (zum Beispiel für die weit verbreiteten Garmin-GPS-Geräte), steht zur Verfügung. Es gibt sogenannte *Renderer*, die Kartenbilder berechnen, und Navigationssoftware, um auf OSM-Daten zu navigieren (im Internet zum Beispiel unter openrouteservice.org). Der größte Teil dieser Software ist Open Source und damit kostenfrei nutzbar. Zugegebenermaßen ist die Software nicht immer leicht zu verwenden und auch der Umgang mit mehreren hundert Gigabyte großen Dankenbanken ist nicht jedermanns Sache. Hier ergibt sich noch ein weites Betätigungsfeld und viele Verbesserungen sind möglich. Die Entwicklung geht aber in die richtige Richtung: Immer mehr Software taugt auch für den Gelegenheitsnutzer.

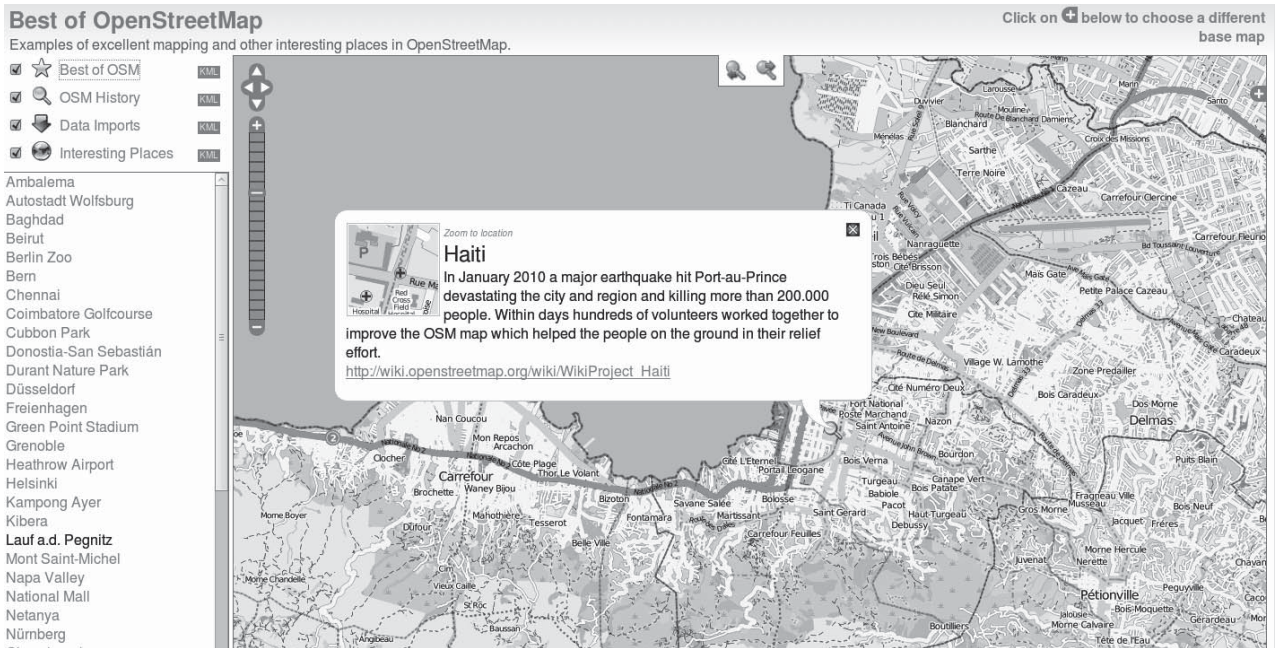


Abbildung 3: Die Webseite bestofosm.org zeigt einige Gegenden, wo OpenStreetMap besonders gute Karten hat. Hier Port-au-Prince, Haiti, wo nach dem Erdbeben in Rekordzeit eine detaillierte Karte entstand.

Mitmachen

OpenStreetMap ist ein Mitmach-Projekt. Es lebt davon, dass viele Leute das erfassen und aktuell halten, was sie interessiert. Für viele ist das ihr Heimatort, andere sind eher thematisch interessiert. Wenn Sie nach der Lektüre auch Lust bekommen haben, etwas beizutragen oder vielleicht auch einfach die Daten nur für eigene Projekte nutzen wollen, finden Sie mehr Informationen auf der deutschen Projektseite (www.openstreetmap.de) oder im Wiki (wiki.openstreetmap.org). Wer so etwas lieber auf Papier nachliest, findet auch alles zu OpenStreetMap in unserem Buch (Ramm, Topf 2010).

Literatur

Ramm, F.; Topf, J. (2010): OpenStreetMap - Die freie Weltkarte nutzen und mitgestalten. 3. überarb. und erw. Aufl. Berlin: Lehmanns Media, ISBN 978-3-86541-375-8

Wolfgang Coy

Zum Bann autonomer Waffensysteme

Zu den neuesten Gerätschaften der russischen Armee gehören aufblasbare Panzer. Auch wenn solche Attrappen schon im Zweiten Weltkrieg eine gewisse Rolle gespielt haben, sind sie doch in ihrer Hightech-Version eine Bereicherung der Tarnung. Von Flugzeug oder Rakete aus schwer zu erkennen, sind sie auch zur Täuschung ferngesteuerter pilotenloser Drohnen sehr gut geeignet und im Vergleich außerordentlich preisgünstig. Erfolgreiche Lowtech-Tarnung gegen Hightech-Angreifer.

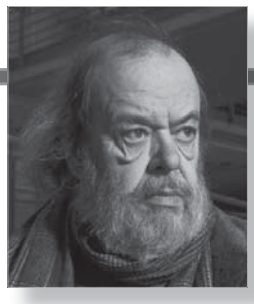
Der weltweite Trend scheint allerdings umgekehrt zu verlaufen. Er folgt, wie so oft, mehr den Trends der US-amerikanischen Rüstungsfirmen. Die Spannweite der Entwicklung reicht bei ferngesteuerten Drohnen vom Winzling, der einem Modellbaukasten entsprungen scheint, bis zur ausgewachsenen Cruise Missile, die das ganze Arsenal moderner Schuss- und Raketenwaffen an Bord hat. Weltweit werden in mehr als 40 Staaten solche Systeme entwickelt und, wie etwa in Afghanistan, im Irak oder in Pakistan, von der US-amerikanischen Armee bereits eingesetzt. Laut Zeitungsberichten arbeiten die USA auch an weltraumtauglichen Drohnen zur Abwehr von Interkontinentalraketen.

Die Vorteile ferngelenkter Waffensysteme sind offensichtlich: Sie sind kleiner und wendiger als bemannte Systeme, sie können sehr lange in der Luft bleiben, ihre Existenz kann notfalls geleugnet und bei Bedarf auf Knopfdruck beendet werden.

Doch nicht nur in der Luft werden Robotwaffen eingesetzt, auch der Bodenkampf wird mehr und mehr durch teilautomatisierte Kriegsgeräte aufgerüstet. Das können Aufklärungssysteme sein, die auch zivilen Nutzen im Katastrophenfall versprechen, aber auch kleine bewaffnete Fahrzeuge, kamerabestückte Fußbälle oder humanoide Kampfroboter mit Maschinenwaffen oder Minen.

Was im ersten Augenblick so aussieht, als wolle die Technologiemacht USA ihre überlegenen Entwicklungskapazitäten zur Humanisierung der Kampfhandlungen einsetzen, zeigt sich bei näherer Betrachtung als Beginn einer neuen Drehung an der Rüstungsspirale. Die Bandbreite solcher teil- oder vollautomatisierten Waffensysteme erlaubt die Teilnahme am Rüstungswettbewerb für Hightech-Armeen ebenso wie für ambitionierte Bastler. Die Basiselemente sind im Versandhandel erhältlich: vergleichsweise einfache Sensorik und Aktorik, die freilich geschickt programmiert werden muss. Verfahren und Algorithmen sind Lehrbüchern oder Tagungsbänden zu entnehmen. Solange keine Waffen oder Sprengstoffe integriert werden, ist ein Robotsystem kaum von ziviler Forschung zu unterscheiden, und der wissenschaftliche Austausch mag über die eine oder andere Schwachstelle hinweghelfen.

An der Humboldt-Universität zu Berlin fand Ende September unter Leitung von Jürgen Altmann von der TU Dortmund und unterstützt von der Deutschen Stiftung Friedensforschung ein internationaler Workshop „Arms Control for Robots – Limiting Armed Tele-Operated and Autonomous Systems" statt, der diese Fragen aus unterschiedlichen Blickwinkeln untersuchte. Die internationale Teilnehmerschaft kam aus der Wissenschaft, vom Militär, aus der Politik und von international tätigen Organisationen. Am Anfang der Diskussionen stand eine Verständigung über den Ist-Stand und die Perspektiven autonomer und ferngelenkter Waffensysteme wie Drohnen oder Kampfroboter. Es wurde eine Einordnung dieser neuartigen Waffensysteme in



Wolfgang Coy

Prof. Dr. **Wolfgang Coy**, Professor für Informatik in Bildung und Gesellschaft an der Humboldt-Universität zu Berlin; Mitglied des FIfF-Beirats.

das bestehende internationale Recht versucht. Dies mündete in einem Aufruf zur Begrenzung und zum Verbot des unverantwortlichen Einsatzes solcher Systeme.

Bei den Teilnehmern des Workshops überwog die Einschätzung, dass wir es mit einer äußerst gefährlichen Waffenentwicklung zu tun haben, die keineswegs eine asymmetrische Feldüberlegenheit der technologisch führenden Staaten erzeugen wird, sondern kurz vor einer breiten Distribution in allen wesentlichen Armeen der Welt steht – wenn sie nicht jetzt durch internationale Übereinkunft geregelt und beschränkt wird. Eine gewisse Übereinkunft konnte darüber erzielt werden, dass selbsttätig agierende Robotersysteme ähnlich wie selbsttätig explodierende Munition einzustufen seien, also etwa wie mehr oder minder raffiniert programmierte Landminen, und dass ihre Herstellung und ihr Einsatz ebenso mittels internationaler Übereinkunft zu verbieten sei. Dies wurde in einem *„Statement of the 2010 Expert Workshop on Limiting Armed Tele-Operated and Autonomous Systems"* festgehalten, in dem eine Übereinkunft zur Kontrolle der Entwicklung, der Beschaffung, der Bereitstellung und des Einsatzes ferngesteuerter und autonomer Robotwaffen gefordert wird. Die folgenden Verbote werden gefordert:

– Further development, acquisition, deployment, and use of armed autonomous robot weapons.

– Arming new kinds of autonomous or tele-operated systems with nuclear weapons.

– The development, deployment, and use of robotic space weapons.

Des weiteren werden die folgenden Einschränkungen gefordert:

– The range and payload of armed tele-operated uninhabited vehicles.

– The number, by class and capability, of armed tele-operated uninhabited systems fielded by any state.

– The endurance of these systems.

– The development, acquisition, and deployment of weaponised uninhabited systems below a minimum size.

Als ein für Informatiker besonders relevantes Sonderthema jenseits der Rüstungskontrolle autonomer Systeme erwies sich die Frage nach den ethischen Dimensionen automatisch ablaufender Kampfhandlungen – verallgemeinert als „Roboter-Ethik" bezeichnet. Diese letzte Frage ist bereits Gegenstand zweier Bücher, deren Autoren auf dem Workshop anwesend waren.

Wendel Wallach, Ko-Autor des Buches *„Moral Machines – Teaching Robots Right from Wrong*, Oxford University Press, 2009" vertritt die Ansicht, Roboter seien im Prinzip so programmierbar, dass sie kontextabhängig durch Anwendung vorgegebener Regeln ethisch vertretbare Entscheidungen treffen können, „deren Ergebnis nicht fehlerhafter als das von Soldaten sei." Diese Gedanken folgen den literarischen Ansätzen Isaac Asimovs, der die berühmten *Drei Gesetze der Robotik* vor Jahrzehnten in einer Kurzgeschichte formuliert hat:

1. *A robot may not injure a human being or, through inaction, allow a human being to come to harm.*

2. *A robot must obey orders given it by human beings except where such orders would conflict with the First Law.*

3. *A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.*

Wendel Wallach und sein Ko-Autor Colin Allan zeigen sich dabei als SF-Leser, die Science, Fiction und Science Fiction wohl etwas durcheinander bringen – was in ihrer wissenschaftlichen Umgebung allerdings niemanden aufzufallen scheint. Anfangs fragen sie sich noch, ob ein regelgestützter Ansatz in ethischen Kontexten technisch umsetzbar sei („Whether Asimov's Three Laws are truly helpful for ensuring that robots will act morally is one of the questions we'll consider in this book") um am Ende eine pragmatisch-utilitaristische Antwort zu geben: „The unsolved problem of technology risk assessment is how seriously to weight catastrophic possibilities against the obvious advantages provided by new technologies." Die Argumentationen folgen dem bekannten KI-Schema des „noch nicht": „Wir können es zwar nicht und haben auch keine Ahnung, wie es gehen soll, aber das ist nur eine Frage der Zeit und vor allem der eingesetzten Mittel." Oder wie die Autoren es formulieren: „Some basic moral decisions may be quite easy to implement in computers, while skill at tackling more difficult moral dilemmas is well beyond present technology." Zum Beispiel die Interpretation des Kontextes – kein neues Problem der KI.

Die amerikanische Armee freilich unterstützt solche Forschungsansätze zur Herstellung von „software tools that are being exploited for the development of computer moral decision making" offenbar mit erheblichen Mitteln, und auch Oxford University Press hält die Überlegungen für wertvoll genug, um sie zu veröffentlichen.

Auch Ronald C. Armin, Autor des Buches *„Governing Lethal Behavior in Autonomous Robots"* (Chapman&Hall, 2009), nahm am Workshop teil. Er verfolgt ähnlich wie Wallace/Allan eine utilitaristische Linie und untersucht die Frage: „How to Represent Ethics in a Lethal Robot?" Seine Überlegungen münden in *Design Options* und *Prototype Implementations* für einen Killer Bot auf Basis eines ethischen *case-based reasoning*.

Die obskuren Thesen dieser Forschungsavantgarde waren im Workshop freilich nicht unbestritten. Sie blieben letztlich auch eher randständig.

Wie groß die Chancen für die erzielte Übereinkunft sind, muss sich freilich erst noch zeigen. Selbst ein Verbot der Landminen durch die 2006 ratifizierte Ottawa-Konvention ist bislang zwar von 156 Staaten ratifiziert, aber 39 Staaten, darunter zentrale Akteure wie Russland, China, Indien, Pakistan und die USA fehlen. Auch wenn alle Staaten unterschreiben, erreicht ein Verbot freilich keine nicht-staatlichen Akteure. Schließlich ist der Bau autonomer Roboter heutzutage schon Schulstoff. Dies sind düstere Aussichten also für diese Waffensysteme des einundzwanzigsten Jahrhunderts.

Nazir Peroz

Aufbau eines nachhaltigen und sicheren IT-Versorgungssystems für afghanische Hochschulen

Das Zentrum für internationale und interkulturelle Kommunikation (ZiiK) der TU Berlin *setzt sich seit 2002 für den Aufbau der akademischen Strukturen im Bereich Informationstechnologie (IT) in Afghanistan ein. Die Ziele sind:*

- *ein nachhaltiges und sicheres IT-Versorgungssystem für die afghanischen Hochschulen aufzubauen,*
- *Computer Science in der Lehre und Forschung zu etablieren,*
- *der Jugend eine neue Perspektive zu geben, und*
- *Afghanistan den Anschluss an die moderne Informationsgesellschaft zu ermöglichen.*

Die Aktivitäten zum Wiederaufbau der akademischen Strukturen in Afghanistan begannen mit einer ersten Delegation vom Auswärtigen Amt *und dem* Deutschen Akademischen Austausch Dienst (DAAD) *im März 2002. Die Strukturen an den Universitäten lagen zu diesem Zeitpunkt völlig brach. Die Bevölkerung war aber von einem beispiellosen Willen zum Neuanfang beseelt, es gab ein ungeheures Interesse der jungen Generation und ein Potenzial zur Friedenssicherung, alle waren bereit, sich für den Wiederaufbau zu engagieren.*

Dieser Beitrag beschreibt exemplarisch die aktuelle IT-Situation an afghanischen Hochschulen, was IT-Infrastruktur, IT-Ausbildung und Management betrifft. Der geschilderte Aufbau des Rechenzentrums an der Universität Kabul zeigt, wie ein solches Teilprojekt abläuft.

IT-Infrastruktur

An vielen afghanischen Universitäten fehlt es an den grundlegenden Voraussetzungen wie einer stabilen Stromversorgung, einer funktionalen Gebäudetechnik für den IT-Einsatz, soliden Netzwerkstrukturen und an bedarfsgerechten, zentralen Rechenzentren und dezentralen PC-Pools für die Fakultäten. Computersysteme sowie IT-Systeme und deren Dienste sind aber in hohem Maße abhängig von einer soliden Stromversorgung. Bislang wird der Strom vorrangig durch Generatoren gewonnen. Das ist eine ineffiziente Insellösung und wenig ökologisch. Eine flächendeckende Energieversorgung ist von großer Bedeutung.

Viele Gebäude und Räumlichkeiten an afghanischen Universitäten und deren Fakultäten sind nicht für den IT-Einsatz geeignet. Sie bieten keinen Schutz vor dem allgegenwärtigen Staub, vor Kälte, Hitze und Diebstahl. Daher müssen entweder neue Gebäude gebaut oder bestehende modernisiert werden.

IT-Ausbildung

Leider existieren im Bereich der IT-Ausbildung große Defizite in Afghanistan. Eine der Hauptursachen sind die mehr als 20 Jahre dauernden Kriege und Bürgerkriege, die das Bildungssystem und die gesamte Infrastruktur stark beeinträchtigt haben. In Afghanistan gibt es derzeit nur an den Universitäten Kabul und Herat Informatik-Fakultäten. Daher fehlen der afghanischen Gesellschaft Fachkräfte für die IT-Bereiche. Weil IT überall immer häufiger als Werkzeug für die Lehre und Forschung, die Verwaltung und für die Wirtschaft eingesetzt wird, kommt aber einer fundierten Ausbildung eine Schlüsselrolle zu.

Mindestens 2.000 bis 3.000 Arbeitsplätze müssen allein an der Universität Kabul mit Rechnern ausgestattet werden, damit die insgesamt etwa 10.000 Mitarbeiter und Studierenden der Universität Kabul sie für ihre vielfältigen Aufgaben nutzen können. Daraus resultiert ein großer Bedarf an kompetenten Fachkräften allein an den Universitäten – ohne Berücksichtigung weiterer Einsatzbereiche. Um dieser Herausforderung gerecht zu werden, ist ein bedarfsorientiertes Ausbildungskonzept nötig, das wiederum durch ein einheitliches IT-Curriculum getragen wird. Ergänzend zu dieser IT-Ausbildung ist eine spezielle Ausbildung für die IT-Verantwortlichen, IT-Beauftragten, IT-Sicherheitsbeauftragten, Netzwerk- und Systemadministratoren erforderlich.

Management

Die afghanischen Hochschulen brauchen eine starke Verwaltungsstruktur, die die IT-Versorgungssysteme der Hochschulen in der Lehre, Forschung sowie technischen Verwaltung nachhaltig unterstützt, modernisiert und koordiniert. Derzeit gibt es keine Koordinierungs- und Beratungsstelle oder Verantwort-

Nazir Peroz

Dr. **Nazir Peroz** ist gebürtiger Afghane und seit über 20 Jahren Dozent an der Fakultät Elektrotechnik und Informatik der TU Berlin im Bereich Informatik und Entwicklungsländer. Seit 2000 leitet er das Zentrum für internationale und interkulturelle Kommunikation. Außerdem ist er Sprecher der Fachgruppe Informatik und Dritte Welt der Gesellschaft für Informatik (GI).

liche, die sich beispielsweise um die Sicherheit der IT-Dienste kümmern.

Da das Versorgungssystem einer Hochschule keine statische Struktur ist, und die afghanischen Hochschulen sich ständig weiterentwickeln, ist an den Hochschulen eine begleitende Entwicklungsplanung nötig. Sie muss auch Gesichtspunkte wie Standardisierung, Datenschutz, die Folgen einer hochschulweiten Entwicklungsstrategie sowie die Anpassung des Versorgungssystems an die technische Entwicklung beachten.

Beitrag zum akademischen Wiederaufbau

Der *Deutsche Akademische Austausch Dienst* (DAAD) fördert mit Mitteln des Auswärtigen Amtes (Sonderprogramm *Stabilitätspakt Afghanistan*) den akademischen Wiederaufbau in Afghanistan. Im Mittelpunkt steht die Verbesserung der Qualität der Lehre durch die Curricula-Entwicklung, Dozentenfortbildung (Studienaufenthalte, Sommer- und Winterakademien, deutsche Gastdozenturen in Afghanistan, Schulungen vor Ort) in ausgewählten Schwerpunktfächern, zu denen auch die Informationstechnologie gehört. Hier werden neben den vorgenannten Maßnahmen auch der Aufbau von Rechenzentren und die Entwicklung einer nationalen IT-Strategie für das Hochschulwesen in Afghanistan angestrebt. Die *Lehrerausbildung* und die *Administratorenschulung* bilden die Grundlage für ein nachhaltiges IT-Versorgungssystem. Die folgenden konkreten Projekte wurden vom Team des ZiiK umgesetzt:

- Errichtung eines modernen Rechenzentrums an der Universität Kabul (ITCK) im Jahr 2003,
- Ausbildung von Mitarbeitern am ITCK, die als Multiplikatoren über 2000 Universitätsangehörigen der Universität Kabul Grundlagenkenntnisse im Umgang mit PCs vermittelt haben,
- Aufbau einer Informatik-Fakultät im Jahr 2004 an der Universität Herat sowie Unterstützung der Lehre an dieser Fakultät,
- Entwurf eines einheitlichen IT-Curriculums für Afghanistan,
- Aufbau und Vernetzung weiterer Fakultätsnetzwerke, um IT in Lehre und Forschung fachspezifisch nutzbar zu machen,
- Aufbau von Informatik-Bibliotheken[1] an der Universität Kabul und der Universität Herat,
- Aufbau eines PC-Workshops mit dem Ziel, alte Rechner funktionsfähig zu machen und die afghanischen Studierenden für eine umweltschonende Entsorgung zu sensibilisieren,
- Organisation und Durchführung von Winter- und Sommerakademieprogrammen sowie
- Organisation und Durchführung von Workshops und internationalen Konferenzen.

Der Erfolg dieser Maßnahmen, die Erfahrungen in diesem Bereich sowie der nach wie vor bestehende Mangel an hochqualifizierten Informatik-Dozenten an afghanischen Universitäten haben die Weltbank im Jahr 2007 veranlasst, ein Masterprogramm für 25 Dozenten (Frauen und Männer) aus sechs verschiedenen Universitäten Afghanistans an der Fakultät IV – Elektrotechnik und Informatik – der TU Berlin für zunächst zwei Jahre zu finanzieren.

Die Masterabsolventen kamen aus den sechs afghanischen Universitäten Kabul, Politechnische Universität Kabul, Universitäten Herat, Balkh, Kandahar und Nangarhar. Sie wurden an der TU Berlin ausgebildet und sind seit ihrem Studienabschluss im März 2010 als Dozenten an ihren Heimatuniversitäten tätig. Damit fungieren sie als Multiplikatoren für eine Informatik-Ausbildung auf internationalem Niveau.

Dieses *Sonderprogramm* wurde als Pilotprojekt konzipiert und verzeichnet inzwischen deutlich sichtbare Erfolge, so dass das Auswärtige Amt die Finanzierung eines weiteren Masterprogramms übernommen hat. In diesem Wintersemester wird es beginnen, die ersten Studierenden werden Ende Dezember 2010/Anfang Januar 2011 eintreffen.

Errichtung eines Rechenzentrums an der Universität Kabul

Das Rechenzentrum an der Universität Kabul (ITCK) bildet das Herzstück des Universitätsnetzwerks, welches grundlegende Dienste und Ressourcen zur Verfügung stellt und die Steuerung des IT-Versorgungssystems an der Universität Kabul übernimmt. Das ITCK ist das Kompetenzzentrum für alle IT-Angelegenheiten der Universität. Die afghanischen Netzwerkadministratoren des ITCK stehen als zentrale Ansprechpartner für alle Fakultäten und Einrichtungen bei Fragen der Versorgung im Bereich IT zur Verfügung.

Die Idee für diese Einrichtung entstand im März 2002, die Vorbereitung und die Planung im September 2002. Am 26. März 2003 fand die feierliche Übergabe des Rechenzentrums mit 55 modernen Arbeitsplätzen, Internetanschluss und Sprachlaboren statt.

Über die damit zusammenhängenden Vorbereitungen wie Analyse der Situation vor Ort, technische Planung, Beschaffung der Hardwareausstattung, Installationen, Umbaumaßnahmen, Stromversorgung, Regelungen für das ITCK, Internetanschluss, Design, Betriebskosten, Eröffnung und das Ausbildungskonzept wird im Folgenden berichtet:

Vorbereitung und Planung

Für die Einrichtung des ITCK stellte der Präsident der Universität Kabul einen großen Raum zur Verfügung. Aus- und Umbaumaßnahmen wie Abtrennungen der Wände, Decken und Säulen der Räume, Sanierung der Räume, Einbau von Gittern an den Fenstern wurden vor Ort mit Unterstützung durch das Technische Hilfswerk (THW) durchgeführt. An der TU Berlin begann zeitgleich die Entwicklung der technischen Konzepte zur Realisierung des ITCK, wie Spezifikationen der Hard- und Software, Installation und Transport der Hardware nach Kabul. Hier ein bebilderter Überblick über das systematische Vorgehen beim Aufbau des ITCK:

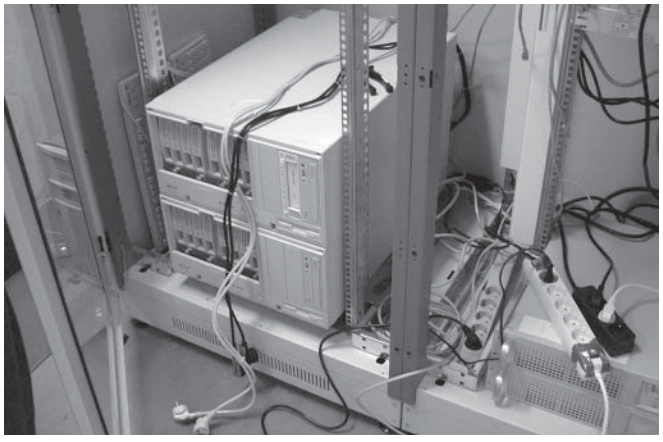
a) Analyse der Situation vor Ort

März 2002: Besuch des ZiiK-Teams an der Universität Kabul im Rahmen der ersten DAAD-Delegation.

Die Gebäude der Universität haben weder Strom noch Wasser. Während manche Gebäude durch Beschuss zerstört wurden, wurden andere nach und nach demoliert und geplündert, indem etwa Kabel aus den Wänden gerissen wurden, um Kupferdrähte zu gewinnen, oder Türen ausgehängt, um sie als Brennholz zu verwenden.

b) Technische Planung

Raumeinteilung: Für den insgesamt 260 qm großen Raum wurde ein Konzept zur Raumeinteilung entwickelt und umgesetzt.



Serversystem

Die Anforderungen an das Serversystem bestanden im Wesentlichen aus der Speicherung großer Datenmengen, auf die von den PCs über das Netzwerk zugegriffen wird. Eine zuverlässige, schnelle Netzwerkinfrastruktur und sichere Datenspeicher mit genügend Kapazitäten waren nötig. Dienste wie Internetanbindung, Benutzerkontenverwaltung, Datensicherung etc. sind Bestandteil des Konzepts.

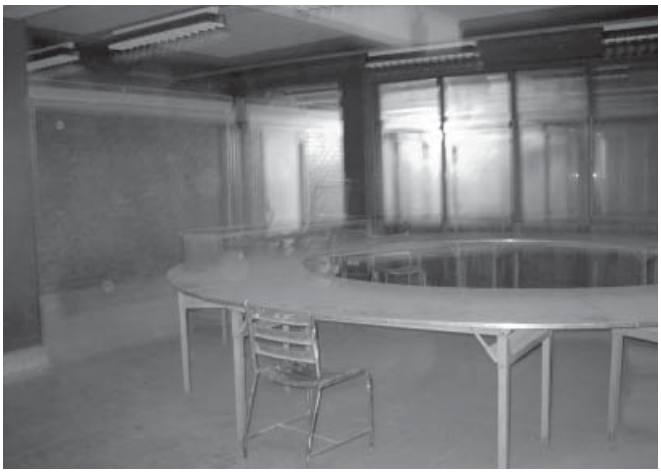
c) Beschaffung der Hardwareausstattung

Wahl der Hard- und Software: Für die Arbeitsplätze wurden Standard-PCs beschafft, einige Komponenten wurden durch besonders robuste Hardware ersetzt, wie z.B. Grafikkarten, Lüfter und Netzteile für den Einsatz unter extremen klimatischen Bedingungen und bei hohem Staubaufkommen. Tastaturen mit persischem Layout wurden beschafft.

Die Arbeitsplatz-PCs wurden mit Windows und die Server mit Linux-Betriebssystemen installiert. Das Konzept bevorzugt Open-Source-Software, aus Gründen der Nachhaltigkeit und Unabhängigkeit für die Lehre.

d) Umbaumaßnahmen und Zeitplan

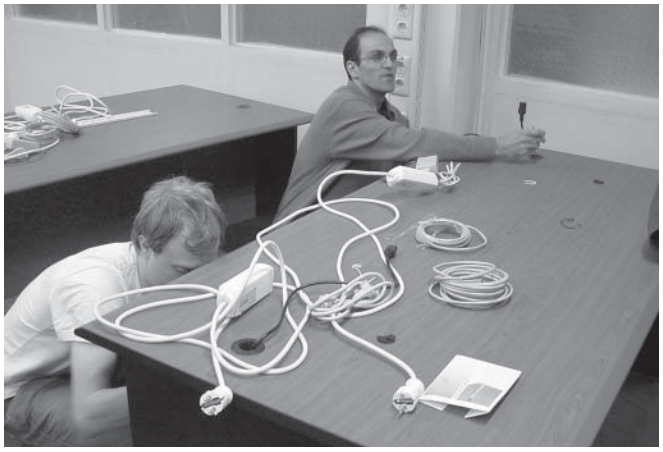
Die Aufräumarbeiten, Umbaumaßnahmen und die Einrichtung der Räume fanden im Zeitraum von 2. Januar bis zum 14. März 2003 statt. Gleichzeitig wurde mit Unterstützung durch das THW die Strom- und Netzwerkverkabelung installiert.



Raum am 2.1.2003

Raum am 3.2.2003

Raum am 24.2.2003

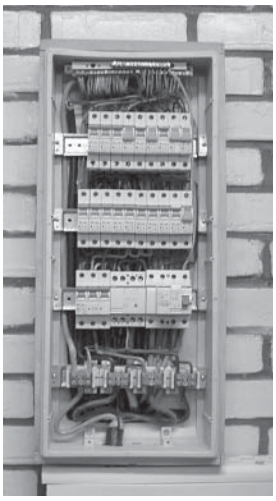


Raum am 2.3.2003

Raum am 14.3.2003

f) Notlösung für die Stromversorgung

Da in Kabul keine kontinuierliche Stromversorgung gewährleistet werden konnte, wurde als Übergangslösung ein Generator angeschafft. Unterbrechungsfreie Stromversorgungen (USVs) sorgen für eine Überbrückung kürzerer Ausfälle und bei Stromschwankungen.



g) Regelungen für die Nutzung des ITCK

Aus Sicherheitsgründen wurde eine Benutzerordnung aufgestellt.

h) Internetanschluss

Eine private Firma richtete eine Satellitenverbindung ein.

i) Design

Ein *corporate design* für das ITCK wurde entwickelt und für Desktop-Hintergründe, Präsentationen, Schilder etc. verwendet.

j) Betriebskosten

Der DAAD übernahm die Kosten für Öl und Wartung des Generators, Internetanschluss, Ausbildungsmaterialien, Gehälter

für das afghanische Personal wie IT-Manager, IT-Techniker, IT-Webmaster, Dozenten, Tutoren, Fahrer und Reinigungskräfte.

k) Eröffnung

Am 26. März 2003 wurde das ITCK eröffnet mit insgesamt 55 PCs, einer flächendeckenden Vernetzung aller Rechner, einem modernen und leistungsfähigen Serversystem sowie umfangreicher Standardsoftware und einem pädagogischen Konzept für die Aus- und Weiterbildung im Bereich IT an der Universität. Jetzt bestand die Möglichkeit zur Kommunikation mit der Weltgemeinschaft. Das ITCK ist gerüstet für die Anforderungen der neuen Lehrpläne und Ausbildungsprogramme. Die Fotos zeigen den damaligen Präsidenten der Universität Kabul, Prof. Popal, und die Gäste.

Schlussbetrachtung

Das ITCK besteht nun seit neun Jahren. Durch das gut durchdachte und nachhaltige Konzept ist das ITCK bis heute ein Vorzeigeprojekt an der Universität Kabul.

Während der ersten Jahre wurde der Betrieb des ITCK vom Team des ZiiK betreut und sichergestellt. Mittlerweile wurden mehrere Generationen von IT-Administratoren sowohl vor Ort in Kabul als auch an der TU Berlin ausgebildet, so dass der Betrieb seit 2006 komplett von afghanischer Seite übernommen werden konnte. Damit hat das Team des ZiiK einen langen Atem bewiesen und einen Beitrag zur nachhaltigen IT-Versorgung an der Universität Kabul geleistet. Seit 2003 wurden über 2000 Universitätsangehörige am ITCK aus- und weitergebildet.

Anmerkungen

1 *An dieser Stelle möchte ich mich herzlich bei Peter Bittner und anderen Mitgliedern der FIfF bedanken. Durch ihre Spenden von Informatikbüchern haben sie die Bibliotheken unterstützt.*

Fotos von Nazir Peroz

Susanne Boll, Rolf Meinhardt (†), Sabine Gronewold, Larissa Krekeler

Mit Information über Integration zur Informatik

Studienprogramm „Informatik für Migrantinnen und Migranten“

Das Fehlen qualifizierter Fachkräfte auf dem Arbeitsmarkt und die Integration von Migranten in Deutschland haben zu vielen Diskussionen geführt, aber noch keine ausreichenden Lösungen erbracht. Dieser Artikel beschreibt einen praktikablen Weg zur Umsetzung eines Konzepts für die Qualifizierung akademischer Migranten am Beispiel eines Studienprogramms in Informatik an der Universität Oldenburg.

Warum ein Studienprogramm Informatik für Migranten?

Nach Recherchen des Instituts der deutschen Wirtschaft Köln (IW) fehlen in Deutschland 65.000 MINT-Fachkräfte (Mathematiker, Informatiker, Naturwissenschaftler und Techniker). Dabei sind insgesamt 2,8 Millionen Migranten fertig ausgebildet nach Deutschland gekommen: Die Akademiker unter ihnen hatten mehrheitlich schon zu mindestens 60% ihr Studium absolviert, die Fachkräfte kamen zu 44% mit einem Berufsabschluss nach Deutschland [I09]. Allerdings gibt es deutliche Schwierigkeiten bei der Anerkennung der im Ausland erworbenen Abschlüsse und damit einhergehend Probleme, in den Arbeitsmarkt einzutreten. Zentrale Ursache ist die geringe Anerkennung der Abschlüsse: etwa 65 % der Anträge werden abgelehnt. Obwohl keine flächendeckenden Studien vorliegen, lassen einzelne Erhebungen einen Schluss auf einen echten Bedarf an der Integration hochqualifizierter Migranten zu. Etwa 5-10% der Aussiedler und knapp 20% der Flüchtlinge haben einen akademischen Abschluss; 70-80% der jüdischen Immigranten aus der ehemaligen Sowjetunion haben eine akademische Ausbildung [M08]. Nach Schätzungen der Universität Oldenburg leben eine halbe Million ausländischer Fachkräfte in Deutschland, deren Abschlüsse größtenteils nicht anerkannt sind. Auch Staatsministerin Maria Böhmer (Beauftragte der Bundesregierung für Migration, Flüchtlinge und Integration) beziffert im November 2009 das Potenzial mit „mehreren hunderttausend qualifizierten Zuwanderern aus verschiedensten Berufen“ [P09].

Allerdings bleibt auch nach Anerkennung der Abschlüsse eine Hürde bei der Integration in den Arbeitsmarkt: Arbeitgeber können die Qualifikation der ausländischen Abschlüsse, die teilweise auch schon einige Zeit zurückliegen, oft nicht einschätzen. Bisher liegen zwar kaum gesicherte Erkenntnisse darüber vor, welche Qualifikationsprofile höher qualifizierte Migranten in Deutschland aufweisen und in welchem Maße ihre mitgebrachten Qualifikationen anerkannt werden. Dennoch zeigen Studien, dass Verfahren zur Anerkennung mitgebrachter Abschlüsse und ressourcenorientierte Qualifizierungsmaßnahmen zu einer verbesserten beruflichen und sozialen Integration führen. Der im Jahr 2006 an der Universität Oldenburg eingerichtete Weiterbildungsstudiengang „Interkulturelle Bildung und Beratung“ mit dem Abschluss *Bachelor of Arts* zeigte bereits, dass die besondere Motivation der Absolventen darin besteht, dass sie einen *normalen*, in ganz Europa anerkannten und berufsbefähigenden Abschluss erhalten [M10]. Viele Migranten haben zuvor bereits Zertifikate im Inland und Ausland erworben, aber bisher keinen formalen oder anerkannten Abschluss. Damit entsteht die besondere Herausforderung der Integration von hochqualifizierten Migranten, bei der sowohl die bereits erworbenen Qualifikationen als auch die Anforderungen des deutschen Arbeitsmarktes Berücksichtigung finden. Da zum einen eine vollständige Anerkennung und Integration in den Arbeitsmarkt nicht gelingt, zum anderen aber eine Vielzahl von relevanten Vorkenntnissen vorhanden ist, stellt sich die Frage, wie ein Studienkonzept in der Informatik aussehen kann, das die Migranten in ihrer jeweiligen Bildungs- und Lebensbiographie abholt und ihnen einen zügigen Weg in den Arbeitsmarkt für Informatikerinnen und Informatiker bietet.

Aus diesem Grund wurde im Jahr 2008 an der Carl-von-Ossietzky Universität, unterstützt vom Niedersächsischen Ministerium für Inneres, Sport und Integration, das Studienprogramm „Informatik für Migrantinnen und Migranten“ entwickelt. Das Studienprogramm berücksichtigt die besondere Situation der Migranten. Diese haben oft zwar ein sehr gutes fachliches Fundament im Bereich der theoretischen, formalen und mathematischen Methoden, es fehlen jedoch aktuelle, praxisorientierte Themen der Informatik wie Programmiersprachen oder modernes Software-Engineering, um auf dem deutschen Arbeitsmarkt trotz des derzeit herrschenden Fachkräftemangels die passende Qualifikation anbieten zu können. Da, wie bereits erwähnt, eine vollumfängliche Anerkennung eines vorangehenden Studiums oft nicht gelingt, prüft das Studienprogramm individuelle mögliche Anerkennungen, um eine gute Balance zwischen dem bestehenden Vorwissen und den wettbewerbsfähigen, neu zu erwerbenden oder aufzufrischenden Kenntnissen und Fertigkeiten in Informatik für den deutschen Arbeitsmarkt herzustellen.

Lebens- und Lernsituation von Migrantinnen und Migranten

Die Migranten leben meist in einer anderen Situation als inländische Studierende nach dem Schulabschluss. Das Alter der in Frage kommenden Studierenden liegt zwischen 25 und 45; sie sind zu einem großen Teil verheiratet und haben Kinder; der bisherige Wohnort ist deutschlandweit verteilt mit Schwerpunkten in Ballungsräumen. Die Erfahrungen aus den bisherigen Studienangeboten des IBKM zeigen eine außerordentlich hohe Lernbereitschaft und ungeheure Motivation der Einwanderer, einen anerkannten Studienabschluss zu erreichen. Die Lernvoraussetzungen sind gleichzeitig sehr heterogen, aber durchaus als gut einzustufen. Der Beratungsbedarf und der Wunsch nach Erfahrungsaustausch und Kommunikation sind allerdings gerade für diese Studierendengruppe enorm hoch. Es besteht eine große Notwendigkeit zur Begleitung bei der Erstellung wissenschaftlicher Arbeiten und bei diskursorientiertem Lernen. Ein Studi-

enprogramm Informatik für Migrantinnen und Migranten muss demnach auf diese besondere Situation eingehen und die Studierenden geeignet unterstützen.

Wie eine explorative Studie des IBKM über hoch qualifizierte Einwanderer ergab, wies die Gruppe der 260 befragten Probandinnen und Probanden in Niedersachsen eine sehr hohe Arbeitslosigkeit (67%) auf; 11% waren lediglich in Honorar-, Teilzeit- oder 400-Euro-Jobs tätig. Die Mehrzahl dieser Gruppe ist in hohem Maß von Armuts- und Unterversorgungsrisiken betroffen. Die weitaus größte Zahl von ihnen war in ihren Herkunftsländern berufstätig (86 %), viele von ihnen in Arbeitsbereichen, für die sie sich durch ein Studium qualifiziert hatten (72%). Vor diesem Hintergrund wird das ganze Ausmaß an beruflicher und sozialer Deklassierung dieser Einwanderer deutlich [P09]. Die Ergebnisse der Oldenburger Untersuchung wurden durch die breit angelegte empirische Studie „Brain Waste“ eindrucksvoll bestätigt [E07].

Universitäre Studienangebote, die die Potenziale von Migrantinnen und Migranten so aufnehmen und weiterentwickeln, dass sie den Strukturen und Anforderungen des deutschen Arbeitsmarktes entsprechen, können die Vermittlungschancen nachhaltig erhöhen. Das zeigen Beispiele aus dem weiterbildenden Bachelor-Studiengang „Interkulturelle Bildung und Beratung“ an der Universität Oldenburg [M10].

Das Studienprogramm „Informatik für Migranten“

Zum Wintersemester 2008/2009 wurde ein Studienprogramm „Informatik für Migrantinnen und Migranten“ als Beratungs- und Betreuungsangebot für Migranten eingerichtet, die bereits in ihrem Heimatland ein Studium absolviert haben, um ihnen durch ein weiterqualifizierendes Studium einen in Deutschland anerkannten und berufsfähigen Abschluss zu ermöglichen. [S10]. Die Teilnehmenden an dem Studienprogramm können einen der Studiengänge der Informatik auswählen:

- Fach-Bachelor Informatik,
- Fach-Bachelor Wirtschaftsinformatik,
- Zwei-Fächer Bachelor Informatik,
- Fach-Master Informatik,
- Fach-Master Wirtschaftsinformatik,
- Fach-Master Eingebettete Systeme und Mikrorobotik,
- Master of Education mit Fach Informatik.

Die Wahl des Studienganges richtet sich einerseits nach der mitgebrachten Qualifikation, andererseits aber auch nach dem Interesse der Studierenden. Teilnehmer im Studienprogramm sind als reguläre Studierende Mitglieder der Universität Oldenburg und haben deshalb auch die anfallenden Semester- und Studienbeträge zu übernehmen.

Vorhandene akademische und berufliche Leistungen werden nach Möglichkeit für das Bachelor- bzw. Masterstudium angerechnet und führen so zu einer Verkürzung der Studienzeit. Fehlende bzw. veraltete Kompetenzen werden über das Studium aufgefrischt bzw. neu erworben. Die Besonderheit des Studienangebotes ist also nicht etwa ein speziell auf die Anforderungen von gut ausgebildeten Migranten gerichtetes Profil, sondern die individuell zugeschnittene Studienplanung und -begleitung. So können die Migranten ihre bisherige Ausbildung gezielt verwenden und ihr Potenzial zielgerichtet ausschöpfen. Sie werden dabei durch intensive Betreuung und individuelle Beratung und Studienplanung unterstützt. Für den Aufbau und die Einführung des Studienprogramms „Informatik für Migrantinnen und Migranten“ war die Konzeption und Umsetzung einer Reihe von Bausteinen notwendig, die im Folgenden kurz vorgestellt werden.

Bewerbung und Aufnahme

Voraussetzung für eine Bewerbung um einen Platz im Studienprogramm ist eine Zulassung zum Universitätsstudium in

Deckblatt des Flyers in russischer Sprache

Deutschland auf Grund eines Hochschulstudiums oder eines Teilstudiums an einer ausländischen Hochschule/Universität. Die Bewerbenden durchlaufen als angehende Studierende der Universität Oldenburg, den *regulären* Weg bis zur Immatrikulation: Sie müssen das für ein Studium an einer deutschen Hochschule notwendige Sprachniveau und eine erfolgreiche Prüfung der Bewerbungsunterlagen durch die Arbeits- und Servicestelle für Internationale Studienbewerbungen e.V. (uni-assist) in Berlin nachweisen. Schon in der Phase der Bewerbung um einen Studienplatz findet eine Betreuung der Teilnehmer durch das Studienprogramm statt. In enger Zusammenarbeit der Mitarbeiterinnen des Studienprogramms mit den zuständigen Instanzen der Universität, wie dem Immatrikulationsamt, dem Sprachenzentrum, ISO (Institute Studies Office), Prüfungsamt und Studentenwerk konnten die Abläufe optimal gestaltet werden.

Anerkennung und Anrechnung

Die zentrale Motivation für hochgebildete Migranten liegt darin, einen anerkannten Studienabschluss in Deutschland zu erlangen und gleichzeitig ihre bisherigen Fachkenntnisse in das Studium einzubringen. Aufgrund unterschiedlicher Lebensläufe der Migranten entsteht der Bedarf, Kenntnisse aufzufrischen, zu aktualisieren und zu ergänzen. Die Prüfungsordnungen der Universität Oldenburg sehen Regelungen vor, nach denen Leistungen anerkannt werden, die an ausländischen Hochschulen erbracht wurden. Darüber hinaus erlaubt die Prüfungsordnung, die Anerkennung von „außerhalb des Studiums abgeleisteten Prüfungsleistungen". Die konkrete Anrechnung der Leistungen erfolgt über den Prüfungsausschuss Informatik. In der aufwändigen Vorbereitung der Anrechnung und Überprüfung der Gleichwertigkeit wird der Prüfungsausschuss durch die Mitarbeiterinnen im Studienprogramm unterstützt. Der Katalog der anzurechnenden Vorkenntnisse wird dem Prüfungsausschuss Informatik vorgelegt, der die Anrechnung durchführt. Die Studierenden schreiben sich zunächst für das erste Fachsemester der Bachelor- bzw. Master-Studiengänge ein und werden nach einer Anrechnung in das entsprechende Fachsemester hochgestuft.

Erstellung eines individuellen Studienplanes

Das Studium der Informatik ist modular organisiert[1] und für die einzelnen Module werden Kreditpunkte als Maßeinheit für den Arbeitsaufwand vergeben. Daraus resultiert ein optimaler Studienplan, der inhaltliche Abhängigkeiten und Restriktionen beinhaltet. Eine individuelle Planung des Studiums ist zwar möglich, verlangt aber die sorgfältige Beachtung dieser Abhängigkeiten, damit das Studium organisatorisch und zeitlich optimal gestaltet wird. Zur Anrechnung des Studiums oder von Teilen im Heimatland ist es notwendig, die Studienpläne individuell zu gestalten und an die jeweiligen Bedürfnisse anzupassen. Nach ausführlicher Prüfung der Unterlagen wird ein Studienplan in Abstimmung mit den Wünschen der Studierenden erstellt, der die fehlenden Module bis zum angestrebten Abschluss und somit einen sinnvollen Studienverlauf beschreibt. Dieser Plan wird im weiteren Studium von Semester zu Semester bedarfsweise aktualisiert und angepasst.

Zusatzveranstaltungen

Neben der Anerkennung von Vorkenntnissen werden für das Studienprogramm ergänzende Fachkurse entwickelt und angeboten. Diese dienen dazu, die fachlichen Kompetenzen der Studierenden zu stärken und anerkannte Vorkenntnisse in den verschiedenen Grundlagen der Informatik aufzufrischen und zu aktualisieren. Die Kurse werden nach Bedarf der Teilnehmenden am Programm angeboten. Das Angebot umfasst insbesondere Bereiche der technischen Grundlagen der Informatik und Programmierung, der Mathematik für Informatik, der Fachsprache sowie auch Vorbereitungskurse auf den Schuldienst speziell für Lehramtsstudierende.

Beratung und Betreuung der Studierenden

Dem Studienbeginn geht eine intensive Beratungsphase voraus, an die sich eine betreuende Begleitung im weiteren Studienverlauf anschließt. In der individuellen fachlichen Beratung, verbunden mit der Anrechnung der Leistungen und der Studienverlaufsplanung, werden zum Studienbeginn sämtliche organisatorischen Fragen geklärt und grundlegende Informationen zum Studium an der Universität Oldenburg vermittelt. Die Studierenden können außerdem an allen einführenden Studienveranstaltungen teilnehmen, die im Department für Informatik für die Studienanfänger angeboten werden: Zu Beginn des Wintersemesters (eine Woche vor Vorlesungsbeginn) finden im Rahmen einer Orientierungswoche Veranstaltungen für alle Studierenden der Informatik und Wirtschaftsinformatik statt, in der vielfältige Informationen bezüglich der Struktur der Universität, ihrer vielfältigen Einrichtungen und Freizeitmöglichkeiten, des Studiums und der Studienorganisation vermittelt werden. Dabei bieten sich gute Möglichkeiten, andere Studierende und Lehrende direkt zu Studienbeginn kennenzulernen. Seit einigen Jahren werden ebenfalls im Wintersemester Sozialtutorien (Ersti-Tutorien) angeboten, um die Studienanfänger in der Eingewöhnungsphase im Studium zu unterstützen. Ein wichtiger Aspekt dieser Tutorien ist das Kennenlernen von Kommilitonen, was nicht selten in die Bildung studienbezogener Arbeitsgruppen mündet. Eine Teilnahme an diesen Tutorien ist für die Studierenden des Studienprogramms zur Eingewöhnung in das Studium sehr hilfreich, damit sie frühzeitig in Arbeitsgruppen mit deutschen Kommilitonen integriert werden können.

Nach dieser Einführungsphase werden die Studierenden im Rahmen des Studienprogramms über regelmäßige wöchentliche Treffen weiter begleitet. Diese Treffen bieten die Möglichkeit, Fragen zum Studium zeitnah zu klären, bei auftretenden Problemen zu beraten und zu vermitteln, Begleitmaterialien zum Studium bereitzustellen, den Studienfortschritt zu überwachen und die Studierenden zu motivieren.

Finanzierung

Das Studienprogramm ist auf eine Aufnahme von maximal 20 Studierenden p.a. ausgelegt. Die Auswahl und Begleitung dieser Studierenden geschieht durch zwei Wissenschaftliche Mitarbeiterinnen, die sich eine Vollzeitstelle teilen. Sie übernehmen die Aufgaben zur Auswahl und Aufnahme der Studierenden und

die Entwicklung der individuellen Studienpläne. Außerdem entwickeln sie parallel zum Aufbau des Studiengangs ein Konzept für zusätzliche Module, die für die Migranten ggf. eine Auffrischung von Grundkenntnissen in Mathematik, technischer und theoretischer Informatik und Einführung in Pädagogik für Migranten ermöglichen, ohne dass sie dafür ein ganzes Modul (im Semester) investieren müssen. Die Einrichtung und Durchführung des Studienprogrammes „Informatik für Migrantinnen und Migranten" wird vom Ministerium für Inneres, Sport und Integration (seit 2010 das Ministerium für Soziales, Frauen, Familie und Gesundheit und Integration (MS)) des Landes Niedersachsen seit dem Wintersemester 2008/2009 gefördert.

Erste Erfahrungen mit dem Studienprogramm

Das Studienprogramm Informatik für Migrantinnen und Migranten ist im Wintersemester 2008/2009 mit vier Studierenden gestartet. In den letzten zwei Semestern wurden insgesamt 19 weitere Teilnehmer aufgenommen, so dass aktuell elf Studierende im Vorsemester *Deutsch*, einer im Bachelor-Studiengang Wirtschaftsinformatik, drei im Bachelor-Studiengang Informatik, eine im Zwei-Fächer-Bachelor Informatik, eine im Master-Studiengang Wirtschaftsinformatik, eine im Bachelor-Studiengang Lehramt für Gymnasium mit Fächerkombination Informatik und Spanisch und eine für Informatik und Mathematik studieren. Drei Studierende haben in der Zwischenzeit ihr Studium wieder abgebrochen.

Die Teilnehmer stammen aus Russland und der Ukraine, aus dem Irak, der Türkei, Argentinien und Venezuela. Das Alter der Studierenden liegt zwischen 28 und 46 Jahren. Die Studierenden sind zu einem großen Teil verheiratet und haben Kinder. Die Minderheit der Teilnehmer wohnt direkt in Oldenburg, die Wohnorte der meisten Studierenden liegen bis zu 100 km von Oldenburg entfernt.

Bisher gab es weitaus mehr Interessenten und aussichtsreiche Bewerbungen für das Studienprogramm, als es die Zahl der derzeitigen Studierenden widerspiegelt. Insbesondere finanzielle Gründe (Studiengebühren sowie fehlende Finanzierungsmöglichkeiten der Lebenshaltungskosten während des Studienverlaufs) und Sprachschwierigkeiten führten zu Absagen seitens der Bewerber.

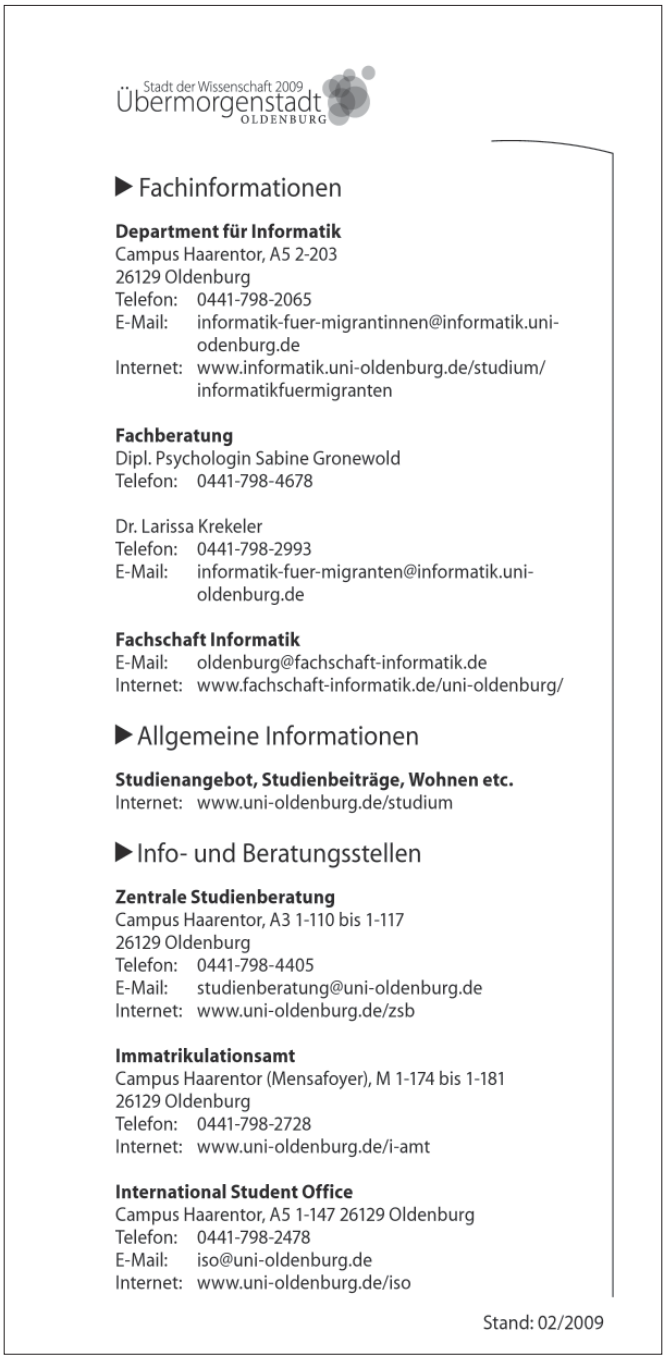
Susanne Boll, Rolf Meinhardt, Sabine Gronewold und Larissa Krekeler

Prof. Dr. **Susanne Boll** ist Professorin im Department für Informatik der Universität Oldenburg. Sie ist Leiterin der Abteilung Medieninformatik und Multimedia-Systeme. Seit 2002 ist sie auch Mitglied im OFFIS – Institut für Informatik und leitet dort als Bereichsvorstand in den Bereichen Gesundheit und Transport eine Vielzahl von internationalen und nationalen Forschungsprojekten. Sie ist außerdem Sprecherin des Technologie-Cluster Mensch-Maschine Interaktion am OFFIS. Frau Boll hat gemeinsam mit Prof. Meinhardt das Studienprogramm Informatik für Migrantinnen und Migranten beantragt und umgesetzt.

Prof. Dr. **Rolf Meinhardt** († 14.5.2010) war Mitbegründer und Hochschullehrer am Interdisziplinären Zentrum für Bildung und Kommunikation in Migrationsprozessen (IBKM) an der Carl von Ossietzky Universität Oldenburg. Schwerpunkte in Forschung und Lehre: Sozial- und Bildungsarbeit mit Migrantinnen und Migranten. Leiter verschiedener Projekte (wie Dezentrale Flüchtlingssozialarbeit, Interkulturelle Qualifizierung von Lehrerinnen und Lehrer aus dem Kosovo, Kooperative Migrationsarbeit in Niedersachsen), Initiator der Kontaktstudiengänge „Interkulturelle Kompetenz in pädagogischen Arbeitsfeldern" und des weiterbildenden BA-Studienganges „Interkulturelle Bildung und Beratung" für hochqualifizierte Einwanderer. Seit 2008 leitete Meinhardt die Leit- und Koordinationsstelle „Studienangebote für hochqualifizierte Migrantinnen und Migranten an niedersächsischen Hochschulen".

Sabine Gronewold hat an der Carl-von-Ossietzky Universität Oldenburg Psychologie mit Nebenfach Informatik studiert und ist dort seit 2007 in verschiedenen Projekten beschäftigt. Aktuell arbeitet sie im Projekt Endspurt im Bereich der Studienberatung und Begleitung von Langzeitstudierenden und im Studienprogramm „Informatik für Migrantinnen und Migranten".

Larissa Krekeler: Wirtschaftsinformatikerin und Mathematikerin, hat an der Universität Lomonosov, Moskau studiert und promoviert. Berufserfahrung in Deutschland (seit 1992): Leitung der EDV und Controlling-Abteilung, HWK-Oldenburg; Mathematik- und Informatik-Lehrerin am Wirtschaftsgymnasium; Wissenschaftliche Mitarbeiterin, Department für Informatik, Uni Oldenburg. In der Lehre war sie als Dozentin für Mathematik und Informatik an der Hochschule für Angewandte Wissenschaft Hamburg, (2 Semester) im Fachbereich Medien & Design, Vorlesungen (3 Semester) Fachhochschule Oldenburg. Schwerpunkte: Didaktik für Informatik, Technische Informatik, Wirtschafts-und Finanzmathematik.



Stadt der Wissenschaft 2009
Übermorgenstadt
OLDENBURG

▶ Fachinformationen

Department für Informatik
Campus Haarentor, A5 2-203
26129 Oldenburg
Telefon: 0441-798-2065
E-Mail: informatik-fuer-migrantinnen@informatik.uni-odenburg.de
Internet: www.informatik.uni-oldenburg.de/studium/informatikfuermigranten

Fachberatung
Dipl. Psychologin Sabine Gronewold
Telefon: 0441-798-4678

Dr. Larissa Krekeler
Telefon: 0441-798-2993
E-Mail: informatik-fuer-migranten@informatik.uni-oldenburg.de

Fachschaft Informatik
E-Mail: oldenburg@fachschaft-informatik.de
Internet: www.fachschaft-informatik.de/uni-oldenburg/

▶ Allgemeine Informationen

Studienangebot, Studienbeiträge, Wohnen etc.
Internet: www.uni-oldenburg.de/studium

▶ Info- und Beratungsstellen

Zentrale Studienberatung
Campus Haarentor, A3 1-110 bis 1-117
26129 Oldenburg
Telefon: 0441-798-4405
E-Mail: studienberatung@uni-oldenburg.de
Internet: www.uni-oldenburg.de/zsb

Immatrikulationsamt
Campus Haarentor (Mensafoyer), M 1-174 bis 1-181
26129 Oldenburg
Telefon: 0441-798-2728
Internet: www.uni-oldenburg.de/i-amt

International Student Office
Campus Haarentor, A5 1-147 26129 Oldenburg
Telefon: 0441-798-2478
E-Mail: iso@uni-oldenburg.de
Internet: www.uni-oldenburg.de/iso

Stand: 02/2009

Auszug aus der deutschen Version des Flyers

Individuelle Studienplanung

Im Folgenden werden beispielhaft die Studienverlaufspläne zweier Teilnehmer des Programmes dargestellt und beschrieben. Die erste Studierende hat ihr Studium im Fach-Bachelor Informatik zum Wintersemester 2008/2009 mit der Auflage aufgenommen, die DSH-Prüfung innerhalb von zwei Semestern studienbegleitend nachzuholen und bringt ein fachfremdes Ingenieurstudium in ihr aktuelles Studium ein. Ihre Studienleistungen aus dem Erststudium im Heimatland lassen sich im Rahmen von neun Modulen (drei Mathematik-Module und sechs Nebenfach-Module) auf das Studium anrechnen. Es fehlen aktuell noch sechs Module aus dem Bereich Informatik, ein Praxismodul sowie die Abschlussarbeit, damit könnte das Studium voraussichtlich zum Ende des Sommersemesters 2011 beendet werden.

Die zweite Studierende im Master Wirtschaftsinformatik hat ihr Studium ebenfalls zum Wintersemester 2008/2009 aufgenommen. Sie hat in Russland Diplom-Wirtschaftswissenschaften studiert und in Deutschland eine Ausbildung im kaufmännischen sowie einige Fortbildungen im IT-Bereich absolviert. Ihre Studienleistungen aus dem Erststudium im Heimatland konnten leider nicht auf das Studium angerechnet werden, so dass sie in ihrem Studium insgesamt elf Module, eine Projektgruppe sowie die Master-Abschlussarbeit absolvieren muss. Inzwischen hat sie alle Module bis auf die Master-Abschlussarbeit erfolgreich absolviert, so dass sie ihr Studium voraussichtlich gegen Ende des WS 2010/2011 erfolgreich beenden wird.

Die beiden Studienpläne zeigen zwei unterschiedliche Studienverläufe, abhängig von der mitgebrachten Qualifikation. Während die Studierende im Fach-Bachelor Informatik zwar mit ingenieurwissenschaftlichem Background, aber bezogen auf die Informatik fachfremd, ins Studium eingestiegen ist, hat die Studierende im Master Wirtschaftsinformatik in relativ kurzer Zeit eine Art Weiterbildungsstudium absolviert. Beide werden in Kürze ihr Studium abschließen und in den Arbeitsmarkt als qualifizierte Fachkraft eintreten.

Beratung und Begleitung - Erfahrungen im ersten Durchgang

In der Startphase des Projekts wurde festgestellt, dass der Beratungsbedarf für die Gruppe der Studierenden mit Migrationshintergrund sehr hoch ist. Die Studierenden waren unerfahren und unsicher im deutschen Studiensystem und hatten einen großen Unterstützungsbedarf. Die Integration der Studierenden in die Studiengänge der Informatik konnte daher nur sehr langsam stattfinden: Die Teilnehmer orientierten sich nur schwer und fanden daher schlecht Anschluss an die Gruppe der übrigen Studierenden. Hinzu kamen sprachliche Schwierigkeiten: Durch fehlende Deutsch-Kenntnisse konnten Texte (insbesondere Übungszettel und Klausuren) nur mit Mühe und großem Zeitaufwand bearbeitet werden. Auch das geringe Sprachverständnis für die Fachsprache verursachte Probleme. Eine intensive Begleitung der Studierenden insbesondere in der Anfangsphase des Studiums erwies sich daher als unbedingt notwendig. Ein Netz von Maßnahmen wurde zu diesem Zweck installiert: Als Erste-Hilfe-Maßnahme wurde ein "Nachhilfetutor" eingestellt, der die Studierenden fachlich individuell im ersten Semester begleitete. Außerdem wurden die Studierenden motiviert, regelmäßig an den "Ersti-Tutorien" (Sozialtutorium) teilzunehmen. Das Angebot der Deutsch-Kurse wurde speziell im Basisbereich verstärkt. Zudem fand eine umfangreiche Betreuung der Studierenden durch die Mitarbeiterinnen des Studienprogrammes in Form einer Begleitung und allgemeinen Beratung rund um das Studium statt. Nach einer Eingewöhnungszeit wurden dann zusätzliche Ergänzungskurse im Bereich Informatik und Mathematik angeboten. Zum Ende des Sommersemesters 2009 fand ein Propädeutikum zum Modul "Programmierkurs Java" statt und in den Semesterferien nach dem Wintersemester 2009/10 wurde ein *Auffrischungskurs* Mathematik angeboten. Diese Kurse hatten, neben der Auffrischung von Fachkenntnissen und

dem *Vertraut machen* mit den deutschen Fachbegriffen, zudem den Vorteil, den Arbeitsaufwand für die entsprechenden Fachmodule etwas zu verringern, die im darauffolgenden Semester belegt werden mussten. Auf diese Weise war der Arbeitsaufwand insgesamt für die Studierenden besser zu bewältigen. Neben den fachbezogenen und sprachlichen Schwierigkeiten traten verstärkt Probleme bezüglich der Finanzierung des Studiums auf: Allein für das Studium fallen Kosten in Höhe von 780€ im Semester an. Hinzu kommen Material- und Fahrtkosten sowie Kosten für den Lebensunterhalt. Viele Studierende hatten bisher zumindest ergänzend Unterstützung durch das ALG 2 erhalten. Diese fiel mit Studienbeginn weg; ein Bafög-Anspruch bestand aber aufgrund des Alters bzw. des vorhergehenden Abschlusses meist nicht. Zur Sicherung des Familieneinkommens mussten sie einer bezahlten Tätigkeit nachgehen, wodurch das Studium erschwert und zeitlich verlängert wurde.

Inzwischen haben sich die Probleme relativiert: die Studierenden haben sich in Lerngruppen organisiert oder Anschluss an bestehende Lerngruppen gefunden, so dass die Arbeit für die einzelnen Module gut zu bewältigen ist. Die sprachlichen Probleme werden langsam kompensiert. Die Studierenden sind zwar meist mit nur zwei bis drei belegten Modulen ins Studium eingestiegen, aber schon im dritten Semester absolvieren sie mehrheitlich den regulären Stundenplan mit bis zu fünf Modulen.

Fazit

Mit dem Studienprogramm an der Universität Oldenburg konnten wir ein erstes Studienangebot für hochqualifizierte Migranten im Bereich der Informatik anbieten. Das Konzept der Begleitung und Beratung hat sich als dringend notwendig und sehr erfolgreich erwiesen. Noch stärker als zunächst schon angenommen, hat die erste Phase des Studienprogramms gezeigt, wie wichtig die Gewöhnung an die Lehr-, Lern- und Studienstrukturen für Migranten in der Informatikausbildung ist. Das mit dem Studienprogramm etablierte Begleitprogramm von der Auswahl über die individuelle Beratung und Begleitung ist neben der Fachausbildung damit eine wichtige Säule der Informatikausbildung für diese besondere Zielgruppe.

Das Interesse am Studienprogramm ist groß - trotz bisher noch eher geringer Werbung und Bekanntheit des Projektes. Aufgrund von zwei Interviews in den letzten zwei Monaten, gab es deutlich mehr Anfragen aus dem gesamten Bundesgebiet. Es resultierten daraus 22 konkrete Bewerbungen, von denen elf direkt ins Studienprogramm aufgenommen wurden. Mit den neu aufgenommenen Bewerbern ist ein altes Problem wieder in den Brennpunkt der Arbeit gerückt – die Finanzierung des Studiums. Hier gibt es gerade für diese Zielgruppe keine ausreichenden Lösungen und es muss dringend nach Möglichkeiten der Abhilfe gesucht werden.

Empfehlungen und Wünsche

Zur Studienvorbereitung gehört der kostenfreien Sprachunterricht sowohl in der deutschen Umgangs- als auch Fachsprache. Diese Sprachförderung ist unverzichtbar und sollte finanziell besser gefördert werden. Darüber hinaus fehlt es an Angeboten zum Erlernen so genannter Schlüsselkompetenzen, wie beispielsweise dem Erlernen von *Interkultureller Kommunikation*. Anstelle der Integration findet an den Hochschulen oft die Isolation der ausländischen Studierenden im zwar friedlichen Nebeneinander, aber in Form des Sich-aus dem-Weg-Gehens statt.

Literatur

[E07] Engelmann, Bettina, Müller, Martina: Brain Waste. Die Anerkennung von ausländischen Qualifikationen in Deutschland, Augsburg 2007

[H04] Hadeed, Anwar: Sehr gut ausgebildet und doch arbeitslos. Zur Lage höher qualifizierter Flüchtlinge in Niedersachsen, Oldenburg 2004

[I09] Institut der deutschen Wirtschaft Köln: Informationsdienst der deutschen Wirtschaft, Ausgabe vom 9.07.2009, http://www-iwkoeln.de/Publikationen/iwd(Archiv/tabid/122/articleid/23673/Default.aspx

[M08] Meinhardt, Rolf: Die ignorierte Elite – zur prekären Lage hochqualifizierter Einwanderer und der Entwicklung von Studienangeboten zu ihrer beruflichen Integration, in Lange, Dirk (Hrsg.): Migration und Bürgerbewusstsein, Wiesbaden 2008

[M10] Meinhardt, Rolf: Akademische Weiterbildung für hochqualifizierte Einwanderer – ein Win-Win-Angebot (erscheint Mitte 2010 im Hampp Verlag Mering)

[P09] Presse- und Informationsamt der Bundesregierung: Integrationspolitik: Gleichberechtigte Teilhabe – der demografische Wandel bringt auch Chancen, Pressemitteilung 493 zum Kongress „Demografischer Wandel: Integration und Gesundheit", Hannover 18.12.2009 http://www.bundesregierung.de/Content/DE/Pressemitteilungen/BPA/2009/12/2009-12-18-ib-demografischer-wandel.html

[S10] Carl-Ossietzky Universität / Department für Informatik: Studienprogramm Informatik für Migrantinnen und Migranten, Oldenburg 2010 http://www.informatik.uni-oldenburg.de/studium/informatikfuermigranten

Anmerkung

1 *Ein Modul ist eine Lehreinheit, die in den Studiengängen der Informatik in der Regel 4 Semesterwochenstunden (SWS) und damit sechs Kreditpunkte umfasst.*

Zu dieser Thematik wird ein Vortrag mit dem Titel Informatik für Migrantinnen und Migranten – Einführung eines neuen Studienprogramms an der Universität Oldenburg *bei der Konferenz HDI 2010 vom 6.-8. Dezember in Paderborn gehalten, der inhaltlich mit dem vorliegenden Artikel wesentlich übereinstimmt.*

Fakultät II Department für Informatik
– Carl-von-Ossietzky Universität Oldenburg
26111 Oldenburg – Germany

Web: *www.informatik.uni-oldenburg.de/studium/informatik-fuermigranten*

Email: *informatik-fuer-migranten@informatik.uni-oldenburg.de*

Interview mit Heidi Schelhowe

Medienbildung in einer digital geprägten Kultur

Auf dem Weg zur selbstbewussten und verantwortungsvollen Gestaltung von Technologie und Gesellschaft?

Heidi Schelhowe ist Hochschullehrerin für Digitale Medien in der Bildung in der Informatik an der Universität Bremen. Mit ihrem interdisziplinär zusammengesetzten Team entwickelt sie Hardware und Software für Bildungskontexte, gestaltet Lernumgebungen und begleitet Lernprozesse empirisch. Sie hatte die Federführung in der Expertenkommission des BMBF zur Medienkompetenz. Mit der FIfF-Kommunikation sprach sie über den Hintergrund und die Ergebnisse dieser Expertenkommission sowie über ihre eigene Arbeit in diesem Themenumfeld. Die Fragen stellte Ralf E. Streibl.

Heidi Schelhowe

FIfF: Das Bundesministerium für Bildung und Forschung veröffentlichte jüngst den Bericht einer Expertenkommission, der Du angehörtest. Im Fokus standen Medienkompetenz und Medienbildung in einer digital geprägten Kultur. Die vielleicht schwerste Frage gleich zu Beginn: Was ist Medienkompetenz?

Heidi Schelhowe: Wir sind im Expertenbericht zunächst davon ausgegangen, dass Medienkompetenz eine Arbeit und Freizeit übergreifende Kompetenz ist, die ein Verständnis davon umfasst, welche Veränderungen sich mit der „digitale geprägten Kultur" ergeben. Medienkompetenz soll als Handlungskompetenz sowohl der Persönlichkeitsbildung dienen als auch der Förderung von Ausbildungs- und Erwerbsfähigkeit. Es geht dabei um weit mehr als den Umgang mit Medien. Die Digitalen Medien, mit dem Computer als Kern, durchdringen alle Poren der Gesellschaft und des Lebens , sie sind in der Arbeitswelt verbreitet, sind das entscheidende Medium der Kommunikation, verändern das Verständnis von Öffentlichkeit, die Art, wie wir Freizeit gestalten, wie wir Informationen gewinnen, wie wir uns selbst wahrnehmen und wie wir kommunizieren. Der Bildungsbegriff bezeichnet eine Veränderung des Selbst- und Weltverhältnisses. Das ist ohne Digitale Medien heute nicht mehr zu denken. Um Prozesse zu initiieren und zu begleiten, in denen ein Verständnis von sich selbst und vom Handeln in der Welt entsteht, braucht es ein Verständnis auch dieses Mediums. Es geht also bei Medienbildung darum zu begreifen, wie wir selbst und unsere Umwelt sich verändern im Umgang und im Bezug auf die Medien, nicht nur um Nutzungskompetenz – auch wenn diese zweifellos dazu gehört.

FIfF: Im Bericht wird die Gefahr einer „digitalen Spaltung der Gesellschaft" erwähnt. Inwiefern kann Medienbildung dem tatsächlich entgegenwirken?

Heidi Schelhowe: Nahezu alle jungen Menschen sind heute mit den Digitalen Medien unterwegs. Jede/r besitzt ein Handy und das Internet gehört – flächendeckender noch als bei den Erwachsenen – zum Alltag. Wir wissen aber aus den Jugendstudien, dass die Vielfalt und Reichhaltigkeit dessen, was mit dem Computer getan wird, sehr stark vom formalem Bildungshintergrund anhängt. Die Vielfalt im Umgang ist bei GymnasiastInnen sehr viel größer ist als bei jungen Menschen in der Hauptschule. Dem kann nur durch Angebote in den Bildungsinstitutionen, sei es in der Schule oder in Freizeitheimen entgegengewirkt werden. Alle

Bundesministerium für Bildung und Forschung BMBF: Kompetenzen in einer digital geprägten Kultur. Medienbildung für die Persönlichkeitsentwicklung, für die gesellschaftliche Teilhabe und für die Entwicklung von Ausbildungs- und Erwerbsfähigkeit. Bericht der Expertenkommission. Bonn/Berlin 2010.

http://www.bmbf.de/pub/kompetenzen_in_digitaler_kultur.pdf

Jugendlichen berichten, dass sie ihre Kenntnisse und Zugangsmöglichkeiten zum Computer in der Regel nicht in der Schule bekommen. Gerade Kinder und Jugendliche aus bildungsfernen Familien bekommen aber oft zu wenig Anregung, die Potenziale des Computers in ganz unterschiedlichen Richtungen zu nutzen. Wie Kinder es in unseren Workshops bisweilen formulieren: „Wir haben gesehen, was man mit Computern alles noch machen kann". Wenn junge Menschen sich auf Spielen und Chatten beschränken, wenn ihnen die Möglichkeiten des Internet für Information, für selbstständiges informelles Lernen, für den Erwerb von Ausbildungs- und Berufsqualifikation und für Partizipation und demokratische Teilhabe nicht deutlich werden, vertieft das Internet die soziale Spaltung.

FIfF: Die Expertenkommission bezeichnet Medienbildung als „integralen Bestandteil von Allgemeinbildung". Kinder und Jugendliche stecken zum einen in formalen Bildungs- und Erziehungskontexten, zum anderen entwickeln sie viele Umgangsweisen mit Medien in informellen Kontexten, durch eigenständige Aneignung, im direkten sozialen Austausch und nicht zuletzt in der Interaktion mit dem Medium und anderen Nutzern. In welchem Verhältnis stehen im Bereich Medienbildung formale Bildungsprozesse und Selbstsozialisation zueinander?

Heidi Schelhowe: Junge Menschen haben häufig selbst, gestützt auf ihre Peers, die notwendigen Fähigkeiten im Umgang mit Digitalen Medien entwickelt. Sie verbringen viel Zeit mit den Medien und haben sich durch Learning-by-Doing eine hohe Nutzungskompetenz angeeignet, mit der sie in der Lage sind, Computerprogramme versiert, rasch und sicher zu bedienen. Dies ist eine Fertigkeit, auf die viele von uns Erwachsenen nur neidisch sein können. Junge Menschen können zu Recht stolz darauf sein, wenn sie sich diese Kenntnisse und Fertigkeiten – oft ohne Hilfe Erwachsener – angeeignet haben. Bei medienpädagogischen Überlegungen sollten wir hier anknüpfen, das zu schätzen wissen und würdigen. Sicher wird dies aber nicht ausreichen, um sich in einer von Medien geprägten Welt gut orientieren zu können. Dazu braucht es mehr als damit umgehen zu können. Hier ist (auch) formale Bildung gefordert. Allerdings glaube ich auch, dass es eine Überforderung ist, wenn die Schulen und die LehrerInnen damit alleine gelassen werden. Es braucht sozusagen „ein ganzes Dorf", um Medienbildung zu verankern. Dazu gehören auch Aktivitäten in den Gemeinden und Stadtteilen außerhalb der Schule, die Verbindung mit Bibliotheken, Sportvereinen, Stadtteilinitiativen. Auch Unternehmen müssen ihren Teil dazu beisteuern. Die Digitalen Medien selbst bieten ja auch neue Chancen, aus der Schule hinaus zu gehen und sich mit der Umgebung und mit der Praxis im Handeln zu verbinden.

FIfF: Die Kommission hat vier Themen- und Aufgabenfelder herausgearbeitet. Würdest Du sie kurz beschreiben und – aus Deiner Sicht – in ihrer Bedeutung einschätzen?

Heidi Schelhowe: Wir haben vier Themen- und Aufgabenfelder identifiziert, auf die sich Medienkompetenz bezieht: Information und Wissen; Kommunikation und Kooperation; Identitätssuche und Orientierung; Digitale Wirklichkeiten und produktives Handeln. Alle diese Bereiche sind wichtig und gewinnen eine besondere Bedeutung mit den computergestützten Medien. In der Medienbildung gibt es einerseits Aufgaben, die sich im Umgang mit Medien generell, also auch mit traditionellen Medien stellen. Informationen einordnen zu können, gehörte z.B. immer schon zur Informationskompetenz, wie sie etwa im Bibliotheksbereich definiert worden ist. Neu aber kommt heute dazu, dass selbst sehr junge Menschen in der Lage sind, Informationen in eine große und anonyme Öffentlichkeit hinein zu verbreiten. Eine neue Herausforderung ist sicherlich auch, dass Wissenserwerb sehr viel mehr als in früheren Zeiten als Gruppenprozess organisiert ist. Mir persönlich war der Bereich „Digitale Wirklichkeiten und produktives Handeln" ein besonderes Anliegen, weil darüber zu wenig gesprochen wird. Es geht um die „doppelten" Wirklichkeiten, die mit dem Computer entstanden sind, die zeichenhafte Repräsentation fast aller Lebens- und Arbeitsbereiche im Medium. Wir können nicht länger sagen, dass das eine – die materiell-physikalische Präsenz - die „Wirklichkeit" sei und das, was im Computer verarbeitet wird, „nur" das Virtuelle. Computerprogramme entstehen aus der Analyse der materiellen Wirklichkeit und sie können sogar direkt physikalische Prozesse auslösen, sie steuern, erzeugen. Was dazwischen passiert, welche Rolle die Algorithmen und Computerprogramme spielen, das muss man heute - zumindest als Prinzip - verstehen, um die Kontrolle zu behalten und Verantwortung übernehmen zu können. Die Digitalen Medien bieten uns heute die Möglichkeit, dass wir dies nicht als „abstrakte" Instruktion vermitteln, sondern handlungsorientiert und gestaltend zugänglich, erfahrbar und be-greifbar machen können.

FIfF: Die Expertenkommission kritisiert, dass in den meisten Bundesländern eine verbindliche Mediengrundbildung in der Aus- und Fortbildung von Lehrerinnen und Lehrern fehlt. Magst Du – vielleicht am Beispiel Bremen – kurz skizzieren, was aus Deiner Sicht sinnvoll und wünschenswert wäre?

Heidi Schelhowe: Wir hatten in Bremen bis zur Einführung des Bachelors in den Studiengängen mit dem Ziel Lehramt eine verpflichtende Lehrveranstaltung „Lernen mit technischen Medien" verankert. Das war nicht viel und die Inhalte waren auch thematisch und von Qualität und Form her recht unterschiedlich. Aber immerhin gab es so etwas. Heute ist das im Pflichtkanon nicht mehr verankert. Bis heute bieten wir eine Zusatzqualifikation, ein Zertifikat „Digitale Medien in pädagogischen Kontexten" an. Man kann dafür Leistungen aus Lehrveranstaltungen, die einen Medienbezug haben, doppelt anerkennen lassen. Für die Studierenden wird es aber immer schwieriger, diese Chance für eine Ausprägung von Medienkompetenz wahrzunehmen in dem engen Kanon ihrer Pflichtangebote. Wir, eine Gruppe von medienpädagogisch engagierten Lehrenden aus verschiedenen Fächern, aus den Erziehungswissenschaften und aus der Informatik, streben in der Reform des Studiums aber an, Medienpädagogik wieder stärker im Pflichtangebot zu verankern.

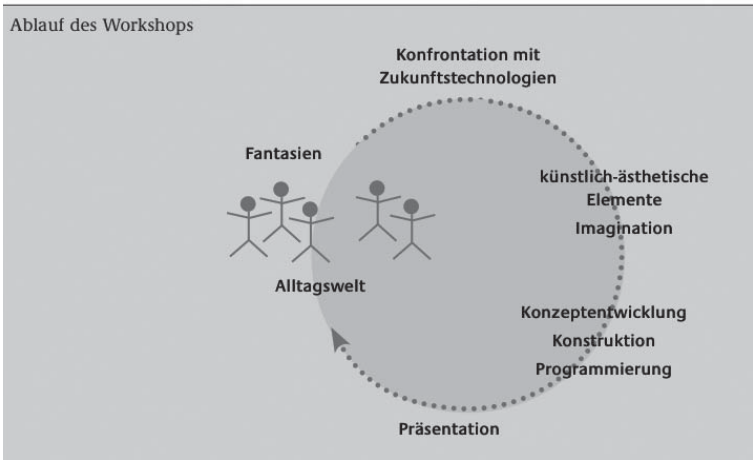
FIfF: Deine Arbeitsgruppe „Digitale Medien in der Bildung" an der Uni Bremen hat ja langjährige Erfahrung u.a. mit Workshops für ganz unterschiedliche Zielgruppen. Kannst Du hierfür ein oder zwei Beispiele skizzieren?

Heidi Schelhowe: In unseren Workshops, die auch Teil unserer Forschungsprojekte sind, geht es darum, aktuelle Entwicklungen Digitaler Medien für jede und jeden zugänglich zu machen. Mit dem eigenen Gestalten wollen wir zum Erlebnis persönlicher Wirksamkeit (statt Ohnmacht gegenüber der technologischen Entwicklung) beitragen. Unser Schwerpunkt in der Medienbildung

liegt im Bereich „Digitale Wirklichkeiten und produktives Handeln". Da wir in der Informatik sind, haben wir den Vorteil, dass wir die Technologien selbst auch so entwickeln können, dass sie für das Lernen geeignet sind. So haben wir z.B. das „Construction Kit EduWear" entwickelt, mit dem Lernende selbst ihre eigenen „intelligenten" Textilien entwickeln können, T-Shirts, Taschen, Fußballschuhe, die mit Sensoren, Aktuatoren und Microprozessor ausgestattet sind. Daran lassen sich wichtige Prinzipien der Computerisierung der Gesellschaft verdeutlichen und diskutieren, ohne naive Technik-Begeisterung oder den erhobenen Zeigefinger. Immer achten wir darauf, dass wir künstlerisch-ästhetische Elemente mit einbeziehen, weil sie Kreativität und Reflexionsfähigkeit fördern. Unsere Workshops laufen unter dem übergreifenden Titel „TechKreativ", siehe *http://www.techkreativ.de.*

FIfF: Es gab mal eine treffliche Karikatur, in der ein „Pädagogik" beschriftetes Männchen sich verzweifelt am Siebenmeilenstiefel eines mit weit ausholenden Schritten voraneilenden *Technik*-Mannes festklammert, um nicht völlig abgehängt zu werden. Was meinst Du: Kann es gelingen, diese oft erlebte Situation zu durchbrechen? Welche Chancen und Möglichkeiten siehst Du - auch vor dem Hintergrund der Arbeit der Expertenkommission?

Heidi Schelhowe: Genau dies ist ein wesentliches Anliegen, das wir bei dimeb mit unserer Forschung und Lehre verfolgen und was für mich auch eine wesentliche Motivation für die Teilnahme an der Expertenkommission war. Insbesondere junge Menschen brauchen die Erfahrung, dass sie mit ihren Fertigkeiten im Medienumgang willkommen geheißen und geschätzt werden, sie brauchen aber auch die Herausforderung, die ein kreativer und



Ablauf des Workshops (aus dem Bericht der Expertenkommission)

verantwortlicher Umgang mit den Medien bedeutet. Wozu wir als Erwachsene verpflichtet sind, ist, mit ihnen zu diskutieren, welche gesellschaftliche Bedeutung, welche positiven Seiten und Gefahren die Medien in den Innovationsprozessen, in der Herstellung demokratischer Öffentlichkeit, in der Bildung usw. haben. Nur so kann es uns gelingen, dass wir der Technik nicht hinterherlaufen, sondern uns als selbstbewusste und verantwortungsvolle GestalterInnen von Technologie und Gesellschaft begreifen und dieses Verständnis auch an die kommenden Generationen weitergeben.

FIfF: Vielen Dank für dieses Gespräch!

Maike Hecht, Carola Schirmer, Susanne Maaß

Hauptsache Linux?!

Diversität & Beteiligung in Software-Migrationsprozessen

Open Source-Software und das Betriebssystem Linux haben sich in den vergangenen Jahren von eher belächelten Spielwiesen von Computerfreaks zu ernst zu nehmenden und attraktiven Alternativen für EndbenutzerInnen aller Art gewandelt. Die Unabhängigkeit von Branchenriesen wie Microsoft, die niedrigen Anschaffungskosten, der verfügbare und damit anpassbare Quellcode und die geringe Verbreitung von Viren, die Linux-Betriebssysteme attackieren, gehören zu den schlagkräftigen Argumenten, die Open Source-Software inzwischen auch für große Organisationen attraktiv machen. Vielfach werden dort bereits Server auf Linuxbasis betrieben. Die Umstellung der Computerarbeitsplätze der EndnutzerInnen (Desktops) haben dagegen erst wenige Organisationen vollzogen.

Der Prozess der Systemumstellung ist bei einem Betriebssystemwechsel ungleich aufwändiger als wenn *nur* eine einzelne Anwendung ausgetauscht werden soll. Der Arbeitsplatz einer jeden EndbenutzerIn verändert sich: FachanwenderInnen müssen nach der Migration sowohl mit einer neuen Grundlage, dem Betriebssystem, als in den meisten Fällen auch mit einer ganzen Reihe von anderen Softwareanwendungen arbeiten, die ihre gewohnten Arbeitsroutinen verändern. Diese Situation führt häufig bereits im Vorfeld eines Migrationsprozesses zu Verunsicherung und Widerstand auf Seiten der MitarbeiterInnen, die ihre erworbenen Fähigkeiten mit dem gewohnten Betriebssystem in Gefahr sehen, während sie für sich keine Vorteile in der Veränderung sehen.

Die Komplexität der Migration und die hohe Zahl an EndnutzerInnen, die von der Umstellung direkt betroffen sind und zukünftig ihre Aufgaben mit anderen Arbeitsmitteln verrichten sollen, verlangen, dass der innovativen Entscheidung für eine Betriebssystemumstellung eine sehr sorgsame Planung des Migrationsprozesses folgen muss - nicht nur in technischer Hinsicht. Während dieser Planung sollten die soziotechnischen Anforderungen an das neue System so genau wie möglich erhoben werden, um sowohl seine Lauffähigkeit als auch seine Aufgabenangemessenheit bestmöglich zu gewährleisten. Gleichzeitig gilt es, alle MitarbeiterInnen im Umstellungsprozess mit ihren Sorgen und Bedenken ernst zu nehmen und beim Umgang mit dem neuen System zu unterstützen. Dabei ist es wichtig, die betei-

ligten Personen in ihrer Heterogenität wahrzunehmen, um Anforderungen differenziert feststellen und ihnen entsprechen zu können.

Die Studie

In einer explorativen qualitativen Studie wurde der Frage nachgegangen, wie unterschiedliche EndnutzerInnen derzeit in Migrationsprozesse einbezogen und welche Unterstützungsangebote ihnen unterbreitet werden. Dabei wurden bewusst Aspekte der Diversität und der BenutzerInnenbeteiligung in den Fokus gerückt: Unter der Annahme, dass die ausgeprägte Heterogenität der MitarbeiterInnen großer Organisationen zu sehr unterschiedlichen Bedarfen in Bezug auf die Unterstützung und Einbeziehung bei Migrationsprozessen führt, sollten einerseits ihre Diversität und deren Einfluss auf den Prozess untersucht werden. Andererseits wurde das Ziel verfolgt, in einem Katalog von *Best Practices* Hinweise auf eine sinnvolle Beteiligung von unterschiedlichen MitarbeiterInnen zu geben und die Notwendigkeit verschiedener Zugänge zur Partizipation aufzuzeigen. Die erarbeiteten Aussagen sind in weiten Teilen auf Software- und insbesondere Betriebssystem-Migrationen im Allgemeinen zu übertragen; sie wurden aufgrund der Aktualität der Umstellung von Windows- zu Linux-Desktops an dieser Konstellation untersucht.

Im Rahmen der Studie wurden 27 MitarbeiterInnen interviewt, die in drei renommierten Projekten in Deutschland in den letzten Jahren den Umstellungsprozess in unterschiedlichen Positionen miterlebt hatten oder die sich noch in einer Testphase für die Umstellung auf den Linux-Desktop am Arbeitsplatz befanden. Befragt wurden MitarbeiterInnen in unterschiedlichen Positionen (IT-Leitung, Fachvorgesetzte, FachanwenderInnen, SupportmitarbeiterInnen) mit unterschiedlichen Methoden (ExpertInneninterview, Fokusgruppe, Interview im Kontext). Die Auswahl der InterviewpartnerInnen geschah unter identitätsrelevanten Diversitätskriterien (Alter, Geschlecht, Bildungshintergrund) und sah einen Längsschnitt durch unterschiedliche Abteilungen vor. Diese Vorgaben sollten davor bewahren, bestimmte Aspekte und Arbeitsplätze aus dem Blick zu verlieren, und eine möglichst große Heterogenität in der – sehr kleinen – Menge der befragten Personen erreichen.

Wer will hier Linux?

Die Ergebnisse der Studie belegen einmal mehr die unterschiedliche Sicht von IT- und Organisationsleitung und anderen MitarbeiterInnen auf die Einführung von Linux: Während die Managementebene hinter der Entscheidung steht und sie neben dem strategischen Imagegewinn als Fortschritt zu einer stärker autonomen und kostengünstigeren Versorgung mit Software preist, berichten AnwenderInnen des Linux-Desktops vor allem von Problemen bei der Umstellung, Produktivitätseinbußen und der Frustration, die daraus resultiert, dass die neuen Arbeitsmittel sie weniger gut unterstützen als die gewohnten. Dies allein aus einer vorherrschenden „Angst vor Neuerungen“ und einer allgemeinen „Ablehnung von Veränderungen“ (vgl. Festinger et al. 1987) zu begründen, greift jedoch zu kurz. Verständlich wird der vorliegende Widerspruch eher, wenn der Blick auf die zu erwartenden Vorteile gerichtet wird, die sehr ungleich verteilt sind: Für Entscheider im strategischen Management bringt Linux die oben genannten Vorteile. Für sie und für die IT-Leitung bieten Software-Umstellungen dieser Größenordnung darüber hinaus die Gelegenheit, Arbeitsprozesse und Softwarelösungen zu vereinheitlichen. Für IT-EntwicklerInnen und MitarbeiterInnen im IT-Support birgt der Übergang zu Linux die Möglichkeit, mit einer neuen Technologie zu arbeiten, neue Systeme und Anwendungen kennenzulernen. Sie entwickeln damit ihre fachliche Qualifikation weiter. Häufig sind sie ohnehin technologieaffin und von sich aus an Neuerungen auf diesem Gebiet interessiert.

Bei den FachanwenderInnen und ihren direkten Vorgesetzten steht dagegen die alltägliche Arbeit im Vordergrund. Der Computer ist ein Arbeitsmittel, das zur Verfügung stehen und funktionieren muss. Jede Veränderung des Gewohnten schränkt ihre Produktivität zunächst einmal ein, führt zu Zeitverlusten und dem häufigen Erlebnis von Misserfolgen. Dies finden die FachanwenderInnen selbst ärgerlich und es kann auch für Team- oder GruppenleiterInnen, die den Arbeitsprozess ihrer MitarbeiterInnen koordinieren müssen, Schwierigkeiten mit sich bringen. Auch kann die Umstellung auf neue Anwendungen bedeuten, dass MitarbeiterInnen, die mit den laufenden Anwendungen gut vertraut sind und den Umgang mit ihnen durch Schulungen und langjähriges Arbeiten eingeübt haben, plötzlich über wertlose Kenntnisse und Erfahrungen verfügen. Bisweilen sehen sie sogar ihre berufliche Identität oder den eigenen Arbeitsplatz bedroht. Vorteile entstehen für sie nur dann, wenn sie eine per-

Maike Hecht, Carola Schirmer und Susanne Maaß

Maike Hecht, **Carola Schirmer** und Prof. Dr. **Susanne Maaß** beschäftigen sich an der Universität Bremen mit Fragen der soziotechnischen Gestaltung von IT-Systemen unter Berücksichtigung von Gender- und Diversitätsaspekten. Das hier vorgestellte Projekt wurde in Kooperation mit IBM Deutschland und der Europäischen Akademie für Frauen in Politik und Wirtschaft, Berlin, mit Förderung des BMBF durchgeführt.

sönliche Affinität zu beispielsweise Linux haben, oder wenn bei der Auswahl und Gestaltung der neuen Softwareanwendungen explizit auf ihre Bedarfe eingegangen wird und sie so im Anschluss an die Migration mit Systemen arbeiten können, die ihren Arbeitsaufgaben stärker angemessen sind. Dies bringt EndanwenderInnen in einem Migrationsprozess in eine sehr fragile, da hochgradig abhängige Situation: Sie sind darauf angewiesen, dass ihre Bedarfe richtig erkannt und gute neue Unterstützungslösungen für sie gefunden werden – die, soweit möglich, die Unzulänglichkeiten der bisher eingesetzten nicht reproduzieren. Eine Software-Migration (auch) zum Vorteil der beteiligten FachanwenderInnen zu gestalten, bedeutet deswegen, sie mit ihren unterschiedlichen Bedarfen wahrzunehmen und Raum für Partizipation zu schaffen.

Fokus Diversität

Das Wahrnehmen von unterschiedlichen Dispositionen und Bedarfen kann zunächst entlang etablierter Diversitätskategorien erfolgen. Dazu zählen in erster Linie Geschlecht, Alter, ethnische Herkunft, soziale Schicht oder körperlich-gesundheitliche Verfasstheit (vgl. u.a. Gardenswartz & Rowe 2002, Krell et al. 2007, S.9). Doch auch wenn diese Kategorien ein sinnvoller Startpunkt sind, lässt sich kaum direkt von ihnen auf spezifische Anforderungen an einen Migrationsprozess oder an die Arbeitsmittelgestaltung schließen. Sie können vielmehr hilfreich sein, um eine kontextabhängige Diversität aufzuspüren, die die spezifischen Arbeitssituationen und -aufgaben beschreibt. Dies schließt nicht aus, dass die genannten identitätsbezogenen Diversitätskategorien zum Teil mit typischen Arbeitsverhältnissen und Arbeitsaufgaben zusammenfallen, was allerdings eher mit einer sozialen Ungleichheit einhergeht, die sich nur scheinbar mit der Differenz der betroffenen Personen begründen lässt (s.a. Krell et al. 2007, S.10). So arbeiten beispielsweise besonders viele Frauen in Teilzeit. Teilzeit gilt als ein Arbeitszeitmodell, das zu einer Verdichtung der Tätigkeiten ohne zeitliche Spielräume führt, was sich wiederum negativ auf die Einstellung zur Migration auswirken kann, da weniger Zeitfenster zum Erlernen und zur Einübung neuer Kompetenzen zur Verfügung stehen als bei Vollzeitbeschäftigten. In diesem Beispiel trägt der Blick auf das klassische Diversitätskriterium *Geschlecht* dazu bei, dass die besonderen Anforderungen von Teilzeitarbeitsplätzen in den Blick genommen werden. Sie helfen zu erkennen, in welcher Hinsicht sich Arbeitsplätze in einer Organisation unterscheiden können.

Kontextuelle Diversitätskriterien können aus den Rahmenbedingungen und der Organisation der Arbeit abgeleitet werden. Sie wirken sich unserer Ansicht nach stärker auf die individuelle Betroffenheit von der Betriebssystemumstellung aus als die etablierten, identitätsbezogenen Kategorien. Abhängig von Arbeitskontext und persönlichem Kontext, in dem eine MitarbeiterIn mit der Software-Umstellung konfrontiert ist, lassen sich dann auch Einstellung und Reaktion zur Migration nachvollziehen oder gar antizipieren. Wir betrachten die kontextuellen Diversitätsfaktoren auf drei Ebenen: Die Ebene der Unternehmensstruktur, die Ebene des Arbeitsplatzes sowie die Ebene der persönlichen Voraussetzungen einzelner MitarbeiterInnen. Auf allen drei Ebenen lässt sich angeben, welche Faktoren dazu führen, dass die Linux-Migration eher positiv oder eher belastend auf die MitarbeiterInnen wirkt.

Auf der *Ebene der Unternehmensstruktur* spielen unter anderem die Organisationsgröße, die Stärke der Hierarchien sowie die Organisationskultur eine Rolle. In großen Organisationen ist die Gefahr, dass der Bedarf an einzelnen Arbeitsplätzen oder von einzelnen ArbeitnehmerInnen untergeht, größer als in kleinen Unternehmen. In starken Hierarchien kann ein Entschluss für die Migration gegebenenfalls leichter durchgesetzt werden – es kann sich aber auch gegenteilig ein größerer Widerstand formieren, der sich in Blockadehaltungen äußert. Auf der *Ebene des Arbeitsplatzes* lassen sich beispielsweise Arbeitsplätze, an denen sehr stark mit anderen kooperiert wird, von solchen unterscheiden, an denen Beschäftigte weit gehend auf sich allein gestellt arbeiten. Weitere Unterscheidungen sind unter anderem Arbeitsplätze in Voll- oder Teilzeit, mit oder ohne Kundenkontakt, zentrale oder dezentrale Arbeitsplätze. Hinter diesen Kriterien stehen Fragen nach Zeitdruck, Flexibilität und Freiräumen in der Aufgabengestaltung, nach Abhängigkeiten sowie nach verfügbaren Hilfen und AustauschpartnerInnen. Je höher Druck und Abhängigkeit und je mühsamer der Zugriff auf Unterstützung ist, desto belastender kann eine Software-Migration für MitarbeiterInnen sein.

Auf der *Ebene der individuellen Voraussetzungen* prägen Interesse und Erfahrung die Einstellung der MitarbeiterInnen zur Linux-Einführung. Eine generelle Aufgeschlossenheit gegenüber Neuem und ein Interesse an Informationstechnik wirken sich beispielsweise eher positiv auf die Einstellung gegenüber einem Betriebssystemwechsel aus, ein hohes Sicherheitsbedürfnis eher negativ. Langjährige Erfahrung kann einerseits zu einer hohen generellen AnwenderInnnenkompetenz führen, die einen Wechsel erleichtert, kann aber auch dazu führen, dass eine MitarbeiterIn das System, bei dessen Nutzung er oder sie Experte ist, nicht aufgeben will.

Anhand dieser Beispiele wird erahnbar, dass eine Vielzahl von Diversitätsfaktoren zusammenwirken und beeinflussen, ob eine Person der Einführung eines neuen Betriebssystems eher offen oder eher ablehnend gegenübersteht. Die Wahrnehmung insbesondere der kontextuellen Diversität verdeutlicht, dass Organisationen unterschiedliche Strategien benötigen, um ihre MitarbeiterInnen gut durch den Migrationsprozess zu begleiten und sicherzustellen, dass sie im Anschluss über aufgabenangemessene Arbeitsmittel verfügen – die im besten Fall nicht nur genauso hilfreich sind wie die gewohnten, sondern Erleichterungen in der Arbeitsbewältigung mit sich bringen.

Fokus Beteiligung

Es wird allerdings ebenfalls deutlich, dass die Vielzahl von Faktoren bei einzelnen ArbeitnehmerInnen in sehr unterschiedlichen Kombinationen auftreten können. Es ist deshalb kaum möglich, klar abgegrenzte Personengruppen zu benennen, für die jeweils aufgrund bestimmter individueller und arbeitsplatzprägender Merkmale eine spezielle Umstellungsstrategie besonders geraten erscheint. Stattdessen sollte eine ganze Reihe unterschiedlicher Informations- und Beteiligungsmöglichkeiten vorgesehen werden, die auf die migrations- und organisationsrelevanten Faktoren abgestimmt sind und von den Beschäftigten aktiv genutzt werden können.

Beteiligung ist hier nicht nur im Sinne der Einbeziehung der gesetzlichen Arbeitnehmervertretung, der Betriebs- oder Personalräte gedacht, sondern wird im Sinne der partizipativen Softwareentwicklung (Schuler & Namioka 1991) verstanden. Ansätze für die Partizipation von EndnutzerInnen bei der Entwicklung und Einführung informationstechnischer Systeme an ihren Arbeitsplätzen wurden bereits in den 80er-Jahren aus der Erkenntnis heraus entwickelt, dass es für Betriebs- und Personalräte mangels Sachkenntnis häufig schwierig ist, ihre Mitbestimmungsrechte bei scheinbar rein technischen Entscheidungen wahrzunehmen. Voraussetzung für Beteiligung, aber auch ihr Ziel, ist die gegenseitige Perspektivenübernahme und das gemeinsame Lernen von SoftwareentwicklerInnen und BenutzerInnen (Floyd 1987). Der Anspruch und die Idee der partizipativen Softwareentwicklung lassen sich auf die Einführung einer neuen Software übertragen. Auch hier müssen Perspektiven der beteiligten Akteure wechselseitig verstanden werden, um im Rahmen der Migration eine funktionierende und aufgabenangemessene Arbeitsumgebung herzustellen. Eine Beachtung der in großen Belegschaften vorherrschenden Diversität der MitarbeiterInnen und Arbeitsplätze fordert dazu heraus, mehrere Möglichkeiten der und Zugänge zur Partizipation zu etablieren.

Die Beteiligung der MitarbeiterInnen in ihrer *schwächsten* Form beginnt mit ihrer Information und dem Etablieren einer angepassten Kommunikationsstruktur. Die Erfahrungen aus unserer Studie zeigen, dass einerseits eine frühzeitige, kontinuierliche und ehrliche Information der MitarbeiterInnen unerlässlich ist, damit diese sich wertgeschätzt fühlen und weiteres Interesse am Migrationsprozess zeigen. Ebenso wichtig ist die Einrichtung von Feedback-Kanälen, über die Rückfragen und Verbesserungsvorschläge an die Organisations- und IT-Leitung weitervermittelt werden können. Dies erfordert anschließend einen angemessenen Umgang mit der Rückmeldung – durch zeitnahe Antwort, tatsächliche Prüfung und Umsetzung von Vorschlägen. Im Hinblick auf die Diversität der MitarbeiterInnen schlagen wir vor, sowohl Abstufungen der Intensität der Information als auch unterschiedliche Zugänge über Push- und Pull-Medien zu realisieren. Dieses Vorgehen hat den Vorteil, dass wichtige Informationen alle Beteiligten erreichen, ohne dass es einen Überfluss an Nachrichten gibt, und dass Interessierte zur Information über weitere Themen eingeladen werden. Die Gratwanderung zwischen „zu wenig", „genügend" und „zu viel" Information lässt sich auf diese Weise besser bewältigen. Sie bedarf allerdings einer guten und ebenfalls frühzeitigen wie kontinuierlichen Planung und Anpassung an die realen Gegebenheiten und ermittelten Bedarfe.

Während Informations- und Kommunikationsangebote über die gesamte Laufzeit des Projekts allen MitarbeiterInnen zur Verfügung stehen sollten, betrifft die direkte Partizipation an Analyse-, Entscheidungs- und Gestaltungsprozessen immer nur einige von ihnen, die entweder aus persönlichen Gründen oder als betriebliche InteressenvertreterInnen daran teilnehmen. Sie sollten in der Analysephase eingeladen werden, zum Verständnis ihrer Arbeitsplätze beizutragen, da eine bloße Analyse des Software-Stacks am Arbeitsplatz häufig zu wenig Auskunft über das Geschehen gibt und erst recht keine Mängelanalyse zulässt. In Workshops mit partizipativer Methodik (u.a. Bødker et al. 2004) kann ein Zusammentreffen mit anderen Stakeholdern gestaltet werden. Auch Tests von Pilotumsetzungen sind in diesem Rahmen möglich. Eine weitere Form der Beteiligung sehen wir im Etablieren von „PatInnenprogrammen". Dabei halten einzelne AbteilungsvertreterInnen den direkten Kontakt zur IT-Abteilung, so dass beide Seiten übereinander informiert sind: Die PatInnen werden so zu MittlerInnen zwischen Bedarf und Angebot. Nicht jede MitarbeiterIn meldet sich jedoch gleich zu Beginn des Aufrufes freiwillig zu einem solchen Beteiligungsangebot. Es sollten deshalb bewusst mehrere, auch spätere Zugänge zur Mitgestaltung geschaffen werden, um nicht den Eindruck einer „verschworenen Gemeinschaft" zu vermitteln.

Im wiederholten direkten Kontakt von IT-GestalterInnen und FachanwenderInnen in gemeinsamen Workshops und/oder Diskussionsrunden steckt die große Chance der eingangs beschriebenen Perspektivenübernahme, die nicht nur zu einem besseren Produkt, sondern vor allem zum wechselseitigen Verständnis und zur Wertschätzung der Arbeit der jeweils anderen führen kann. Beides wurde in allen drei befragten Organisationen als aktuell sehr wenig ausgeprägt beschrieben, was zu massiven Problemen und Unstimmigkeiten auf beiden Seiten führte. In der IT wurde das mangelnde Verständnis der AnwenderInnen für die Arbeitsbelastung der IT und Terminverschiebungen kritisiert, das den Eindruck entstehen ließ, es sowieso nicht recht machen zu können. AnwenderInnen, insbesondere die Fachvorgesetzten, fühlten sich in ihrer Fachexpertise übergangen und von der IT mit pauschalen Lösungen abgespeist. Diese Erfahrungen sind bekannt und typisch für Prozesse der Software-Entwicklung und -Einführung in Organisationen. Bei der für viele Menschen großen Unbekannten *Linux* ist es deshalb umso wichtiger, die Beteiligten an einen Tisch zu holen und gemeinsam Strategien auszuloten.*

Literatur

Keld Bødker, Finn Kensing, Jesper Simonsen (2004): Participatory IT Design. MIT Press Cambridge, MA, London.

Leon Festinger, Martin Irle, Volker Möntmann (1987): Theorie der kognitiven Dissonanz. Huber, Göttingen.

Christiane Floyd (1987): Outline of a Paradigm Change in Software Engineering. In: Gro Bjerknes, Pelle Ehn, Morten Kyng (Eds.): Computers and Democracy – A Scandinavian Challenge. Avebury, Aldershot.

Lee Gardenswartz, Anita Rowe (2002): Managing Diversity. McGraw-Hill, New York [u.a.].

Gertraude Krell, Barbara Riedmüller, Barbara Sieben, Dagmar Vinz (2007): Einleitung - Diversity Studies als integrierende Forschungsrichtung. In: dies. (Hg.): Diversity studies: Grundlagen und disziplinäre Ansätze. Campus, Frankfurt/Main [u.a.], S. 8-16.

Yuliya Pysarenko (2010): Software-Migration partizipativ gestalten. Ein Modell zur Migration auf Linux im Desktop-Bereich. Masterarbeit, Fachbereich Mathematik/Informatik, Universität Bremen.

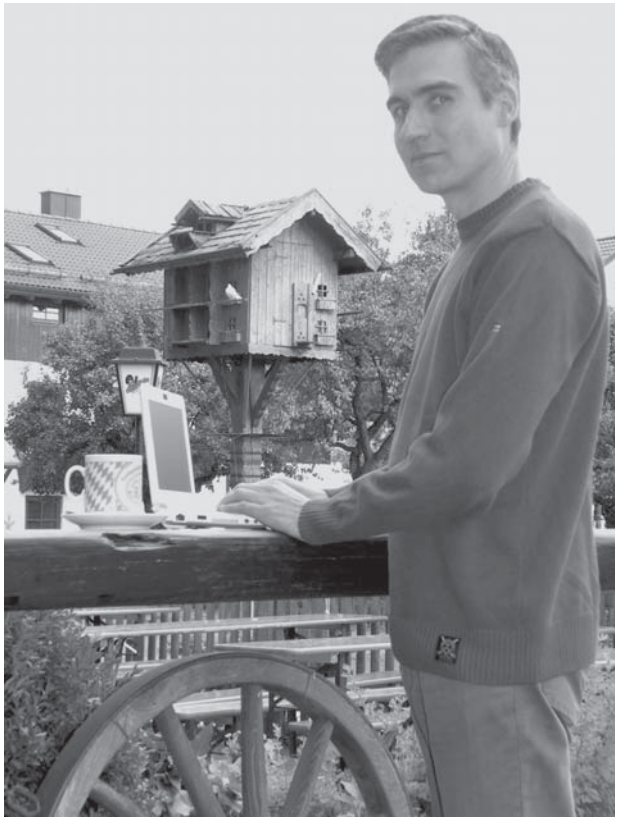
Douglas Schuler, Aki Namioka (1991): Participatory Design: Principles and Practices. Erlbaum, Hillsdale, NJ, USA.

** Im Rahmen des beschriebenen Projekts wurde eine Masterarbeit erstellt, die einen guten Überblick und einen praxisorientierten Leitfaden zur partizipativen Gestaltung von Software-Migrationsprozessen liefert (zum Weiterlesen empfohlen: Pysaranko 2010).*

Dagmar Boedicker

Datenschutz, für den man keinen Euro zahlt

In Bayern gehen die Uhren anders, vielleicht steht der Mann deshalb so entspannt in einem Wirtsgarten vor seinem Rechner. Es ist Andreas Stürzl, von Beruf ist er Datenschutzbeauftragter. Als Freiberufler kann er sich seine Zeit einteilen, zwischen der Arbeit als zertifizierter TÜV-Datenschutz-Auditor, Datenschutz-Manager und Lehrbeauftragter an der FH Rosenheim bleibt ein bisschen Luft für den Biergartenbesuch.



Andreas Stürzl bei der Arbeit

Und er kann seinen Kaffee auch bezahlen, obwohl er keinen Euro in der Tasche hat, dafür aber eine Karte mit dem geschwungenen Logo der Regionalwährung, des *Chiemgauers*. Dass er mit der Karte zahlen kann, das dachte er wenigstens, bis ihm die freundliche Bedienung bedauernd mitteilt, dass das Lesegerät kaputt ist. Macht nix, er hat auch noch ein paar Chiemgauer-Scheine dabei.

Die Scheine sind ziemlich fälschungssicher, soweit Geld das überhaupt sein kann. Wie erfolgreich listige Fälscher sind, beweisen die falschen Euro-Fuffziger ja oft genug. Der Chiemgauer hat sogar elf Sicherheitsmerkmale, fünf davon öffentlich: Er ist auf Spezialpapier gedruckt, hat eine Silberaufschrift mit Prägung, ein Wasserzeichen und auf der Rückseite wurde eine kopiergeschützte Farbe verwendet Sie verfärbt sich beim Kopieren. Feine Guillochen-Linien wie bei *richtigen* Geldscheinen und eine fühlbare Prägung des Logos sind ebenfalls Teil der Sicherheitsausstattung. Und wenn Chiemgauer gedruckt werden, geht es zu wie beim staatlichen Gelddrucken: Unter Zeugen werden die Papierbögen gezählt, geschnitten und gedruckt, jeder Arbeitsschritt und jeder Bogen schriftlich quittiert.

Warum sollte ich?

Andreas ist ziemlich rührig, er ist Mitglied der DVD und will es auch beim FIfF werden, engagiert sich bei der *dsb-group*, einem relativ kleinen Verein von vorwiegend freien Datenschutzbeauftragten, gegründet von Mitarbeitern der FH Augsburg. Sein Geschäft läuft gut, zumal er auch in Sachen IT-Sicherheit berät. Wenn ich ihn um eine Beratung bitten würde, könnte auch ich in Chiemgauern zahlen. Ich habe zwar keine, weil ich nicht Mitglied im Chiemgauer-Verein bin, das könnte ich aber ganz ohne Kosten werden und dann meine Euros umtauschen. Andreas *muss* übrigens die Chiemgauer annehmen, aber er will es natürlich auch.

Warum sollte ich eine Regionalwährung benutzen? Sind Euros nicht einfacher? Andreas hält dagegen: Schließlich seien Chiemgauer genauso einfach wie der Euro. Obendrein fließen aber 3% des Umsatzes in soziale Zwecke. Als einfache Konsumentin, die Chiemgauer nur ausgibt, kann ich selbst entscheiden, welches Projekt ich unterstützen möchte, ich muss die 3% aber gar nicht selbst abzweigen. Das tun diejenigen, die sich in der Regionalwährung bezahlen lassen. Wer Chiemgauer einnimmt, nimmt einen Wertverlust in Kauf, der sich auf 3% alle drei Monate beläuft. Dann kauft man eine Marke im Wert dieser 3%, klebt sie auf den Schein, und erhält so dessen Wert aufrecht. Weil alle Besitzer des lokalen Gelds es deshalb nicht sparen, sondern möglichst vor Ablauf der drei Monate ausgeben, bleibt es im regionalen Kreislauf und stärkt lokale Produzenten und Arbeitgeber.

Für Lebensmittel und andere Waren des täglichen Gebrauchs florieren die Geschäfte. Nur sehr spezialisierte Branchen tun sich nicht ganz so leicht, weil sie ihre eigene Beschaffung nicht immer völlig lokal organisieren und bezahlen können. Langfristig

Dagmar Boedicker

Dagmar Boedicker ist Journalistin und technische Redakteurin.
Sie hat Politikwissenschaft studiert.

soll der Chiemgauer aber für 15% der regionalen Umsätze den Euro ersetzen.

Was sind das für Menschen – die Vereinsmitglieder?

Sie legen Wert auf ihre Privatsphäre und zahlen deshalb nicht gern bargeldlos. Und sie wollen die Arbeitsplätze in der Region erhalten, im Einzelhandel, dem Gewerbe oder der Gastronomie. „Wo sollen meine Kinder später eine Lehrstelle oder einen Arbeitgeber finden, wenn große Ketten oder Discounter alles bodenständige Wirtschaftsleben verdrängen?“, fragt sich Andreas, wie viele andere. Der große Anteil an nachhaltig erzeugten Produkten spricht ebenfalls für den Willen der Vereinsmitglieder, wert-, verantwortungs- und sicherheitsbewusst zu leben und zu konsumieren.

Man kann ihnen nur viel Erfolg dabei wünschen.

Quellen

Der Chiemgauer http://www.chiemgauer.info
Andreas Stürzl http://www.interaktiv-edv.de/

Chiemgauer-Scheine

Kai Nothdurft

Passwörter, ein Sicherheitsrisiko

Bis vor einigen Wochen dachte ich, schon alles über die Risiken von Passwörtern zu wissen. Dann las ich in der Süddeutschen Zeitung am 22.10.2010 einen Artikel[1], der mich doch noch schockierte: Dort wurde berichtet, dass Bill Clinton während seiner Dienstzeit als US-Präsident eine Plastikkarte mit den Freigabecodes für den Nuklearen Atomschlag verlegt hatte. Noch schlimmer: Jimmy Carter hatte zuvor angeblich sogar eine solche Karte in seinem Jackett vergessen, als er es zur Reinigung gab. Mit den Codes auf der Karte kann man sich am Telefon als US-Präsident ausgeben und den Nuklearschlag autorisieren. Ich möchte mir nicht ausmalen, was da hätte passieren können.

Diese Vorfälle beleuchten schlaglichtartig einige gravierende Sicherheitsrisiken beim Einsatz von Passwörtern. Passwörter – selbst so wichtige – können verloren gehen oder vergessen werden, was zunächst mal den Besitzer von seiner Ressource aussperrt, zu der sie ihm Zugang gewähren sollen.

Man kann Passwörter aber auch erraten oder abhören. Die rechtmäßige Besitzerin bemerkt womöglich erst, dass ihr Geheimnis keines mehr ist, wenn es zu spät ist und das Wissen um das Geheimnis missbraucht wird.

Im Volksmärchen kompromittiert Ali Baba den Zugangscode zur Räuberhöhle durch Belauschen der *Passphrase* „Sesam öffne Dich“. Da die Geschichte so populär ist, dürfte diese Phrase sehr wahrscheinlich auch bei einem *Dictionary Attack* zum Einsatz kommen, bei der ein Angreifer, um an das Passwort zu gelangen, gar nicht alle Kombinationsmöglichkeiten per Brute Force durchprobiert, sondern wahrscheinliche und oft verwendete Wörter (oder Phrasen) der Gemeinsprache verwendet. Die für den Angriff verwendeten Dictionaries werden immer umfangreicher und erfassen längst auch fiktive Namen aus Literatur und Filmen oder Begriffe aller möglichen Fremdsprachen. Damit kommt ein Passwort Crack Programm sehr viel schneller zum Ziel, als wenn es alle theoretisch denkbaren Kombinationen ausprobiert.

Gegen den *Dictionary Attack* hilft es, keine Phrasen oder Wörter oder Kombinationen von solchen Wörtern mit eingängigen Zahlen wie Nine/11 zu verwenden. Auch muss man einfach erratbare Daten aus dem persönlichen Interessenumfeld wie Hobbies, den Namen des Partners oder das Geburtsdatum eines Bekannten meiden, erst recht wenn diese Informationen in einem Web2.0 Profil öffentlich zugänglich sind.

Gegen das Durchprobieren per *Brute Force* hilft es theoretisch, längere Zeichenketten einzusetzen oder neben Buchstaben und Zahlen auch Sonderzeichen und Groß- und Kleinschreibung zu verwenden, um so die Anzahl der Zeichen pro Stelle und den Zeitaufwand für das Durchprobieren zu erhöhen.

Leider steigt die Rechenleistung zum automatischen Durchprobieren oder dem Ausprobieren der Dictionaries-Begriffe nach Moore‘s Gesetz rasant an, weshalb immer längere Passwörter nötig werden oder diese immer schneller gewechselt werden müssen, damit das Passwort länger geheim bleibt, als ein Crackprogramm braucht, um es zu erraten. In diesem Sinne sichere Passwörter überfordern den Benutzer schnell, so dass er sie entweder vergisst oder aufschreibt, was beides wiederum mit Risiken verbunden ist.

Gegen den *Brute-Force-Angriff* wurden deshalb mehrere Sicherheitsmechanismen entwickelt – so sperren gut konfigurierte IT Systeme einen *Account* nach einer bestimmten Anzahl von Fehlversuchen. Dies funktioniert aber nur solange, wie die Angreiferin keinen Lesezugriff auf die im System gespeicherte Passwortliste hat, da sie diese sonst herunterkopieren und auf einem anderen System die Brute Force Attacke durchführen kann. Das Passwort muss dem System bekannt, also auch irgendwo gespeichert sein, da es sonst die Richtigkeit bei der Eingabe nicht überprüfen kann. Auf einem PC, an dem sich ein Benutzer lokal einloggt, liegt das Passwort auf dem Bootmedium gespeichert und kann, wenn dieses nicht voll verschlüsselt ist und mit *Preboot Authentication* arbeitet, dort von einer Angreiferin mit physikalischem Zugriff ausgelesen werden.

Inzwischen sind die Passwortlisten bei allen gängigen Betriebssystemen als *Hashcode* verschlüsselt gespeichert. Beim Login-Versuch wird auf die Benutzereingabe die Hashoperation durchgeführt, die die selbe Prüfsumme ergeben muss, um die Richtigkeit der Eingabe zu bestätigen. Dadurch kann die Liste selbst von einen Leseberechtigten nicht einfach nach dem Eintrag durchsucht werden, sondern man muss auf alle potenziellen Passwörter den zugehörigen Hash bilden und das Ergebnis mit den Hashes in der Liste vergleichen. Da diese Operation zusätzliche Rechenzeit benötigt, vergrößert sich der Aufwand für die Brute Force Attacke.

Doch auch gegen diesen Verzögerungsmechnismus gibt es eine Angriffsmethode, sogenannte *Rainbow Tables*. Das sind Tabellen, in denen die Ergebnisse dieser Operationen für alle Kombinationen kürzerer Passwörter bereits vorausberechnet sind und das Crackprogramm „nur" noch diese riesigen Tabellen nach dem passenden Hash absuchen muss. Passwörter mit weniger als zehn Zeichen Länge können mit der Rechenleistung normaler PCs so bereits in wenigen Stunden geknackt werden. Mit spezialisierter Hardware wie parallel rechnenden Grafikkarten und Ablage der nicht im Hauptspeicher gehaltenen Teile der Rainbow Tables auf schnellen *solid state disks* kann dies bedeutend schneller erfolgen.[2]

Zusätzlich sind Passwörter wie bereits erwähnt von der Ausspähung bedroht. Eine *Malware* auf dem Eingabesystem kann die Passworteingabe belauschen, physikalisch kann ein *Keylogger* als Hardware an das Keyboard angeschlossen werden. Bei der Übertragung kann das Passwort abgefangen oder mitgelesen werden. Schon bei der Eingabe kann die Besitzerin beobachtet werden, durch einen *Shouldersurfer*, der ihr z.B. im ICE oder in der Flughafen Lounge über die Schulter schaut und die Handykamera mitlaufen lässt. Inzwischen muss man in der Öffentlichkeit schon Ecken suchen, an denen einem nicht eine installierte Überwachungskamera beim Eintippen zuschaut. Auf einem Bahnsteig während der Wartezeit den Email Account zu checken, kann dem beobachtenden Voyeur ineteressante Einsichten bieten. Auch in dieser Beziehung erhöhen CCTV Systeme also nicht unbedingt die Sicherheit.

Abgefahren muten dagegen schon weitere Angriffe an, bei denen Abstrahlungen (Tempest) oder die Akustik des Tastaturanschlags aufgenommen und ausgewertet werden, um daraus das Passwort zu gewinnen. Eine unverschlüsselte Funktastatur schreit das darin eingegebene Passwort dagegen sogar absichtlich in die Welt hinaus, abhängig von Faktoren wie Signalstärke, Wellenlänge oder Empfindlichkeit des Empfängers und der Dämpfungüber nur wenige Meter oder aber auch deutlich weiter.

Bei all diesen Risiken fragt man sich, warum Passwörter überhaupt noch zum Einsatz kommen. Die Antwort ist ebenso trivial wie erschreckend: Sie sind als Schutzmechanismus vergleichsweise billig und einfach zu implementieren.

Alternativen sind zum Beispiel Zertifikate, für die aber eine PKI (Public-Key-Infrastruktur) benötigt wird, oder auch Biometrie, die aber auch eine Reihe von Risiken und Problemen mit sich bringt.

Höhere Sicherheit lässt sich durch *Multifactor Authentisierung* erreichen, bei der das Wissen um das richtige Passwort als Sicherheit ersetzt oder ergänzt wird um andere Mechanismen wie z.B. den Besitz eines Tokens. Token bedeuten aber zusätzliche Hardware, die hergestellt und gewartet werden muss, wodurch zusätzliche Kosten entstehen. Sie müssen zunächst auch sicher zum rechtmäßigen Besitzer gelangen, was ebenfalls Aufwand bedeutet.

Solange selbst Risiken wie ein Missbrauch von Atomwaffen mit Passwörtern abgesichert werden, ist es bis zu ihrer flächendeckenden Ablösung aber wohl noch ein weiter Weg.

Anmerkungen

1 http://www.sueddeutsche.de/politik/zahlencode-fuer-atomwaffen-einsatz-der-verlorene-keks-1.1015164

2 http://www.heise.de/security/meldung/Passwortknacker-100-mal-schneller-durch-SSD-949988.html

Kai Nothdurft

Kai Nothdurft studierte Informatik an der Uni Bremen und beschäftigte sich schwerpunktmäßig mit Datenschutz und IT-Sicherheit. Nach dem Studium arbeitete er 5 Jahre als Freiberufler im Schulungs- und Consultingbereich. Seit 1999 arbeitet er als IT-Sicherheitsbeauftragter für ein großes deutsches Versicherungsunternehmen.

Lesen –
Neues für den Bücherwurm

Sebastian Jekutsch

High Tech für Niedriglohn

Neotayloristische Produktionsregimes in der IT-Industrie in Brasilien und Mexiko

In Elektro-Discountern jagt ein Schnäppchen das nächste. Bekannte und Freunde belächeln uns, wenn wir nicht das preiswerteste Angebot gefunden haben. Telekommunikation ist so günstig geworden, dass der Enkel jährlich das neueste Handymodell unterm Weihnachtsbaum findet.

All das ist nur möglich, weil Informationstechnik weltweit optimiert hergestellt wird. Optimiert heißt: Der billigste Anbieter gewinnt. Die Rohstoffe kommen aus Erzminen in Peru oder dem Kongo, die Fertigung findet in China statt, repariert werden die Geräte in Mexiko und wenn mal recycelt wird, dann in Indien oder der Elfenbeinküste. In Europa wären die damit verbundenen Arbeitsplätze illegal: Geringer Verdienst, Versammlungsverbote, Gifte am Arbeitsplatz, fehlende Krankenversicherung, Kinderarbeit. Illegal? Egal! … sagen die einen. Entwicklungshilfe! … sagen die anderen. Dabei ist es letztlich eine moderne Form des Kolonialismus: Hilfe zur Selbsthilfe sähe anders aus, der Wohlstand der breiten Bevölkerung wächst mitnichten.

Kontraktfertigung nennt man es, wenn die Markenfirmen nicht mehr selbst produzieren, sondern die Fertigung aus der Hand geben an weithin unbekannte, riesige Betriebe. Typische Regionen sind China, Osteuropa und Lateinamerika. Die Niedriglohnländer locken mit gewerkschaftsfreien Zonen, fehlenden arbeitsrechtlichen und Umweltauflagen und Steuererleichterungen. Bei dieser globalen Wertschöpfungskette mischen Brasilien und vor allem Mexiko munter mit.

Mexiko war einst die bevorzugte Outsourcing-Region der U.S.-Betriebe. Im Rahmen von Freihandelsabkommen und der Liberalisierung der Märkte genoss man einerseits die Nähe, andererseits die geringen Löhne und flexible Auftragsvergabe. Mit der Krise um die Jahrhundertwende und der zunehmenden Konkurrenz aus Fernost verlor Mexiko jedoch zunehmend an Boden bei der IT-Fertigung. Eine weitere Senkung der Standards für die Arbeiterinnen und (wenigen) Arbeiter war die Folge.

Brasilien hat im Gegensatz traditionell für den Eigenbedarf gefertigt, unter anderem in entlegenen Amazonasgebieten mittels nationaler Förderprogramme. Auch hier haben die globale Konkurrenz und der Preisverfall die heimischen Strukturen verfallen lassen. Inzwischen werden hier hauptsächlich Spezialteile hergestellt und vertrieben. Brasilien war aber nie so exportabhängig wie Mexiko, was mit der insgesamt deutlich zufriedenstellenderen arbeitsrechtlichen Situation korreliert.

Die Historie der Kontraktfertigung und aktuelle Situation in Mexiko und Brasilien beschreibt Martina Sproll ausführlich in dem vorliegenden Buch „High Tech für Niedriglohn". Die Länder werden übersichtlich verglichen anhand eines einheitlichen Schemas: Standorte, Arbeitsprozess, Gesundheitsschutz, Löhne, Arbeitszeiten, geschlechtliche Arbeitsteilung, Rekrutierung, Gewerkschaften.

Das Buch ist eine Promotionsschrift. Der wissenschaftliche Teil umfasst unter anderem die Analyse von Produktionsregimes auf der Basis von Burawoys *Politics of Productions*, die einerseits die betrieblichen Abläufe *(relations in production),* andererseits die von außen einwirkende Landes-, Tarif- und soziale Firmenpolitik *(relations of production)* integriert betrachtet.

Der wissenschaftliche Fortschritt des Textes liegt in der Erweiterung seines Ansatzes sowohl um arbeitsorganisatorische und geschlechtsspezifische Bedingungen als auch im Einbeziehen der Reproduktionsweise (also Erhaltung) der Arbeitskraft und aktueller Aspekte der Globalisierung. Methodisch basiert die Arbeit auf Dokumentenanalyse, Feldtagebüchern und ExpertInnen-Interviews, sowohl mit Arbeiterinnen als auch dem mittleren Management. Das Buch wird besonders interessant, wenn aus den Interviews zitiert wird.

Man lernt einiges. Geholfen hat mir zum Beispiel die gut beschriebene geschichtliche Einbettung und Entwicklung des (Neo-)Taylorismus. Vieles in dem Buch geht natürlich über das Interesse von Laien hinaus. Ihnen kann ich als Einstieg und Motivation für mehr den letzten Teil des Buchs, das Resümee, wärmstens empfehlen, gefolgt von der Zusammenfassung der empirischen Ergebnisse aus Mexiko und Brasilien.

Sproll, Martina; High Tech für Niedriglohn: Neotayloristische Produktionsregimes in der IT-Industrie in Brasilien und Mexiko; 395 Seiten; Westfälisches Dampfboot; 1. Auflage Mai 2010; ISBN: 978-3-89691-792-8; € 34,90

Barbara M. Oechsler

»Es wird mal wieder Zeit …«

Notizen aus dem FIfF-Büro

Ralf Streibl rief mich im FIfF-Büro an, fragte: „Hast Du nicht Lust einen Artikel über die Geschäftsstelle zu schreiben? Den letzten haben wir in der zweiten Ausgabe aus dem Jahre 2001 gehabt – zu der Zeit, als wir gerade mit der Geschäftsstelle nach Bremen gezogen sind. Ich finde, es wird mal wieder Zeit." „Ja gerne", beantwortete ich ihm seine Frage.

Wir sind seit Jahren fest in Bremen etabliert und teilen uns ein wunderschönes Eckbüro mit der Bremischen Stiftung für Rüstungskonversion und Friedensforschung in der Villa Ichon im Bremer Viertel. Im März 2009 übernahm ich Anja Riemers Stelle und erledigte mit Christian Lilienthal gemeinsam die zahlreichen Aufgaben in der Geschäftsstelle. Christian beendete ein Jahr später sein Studium als Verfahrenstechniker und ist nun andernorts fest in Lohn und Brot.

Meine neue Kollegin, Ingrid Schlagheck, die seit April dieses Jahres mit mir erfolgreich das Büro organisiert, bringt nicht nur ordentlich frischen Wind in unsere von Natur aus komplexen Verwaltungsstrukturen, sondern bereichert die Geschäftsstelle durch ihr kaufmännisches und logistisches Fachwissen. Ihr beruflicher Werdegang führte sie vom Buchhandel über verschiedene Bibliotheken in die Pressestelle der Bremer Universität und somit in die Reichweite des FIfF.

Als ausgebildete Versicherungskauffrau habe ich lange Jahre fest angestellt gearbeitet und mich mit 33 Jahren entschlossen Informatik zu studieren. Als ordentliche Studentin an der Bremer Uni eingeschrieben, bin ich ziemlich schnell auf das FIfF gestoßen und wurde von Ralf für die Geschäftsstelle angeworben.

Das »Tagesgeschäft«

Neben der Mitgliederverwaltung und Administration, die der Verein so mit sich bringt, machen wir vierteljährlich die große FK-Versandaktion (Abkürzung für die FIfF-Kommunikation).

Der Kontakt zu unseren Mitgliedern liegt uns besonders am Herzen. Oft erhalten wir Anfragen aus dem Mitgliederkreis und auch von außerhalb. Wir sind immer bemüht, diesen Kommunikationskanal zwischen dem FIfF und unseren Mitgliedern und darüber hinaus offen zu halten. Dafür stehen uns mehrere Kompetenzteams zu unseren Schwerpunktthemen zur Verfügung, die sich aus dem Vorstand, Beiratsmitgliedern und unseren aktiven Mitgliedern zusammensetzen. Trifft eine Anfrage ein, leiten wir sie an einen oder mehrere Expertenkreise weiter. Meistens wird so schnell jemand gefunden, der mit dem Anfragenden in Kontakt tritt.

Wir freuen uns über jede Anfrage und über aktive Mitarbeit. Neben unserer großen Versandaktion einmal im Quartal, versenden wir auch immer wieder Info-Pakete an Mitglieder und unsere Regionalgruppen, die auf Tagungen und Veranstaltungen einen FIfF-Stand aufbauen wollen und dafür Plakate, unsere aktuellen Zeitschriften und Broschüren benötigen. Sagt uns früh genug Bescheid und wir helfen Euch gerne bei der Planung.

Seit einigen Monaten haben wir für Bestellungen die e-Mail Adresse *shop@fiff.de* eingerichtet. In der Geschäftsstelle können unsere sämtlichen Publikationen, wie z.B. die aktuelle Broschüre zur elektronischen Gesundheitskarte, FIfF-Kommunikationen aus dem Archiv, Bücher und Liebhaberstücke käuflich erworben werden können. Ein Shop auf unserer Webseite ist in Planung, zukünftig kann man dann auch dort die eine oder andere „antiquarische" Tagungstasse, Zeitschrift oder anderes bestellen.

Ingrid Schlagheck

Barbara M. Oechsler

In diesem Sinne freuen wir uns auf ein aktives, reges und kommunikatives 2011 mit Euch.
Ein schönes Weihnachtsfest im Kreise Eurer Familie und einen guten Rutsch ins Neue Jahr.

Eure Geschäftsstelle
Ingrid Schlagheck und Barbara M. Oechsler

FIfF e.V.

Im FIfF haben sich rund 700 engagierte Frauen und Männer aus Lehre, Forschung, Entwicklung und Anwendung der Informatik und Informationstechnik zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen und Bezüge des Fachgebietes verantwortlich fühlen. Wir wollen, dass Informationstechnik im Dienst einer lebenswerten Welt steht. Das FIfF bietet ein Forum für eine kritische und lebendige Auseinandersetzung – offen für alle, die daran mitarbeiten wollen oder auch einfach nur informiert bleiben wollen.

Vierteljährlich erhalten Mitglieder die Fachzeitschrift FIfF-Kommunikation mit Artikeln zu aktuellen Themen, problematischen Entwicklungen und innovativen Konzepten für eine verträgliche Informationstechnik. In vielen Städten gibt es regionale AnsprechpartnerInnen oder Regionalgruppen, die dezentral Themen bearbeiten und Veranstaltungen durchführen. Jährlich findet an wechselndem Ort eine Fachtagung statt, zu der TeilnehmerInnen und ReferentInnen aus dem ganzen Bundesgebiet und darüber hinaus anreisen. Darüber hinaus beteiligt sich das FIfF regelmäßig an weiteren Veranstaltungen, Publikationen, vermittelt bei Presse- oder Vortragsanfragen ExpertInnen, führt Studien durch und gibt Stellungnahmen ab etc. Das FIfF kooperiert mit zahlreichen Initiativen und Organisationen im In- und Ausland.

Das FIfF-Büro

Geschäftsstelle FIfF e.V.
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
E-Mail:fiff@fiff.de

Die aktuellen Bürozeiten entnehmen Sie bitte unseren Webseiten.

Bankverbindung:
Sparda Bank Hannover eG
Kontoverbindung: 800 927 929
BLZ 250 905 00
IBAN: DE66 2509 0500 0800 9279 29
BIC: GENODEF1S09

FIfF im Netz

Das ganze FIfF:
www.fiff.de

FIfF-Mailingliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/fiff-L
Beiträge an: *fiff-L@lists.fiff.de*

FIfF-Mitgliederliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/mitglieder
Beiträge an: *mitglieder@lists.fiff.de*

Mailingliste Videoüberwachung:
An- und Abmeldung unter
http://lists.fiff.de/mailman/listinfo/cctv-L
Beiträge an: *cctv-L@lists.fiff.de*

Beirat

Michael Ahlmann (Bremen); **Peter Bittner** (Köln); **Dagmar Boedicker** (München)**; Prof. Dr. Wolfgang Coy** (Berlin); **Prof. Dr. Wolfgang Däubler** (Bremen); **Prof. Dr. Leonie Dreschler-Fischer** (Hamburg), **Prof. Dr. Christiane Floyd** (Hamburg); **Prof. Dr. Klaus Fuchs-Kittowski** (Berlin); **Prof. Dr. Michael Grütz** (Konstanz); **Prof. Dr. Thomas Herrmann** (Dortmund); **Prof. Dr. Wolfgang Hesse** (Marburg); **Dr. Eva Hornecker** (Glasgow/UK); **Werner Hülsmann** (Konstanz); **Ulrich Klotz** (Frankfurt); **Prof. Dr. Klaus Köhler** (München); **Prof. Dr. Herbert Kubicek** (Bremen); **Prof. Dr. Klaus-Peter Löhr** (Berlin); **Dipl.-Ing. Werner Mühlmann** (Oppburg); **Prof. Dr. Frieder Nake** (Bremen); **Prof. Dr. Rolf Oberliesen** (Bremen); **Prof. Dr. Arno Rolf** (Hamburg); **Prof. Dr. Alexander Rossnagel** (Kassel); **Prof. Dr. Gerhard Sagerer** (Bielefeld); **Prof. Dr. Gabriele Schade** (Erfurt); **Prof. Dr. Dirk Siefkes** (Berlin); **Prof. Dr. Marie-Theres Tinnefeld** (München); **Dr. Gerhard Wohland** (Waldorfhäslach)

FIfF-Vorstand

- **Stefan Hügel (Vorsitzender)** – Frankfurt am Main
- **Jens Rinne (stellv. Vorsitzender)** – Mannheim
- **Carsten Büttemeier** – Bremen
- **Sylvia Johnigk** – München
- **Prof. Dr. Hans-Jörg Kreowski** – Bremen
- **Prof. Dr. Dietrich Meyer-Ebrecht** – Aachen
- **Kai Nothdurft** – München
- **Raffael Rittmeier** – Bremen
- **Prof. Dr. Britta Schinzel** – Freiburg
- **Julia Stoll** – Grenzach-Wyhlen
- **Ralf E. Streibl** – Bremen
- **Joerg Zeltner** – Köln

Kopieren, ausfüllen und einsenden an:
FIFF e.V.
Goetheplatz 4
D-28203 Bremen
Fax: (0421) 33 65 92 56

Vielzweckschnipsel

Das möchte ich:

- ❑ aktives Mitglied des FIfF werden.
  Normale Mitgliedschaft mit Stimmrecht und Bezug der FIfF-Kommunikation. Der Mindestbeitrag ist für Verdienende **60 Euro** und für Studierende und Menschen in vergleichbarer Situation **15 Euro**. (Für Studierende ist das erste Jahr kostenlos.)
- ❑ förderndes Mitglied des FIfF werden.
  Mitgliedschaft ohne Stimmrecht, z.B. für Institutionen. Der Mindestjahresbeitrag beträgt **60 Euro**.
- ❑ die FIfF-Kommunikation zum Preis von **28 Euro** jährlich frei Haus abonnieren.
- ❑ dem FIfF etwas spenden.
- ❑ Ich überweise den Betrag auf das **Konto 800 92 79 29** bei der Sparda Bank Hannover eG, BLZ **250 905 00** oder nutze die internationale Kontonummer **IBAN: DE05 2509 0500 0000 9279 29** , **BIC: GENODEF1S09.**
- ❑ Der Mitglieds- bzw. Abobeitrag soll per Lastschriftverfahren von meinem Konto abgebucht werden.

Datum _____ Unterschrift _____

Einzugsermächtigung

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

Name: _____

Jahresbeitrag: _____ EUR, erstmals: _____

Konto-Nr.: _____ BLZ: _____

Geldinstitut: _____

Datum _____ Unterschrift _____

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

Die/der bin ich:

Name: _____

Straße: _____

Wohnort: _____

ggf. Mitgliedsnummer: _____

Telefon (privat) _____ (Arbeit) _____

E-Mail: _____

- ❑ Ich möchte als Mitglied per E-Mail über Aktionen, Beschlüsse u.ä. informiert werden; meine E-Mail: _____

Was sonst noch so geht:

- ❑ Ich möchte mehr über das FIfF wissen, bitte schickt mir: _____
- ❑ Ich möchte gegen Rechnung und zuzüglich Portokosten bestellen: _____
- ❑ Ich möchte das FIfF über einen Artikel oder ein Buch informieren: _____
- ❑ Ich möchte zur FIfF-Kommunikation beitragen mit
  - ❑ einem Manuskript zur Veröffentlichung
  - ❑ einer Anregung (siehe unten)

  _____
- ❑ Der Vielzweckschnipsel ist nichts für mich. Ich möchte einen richtigen Brief schreiben.

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	**1.200 Stück**
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Carsten Büttemeier (Koordination), Dagmar Boedicker, Stefan Hügel, Sylvia Johnigk, Hans-Jörg Kreowski, Jens-Holger Streck, Ralf E. Streibl
Schwerpunktredaktion	Carsten Büttemeier und Ralf E. Streibl mit Unterstützung von Dagmar Boedicker, Stefan Hügel, Werner Hülsmann, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Kai Nothdurft und Raffael Rittmeier
V.i.S.d.P.	Ralf E. Streibl
FIfF-Überall	Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert@mtsf.de.* Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *http://www.fiff.de/regional*
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *sj@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *res@fiff.de*
Layout	Berthold Schroeder
Titelbild	»@Welt« von Berthold Schroeder
Druck	Meiners Druck, Bremen

Die FIfF-Kommunikation ist die Zeitschrift des „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V." (FIfF). Die Beiträge sollen die Diskussionen 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 gern erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Aktuelle Ankündigungen

(mehr Termine unter *www.fiff.de*)

27C3: We come in peace
CCC Chaos Communication Congress
27. – 30.12.2010 in Berlin

CPDP 2011 European Data Protection: In Good Health?
The annual Conference Computers, Privacy & Data Protection
25. – 28.1.2011 in Brüssel
http://www.cpdpconferences.org/

Verleihung der BigBrotherAwards
1.4.2011 in Bielefeld
www.bigbrotherawards.de

!!! Stichtag der Volkszählung 2011 !!!
9.5.2011 – siehe auch *www.zensus11.de*

FIfF-Jahrestagung 2011
11. – 13.11.2011 in München

FIfF-Vorstandssitzung
22.1.2011 (Ort noch offen)

FIfF-Kommunikation

1/2011 – »transparenz.arbeit.kontrolle«
Stefan Hügel, Ralf E. Streibl u.a.
(Redaktionsschluss: 2.2.2011)

2/2011 – »IT in Europa«
Stefan Hügel, Dagmar Boedicker u.a.
(Redaktionsschluss: 30.4.2011)

W&F – Wissenschaft & Frieden:

4/10 – Konflikte zivil bearbeiten

1/11 – Moderne Kriegführung

2/11 – Kosten des Krieges

DANA – Datenschutz-Nachrichten:

1/11 – Tagungsnachlese

2/11 – Das Ende personenbezogener Daten als Auslöser von Datenschutz?

Das FIfF-Büro

Geschäftsstelle FIfF e.V.
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
E-Mail: fiff@fiff.de
Die Bürozeiten finden Sie unter *www.fiff.de*

Kontakt zur Redaktion der FIfF-Kommunikation:
redaktion@fiff.de

Wichtiger Hinweis: Postvertriebsstücke wie die FIfF-Kommunikation werden von der Post auch auf Antrag nicht nachgesandt; daher bitten wir alle Mitglieder und Abonnenten, dem FIfF-Büro jede Adressänderung rechtzeitig bekannt zu geben!

Schluss FIfF

Derzeit läuft in vielen Städten der Dokumentarfilm „Plug and Pray“ von Jens Schanze (D 2010, 91min) in den Kinos. Die Premiere des Films fand im Umfeld der FIfF-Jahrestagung in Köln statt. Dort und bei weiteren Diskussionsveranstaltungen zum Filmstart (z.B. in Aachen, Berlin und München) waren FIfF-Mitglieder aktiv beteiligt.

In dem Film kommen verschiedene Protagonisten aus den Bereichen Robotik und Künstliche Intelligenz zu Wort. Eingewoben sind Gespräche mit Joseph Weizenbaum, gedreht nicht lange vor seinem Tod. Bei allen, die die Gelegenheit hatten, Joe Weizenbaum persönlich zu erleben, werden beim Ansehen des Filmes eigene Erinnerungen an Vorträge und Gespräche mit diesem besonderen Menschen wach werden. Wir freuen uns, dass dieser Film dazu beiträgt, das Vermächtnis dieses engagierten und renommierten ‚whistleblowers‘ zu wahren.

Über den Film

Ist der Mensch eine Maschine aus Fleisch? PLUG & PRAY öffnet die Tür zu den geheimen Laboratorien der künstlichen Intelligenz, taucht ein in eine Welt, in der Computertechnologie, Robotik, Biologie, Neurowissenschaft und Entwicklungspsychologie verschmelzen. Es ist beeindruckend, was sie heute schon kann, amüsant, wie sie noch an vielem scheitert und fragwürdig, worauf sie hinaus will. Joseph Weizenbaum, Computerpionier und Kritiker des technologischen Größenwahns, tritt an zu seinem letzten philosophischen Duell mit den Männern, die das nächste Produkt der digitalen Revolution entwickeln: den Roboter, der uns ersetzen soll. In PLUG & PRAY eröffnet Regisseur und Grimmepreisträger Jens Schanze einen Dialog zwischen den euphorischen Forschern und dem altersweisen Professor über die Frage, worin Menschsein eigentlich besteht, der schließlich in ein eindringliches Plädoyer für die Humanität und die Ehrfurcht vor dem natürlichen Mysterium von Leben und Tod mündet.

Weitere Informationen:

plug-pray.de

Geeignete Texte für den SchlussFIfF bitte mit Quellenangabe an *redaktion@fiff.de* senden.