H 7625

FIfF Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

23. Jahrgang 2006 Einzelpreis: 5 EUR **4/2006 - Dezember 2006**

Gesichter des Informatikjahrs

Ein Jahr neuer Reisepass

Informationsfreiheitsgesetz

Versteckte Daten

ISSN 0938-3476

• Aktuelles • FIfF e.V. • viele Fotos •

FIfF Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Titelbild: Berthold Schroeder. Wir danken dem Staatlichen Museum für Völkerkunde München für die Aufnahmegenehmigung und Claus Stark für das Foto vom Roboterhund.

Inhalt

inhalt

Ausgabe 4/2006

Dagmar Boedicker

Editorial

Hoffentlich sind Sie nicht enttäuscht, wenn Sie dieses Heft aufschlagen – mit dem Schwerpunkt hat es diesmal leider nicht geklappt. Warum, das können Sie nachlesen unter *In eigener Sache*. Wir haben statt dessen eine Nachlese gehalten zum Jahr der Informatik, und wir haben eine schöne Fotostrecke mit den besten Bildern des FIfF-Fotowettbewerbs für Sie zusammengestellt. Weil in Schwarz-Weiß und naturgemäß kleinerem Format, kann sie natürlich kein Ersatz für die Ausstellung im Bremer Flughafen sein, aber wer nicht zur Jahrestagung kommen konnte, hat so zumindest einen Eindruck. – Die meisten übrigen Beiträge (siehe unten) haben wie gewohnt einen Inhalt, der nicht gerade beruhigen kann, es ist mir deshalb ein besonderes Vergnügen, eine gute Nachricht mitzuteilen.

Es scheint nämlich, dass die Begehrlichkeiten in puncto personenbezogene Daten manchmal an ganz natürliche Grenzen stoßen, selbst wenn die Hamster-Instinkte mancher Politikerin recht Verfassungs-vergessen daherkommen. Wenn es mit der Bildung nicht so läuft wie gewünscht, kann es ja wohl nur an den Schülerinnen und Schülern liegen? Der Schüler, das unbekannte Wesen, muss dringend erfasst, durchleuchtet, statistisch bewertet werden. *Der* Schüler? Alle! Eine bundesweite Datenbank sollte registrieren, wo es denn hapert bei den Übergängen von einer Schulform zur anderen, einem Bundesland ins nächste. Alles wissen heißt alles richtig machen? So kam vom Bund und der Kultusministerkonferenz (KMK) die Idee, erst mal die Daten aller 12 Millionen Schüler zu erfassen. Alle Schülerinnen und Schüler bekommen ein Personenkennzeichen. Geburtsort, Ursprungsland der Eltern, Sprache zuhause, Bildungsweg, ... werden in den Ländern erhoben und zentral gespeichert. – Vom Bund? Moment mal, der hat doch gerade in der Föderalismusreform alle Schulangelegenheiten an die Länder abgegeben!

Das ist ein erster Stolperstein, über den sich die Möchtegern-Sammler anscheinend genauso wenig Gedanken gemacht haben wie über die informationelle Selbstbestimmung von Schülern und Eltern. Dabei gäbe es auch jetzt schon genug Daten, aber die Lehrer fehlen. In den Jahren seit der ersten PISA-Studie haben sich wirklich genügend Erkenntnisse über die Defizite an den Schulen angesammelt, und es mangelt auch nicht an Lösungsansätzen. Die gute Nachricht ist die, dass dieses Projekt wohl über Gedankenspiele nicht hinauskommen wird, vor allem deshalb, weil etliche Länder ihr knappes Geld lieber nicht für die Erfassung aller Schülerdaten ausgeben möchten. Ein hoffentlich

weiterer Nagel im Sarg ist die Verleihung des *BigBrotherAwards* am 20. Oktober – da hat die Jury einen guten Griff getan (aber das tut sie ja eigentlich immer).

Die Beiträge

Gerrit Hornung von provet (Projektgruppe verfassungsverträgliche Technikgestaltung) gibt in *Ein Jahr neuer Reisepass – quo vadis Biometrie?* einen kritischen und informativen Überblick zu den Problemen mit der Technik, Handhabung und den rechtlichen Grundlagen der Pässe, und er fragt, wie legal die Eingriffe in die Persönlichkeitsrechte der europäischen Bürger eigentlich sind.

Die Privatisierung der Weltpolitik von Tanja Brühl ist ein Nachtrag zum letzten Heft der FIfF-Kommunikation (3/2006 – Entwicklung, Macht und Medien). Tanja Brühl erläutert darin den wachsenden Einfluss privater Akteure in der UN, der sich leider keineswegs bei den zivilgesellschaftlichen Organisationen konzentriert. Ebenfalls ein Nachtrag ist der Artikel von Christoph Dankert aus New York über den *IT-Stacheldraht*. Er beschreibt die Grenzsicherung der USA gegenüber Mittelamerika durch IT-Instrumente. Zu einem internationalen Thema findet sich auch eine Rezension in der Rubrik *Lesen*, die Besprechung des spannenden Sammelbands *Human Rights in the Global Information Society*. Die Rezensionen sind übrigens alle von lesenswerten Büchern.

Dagmar Boedicker

Dagmar Boedicker ist technische Redakteurin und Trainerin für Softwaredokumentation.
Sie hat Politikwissenschaft studiert und ist stellvertretende Vorsitzende des FIfF e.V.

Paul Wagstaff arbeitet zusammen mit Michael Riemer an einem Projekt, das FIfF in internationalem Rahmen zusammen mit anderen Akteuren plant. Er schildert aus seiner langjährigen Erfahrung in der Entwicklungszusammenarbeit Ideen und Randbedingungen für dieses Projekt *Bridging the Digital Divide*, es soll in einer Arbeitsgruppe auf der FIfF-Jahrestagung angeschoben werden. – Ute Twisselmann schreibt auf Englisch unter dem Titel *IT Architecture Landscapes in the Context of Multinational Processes* über die Gründe, warum Unternehmen ihre IT-Architekturen ändern, welche Schwierigkeiten sich dabei in der internationalen Zusammenarbeit ergeben und welche Vorbereitung Projekt-Mitarbeiter und -Leitung dafür brauchen.

Gender ist immer wieder ein Thema in der FIfF-Kommunikation, diesmal haben wir einen Bericht: von Kordula Kugele und Martina von Gehlen über die Erfahrungen mit der *informatica feminale* in Freiburg, die dieses Jahr schon zum 6. Mal stattgefunden hat. Einen Bericht zum 10. Jubiläum der *informatica feminale* in Bremen werden wir hoffentlich im nächsten Heft bringen können.

In ihrem Beitrag *Versteckte Informationen in elektronischen Dokumenten* schreibt Barbara Wiesner mit Studierenden über versteckte Daten, die man in Microsoft Word Dokumenten und anderen Formaten findet. Die Gruppe hat nicht nur analysiert, welche Informationen in Dokumenten zu finden sind, sondern auch, welche Fehler der Benutzer zu dieser ungewollten Transparenz führen können.

Annette Hauschild bewertet das Informationsfreiheitsgesetz, das seit 1. Januar 2006 in Kraft ist; Dietrich Meyer-Ebrecht macht sich Gedanken zur Software-Fehlern im Auto, und wir drucken eine Rede der Abgeordneten Silke Stokar (Grüne/B 90) unter dem Titel *Informationspflicht für Unternehmen bei Datenschutzpannen einführen*.

Und dann gibt es natürlich wieder Neuigkeiten in der Rubrik FIfF e.V., beispielsweise in Stefan Hügels Beitrag FIfF International über die Mitgliedschaft des FIfF in *EDRi (European Digital Rights)* und der *European At-Large Organisation* des ICANN. Hans-Jörg Kreowski erzählt in seinem *Brief an das FIfF* von der Tagung *Informatik und Rüstung*, etwas ausführlicher tut das Ingo Ruhmann in seinem Bericht von der Tagung, die übrigens gut besucht und offensichtlich sehr interessant war.

Eine informative Lektüre wünscht,

Dagmar Boedicker

Hans–Jörg Kreowski

Brief an das FIfF

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser der FIfF-Kommunikation,

am 29. und 30. September 2006 fand an der Humboldt-Universität zu Berlin in Adlershof die Tagung *Informatik und Rüstung* statt. Sie lief als eine Veranstaltung der Wissenschaftsjahre 2005 und 2006 (Einsteinjahr und Informatikjahr), gefördert vom Bundesministerium für Bildung und Forschung.

Neben Arbeitsgemeinschaft für Friedens- und Konfliktforschung (AFK), Deutsche Stiftung Friedensforschung (DSF), Forschungsverbund Naturwissenschaft, Abrüstung und internationale Sicherheit (FONAS), NaturwissenschaftlerInnen Initiative Verantwortung für Frieden- und Zukunftsfähigkeit (NATWISS) und Vereinigung Deutscher Wissenschaftler (VDW) trat auch das FIfF als Veranstalter auf und hatte einen maßgeblichen Anteil an der Programmgestaltung (siehe www.einstein-weiterdenken.de für nähere Informationen). Die Veranstaltung hatte 130 angemeldete Teilnehmerinnen und Teilnehmer; am Freitagabend zur Eröffnung waren noch mehr da – sicher auch dank der Zugkraft von Joseph Weizenbaum.

Mich hatten die Organisatoren um ein 20-minütiges Referat zum Thema *Verantwortung des Informatikers heute* gebeten, das als Einführung für eine am Samstagnachmittag folgende Arbeitsgruppe zum selben Thema dienen sollte. Es folgt eine kurze Zusammenfassung.

Schon das Wort Verantwortung ist mit den Silben *ant* und *wort* sehr interessant, verlangt es doch eine Gegenposition oder Gegenrede. Lawinen und Wirbelstürme haben keine Verantwortung für die eintretenden Folgen, sie geschehen. Vernunftbegabte Menschen, die gleichzeitig und vielleicht noch viel stärker unvernunftbegabt sind, können sich in ihrem Denken und Handeln zwischen verschiedenen Optionen entscheiden. Verantwortung erwartet eine Entscheidung zugunsten der Vernunft. Leider ist es in Einzelfällen nicht immer einfach zu wissen, was vernünftig ist, und es wird häufig verschiedene Sichten geben. Verantwortungsvolles Tun ist keine Ja-Nein-Entscheidung, sondern bedarf der Auseinandersetzung. Viele Menschen können sich recht schnell darauf verständigen, dass das Führen von Kriegen – zumindest von Angriffskriegen – verantwortungslos ist. Im 2. Buch Mose 20 fordert das fünfte Gebot „Du sollst nicht töten". In §2(2) des Grundgesetzes der Bundesrepublik Deutschland wird das „Recht auf Leben und körperliche Unversehrtheit" garantiert. Christlich gebundene und demokratisch denkende Menschen sollten also kein Problem mit einer pazi-

fistischen Grundhaltung haben. Mit der Charta der Vereinten Nationen versprechen 192 Staaten, dass sie „künftige Generationen vor der Geißel des Krieges … bewahren wollen." Dass in den 60 Jahren, die es die UN-Charta bereits gibt, dieses Prinzip hundertfach verletzt worden ist, spricht nicht gegen die Utopie, sondern zeigt, dass noch viel geschehen muss, bis Vernunft die Welt regiert. Zumindest auf dem Papier sind sich die Vereinten Nationen auch darüber einig, dass zu einem friedlichen Miteinander nicht nur die Abwesenheit von Krieg gehört, sondern auch die Wahrung der Menschenrechte und die Förderung „sozialen Fortschritts und eines besseren Lebensstandards in größerer Freiheit". Die Erkenntnis, dass die Staaten der Welt eine Verantwortung für Frieden, Menschenrechte und ein menschenwürdiges Leben aller haben, ist keine Erfindung des 20. Jahrhunderts und bedurfte nicht zweier Weltkriege. Beispielsweise hat Immanuel Kant (1724 - 1804) in seiner Schrift *Zum ewigen Frieden* Elemente der UN-Charta vorweggenommen. Es heißt dort u.a.:

„Stehende Heere sollen mit der Zeit ganz aufhören ... Die bürgerliche Verfassung in jedem Staate soll republikanisch sein". (Dabei ist *republikanisch* im Sinne von *demokratisch* gemeint.) Bemerkenswert ist, dass Kant nicht nur Kriege verhindern will, sondern totale Abrüstung empfiehlt, die das Führen von Kriegen gänzlich unmöglich machen würde.

Die Überlegungen von Kant sind in neuerer Zeit zum Beispiel von Hans Jonas (1903 – 1993) in seinem Werk *Das Prinzip Verantwortung* aufgegriffen worden. Er fordert: „Handle so, dass die Wirkungen deiner Handlungen verträglich sind mit der Permanenz menschlichen Lebens auf der Erde". Sein Ausgangspunkt ist die Einsicht, dass die technologischen Entwicklungen inzwischen so weitreichend, nachhaltig und potenziell vernichtend sind, dass der verantwortliche Umgang mit diesen Technologien allergrößte Vorsicht verlangt. Von Hans Jonas ist der Schritt zur Informatik nicht weit. In den Ethischen Leitlinien der GI (Gesellschaft für Informatik) liest man im Artikel 11 über Soziale Verantwortung: „Die GI unterstützt den Einsatz von Informatiksystemen zur Verbesserung der lokalen und globalen Lebensbedingungen. Informatikerinnen und Informatiker tragen Verantwortung für die sozialen und gesellschaftlichen Auswirkungen ihrer Arbeit; sie sollen durch ihren Einfluss auf die Positionierung, Vermarktung und Weiterentwicklung von Informatiksystemen zu ihrer sozial verträglichen Verwendung beitragen". Es wäre wohl zu viel verlangt, von der GI klare und eindeutige Präzisierungen zu erwarten. Hervorzuheben ist allerdings, dass diese Organisation, die über 20.000 Informatikerinnen und Informatiker vertritt, überhaupt zugesteht, dass die Arbeit in der Informatik und mit den Methoden und Technologien, die die Informatik hervorbringt, zu ethischen Problemen und Konflikten führt und Verantwortung mit sich bringt. Ich möchte ergänzend ein paar Punkte ansprechen, die aus meiner Sicht zu einer verantwortlichen Informatik gehören. In erster Linie gilt es, zu mahnen und zu warnen vor der Nutzung von I&K-Technologie bei der Perfektionierung der militärischen Tötungsmaschinerie, der ersatzlosen Vernichtung von Erwerbsarbeit und der massiven Einschränkung von Grundrechten. Das sind unverändert die Forderungen an verantwortungsbewusste Informatikerinnen und Informatiker, die das FIfF seit seiner Gründung unterstützt und mit denen es sich im Einklang mit den Postulaten der Verantwortungsethik befindet. Mit der immer weiter vorangetriebenen Ausbreitung der Computertechnik in alle gesellschaftlichen Bereiche und den vorläufig nur schemenhaft absehbaren Folgen sowohl bezüglich der Chancen als auch der Risiken muss Verantwortung weiter reichen. Es ist an der Zeit, sich phantasievoll und kreativ einzumischen in Fragen der Nutzung von I&K-Technologie.

Wie kann sie beim Herstellen friedlicher Strukturen eingesetzt werden, die Krieg nicht nur unnötig, sondern auch unmöglich machen? Wie beim Überwinden der digitalen Spaltung? Wie beim Schaffen von Arbeitsplätzen? Wie kann die elektronische Überwachung so kontrolliert werden, dass sie im gesetzlich erlaubten Rahmen bleibt, und wie technisch so ausgelegt werden, dass sie erst gar nicht missbraucht werden kann? Wie lässt sich ein Gegengewicht zur Technikeuphorie bilden, das die nötige Ernsthaftigkeit beim Umgang mit Technik herstellt, ohne sie zu verteufeln? Wie kann man faire Chancen für eine kritische Wissenschaft erreichen? Bei der letzten Frage denke ich vor allem daran, dass in den Industrieländern viele Milliarden für Forschungsförderung ausgegeben werden, die ganz überwiegend dem Militär, der Wirtschaft und dem Staat mit seinem Verwaltungsapparat zugute kommen, während für die Frage der Verantwortbarkeit der wissenschaftlichen und technischen Entwicklungen nur ein verschwindend geringer Bruchteil zur Verfügung steht. Da die Tagung mit Mitteln finanziert wurde, die vom Einsteinjahr 2005 übrig geblieben sind (also aus diesem Bruchteil), und deshalb auch unter dem Motto stand „Einstein weiterdenken", möchte ich mit einem Einstein-Zitat schließen: „Das Denken der Zukunft muss Kriege unmöglich machen." Dem ist an dieser Stelle und in diesem Moment nichts hinzuzufügen.

Mit fiffigen Grüßen

Hans-Jörg Kreowski

Dagmar Boedicker

In eigener Sache

Überraschungen sind nicht immer angenehm, sie können mit viel Arbeit und Ärger verbunden sein, stressig und hektisch. Angekündigte Überraschungen können noch unangenehmer sein, wenn auf drängendes Nachbohren die nagenden Zweifel an der Zuverlässigkeit einer Schwerpunktredaktion bestätigt werden durch ein dürftiges „Ich bin dran ...". Dann müssen alle in der Redaktion Sonderschichten einlegen und sehen, wo sie Beiträge finden. Dafür, dass auch diesmal wieder eine FIfF-Kommunikation entstanden ist, herzlichen Dank an alle, die geholfen haben!

Nachschlag zum vorigen Schwerpunkt

Entwicklung, Macht und Medien

Christoph Dankert

Der IT-Stacheldraht

Grenzsicherung gegen Mittelamerika durch IT-Instrumente

Abrupt bremst der Fahrer des 10 Jahre alten Vans auf der staubigen Straße, wenige Meilen vor der Grenze zur Hoffnung auf ein besseres Leben. In der Erwartung, die Armut endgültig hinter sich zu lassen, ist Antonio so aufgeregt wie noch nie in seinem Leben. 1.500 Dollar – mehr als das Dreifache des durchschnittlichen Monatslohns eines Arbeiters in Mexiko – hat er dem Fahrer des Vans bezahlt, um ihn ins Land der unbegrenzten Möglichkeiten zu bringen. Die Luft ist noch immer heiß, obwohl es mittlerweile drei Uhr nachts sein müsste. Plötzlich kommt im Hintergrund Motorengeräusch auf, und bald darauf werden die Umrisse eines kleinen Flugzeugs deutlich. Dies ist eine der neuen unbemannten Überwachungsdrohnen, die die US-Grenzschützer in diesem stark frequentierten Teil der Grenze einsetzen. Dank neuartiger Bildverarbeitungsverfahren erkennen diese Drohnen Menschen im Umkreis von bis zu 10 km und mit Hilfe der Infrarotkameras sogar nachts. Die Bewegungssensoren entlang der Grenze signalisieren zusätzlich, wenn Menschen sich der Grenze nähern. Und schließlich gibt es noch die fest installierten Kameras entlang der Grenze, die mit dem Grenzkontrollsystem gekoppelt sind und Wiederholungstäter sofort mit Namen und Anschrift identifizieren. – Was hier wie eine Szene aus einem Science-Fiction-Film klingt, ist an der Grenze zwischen den USA und Mexiko fast schon Realität.

Die 3.141 km lange Grenze zwischen Mexiko und den Vereinigten Staaten von Amerika ist eine der meistfrequentierten Grenzen in der Welt. Nach den Angaben der US-Botschaft in Mexiko überqueren jedes Jahr etwa 350 Millionen Menschen die Grenze via Flugzeug, per Schiff, im Bus, Auto, LKW oder zu Fuß. Etwa eineinhalb Millionen davon, so schätzt das *Pew Hispanic Center,* sind illegale Einwanderer. Rund 80 % davon kommen aus Mexiko selbst, und weitere 20 % kommen aus Mittel- und Südamerika.

Als traditionelles Einwanderungsland sind die Debatten um die Sicherung der Grenzen der USA so alt wie die Grenzen selbst. Die 1848 endgültige fixierte Grenze mit Mexiko ist jedoch, im Gegensatz zur Grenze mit Kanada, das größere Problemkind. Die illegalen Einwanderer, die oft vor erschreckender Armut in die als Paradies anmutenden Vereinigten Staaten fliehen, sind vor allem der US-Landwirtschaft als billige Arbeitskräfte mehr als willkommen. Nach einer Studie der University of California in Davis sind etwa 45 % aller landwirtschaftlichen Arbeiter in den USA illegale Einwanderer, und dies hat seinen Grund unter anderem darin, dass US-Amerikaner diese Arbeit nur ungern verrichten würden und viele offene Stellen ohne die illegalen Einwanderer nicht besetzt werden könnten. Das Argument der Gegner illegaler Einwanderer lautet hier, dass die Stellen nur deshalb nicht besetzt werden können, weil sie wegen der illegalen Einwanderer nicht besser bezahlt zu werden brauchen.

In den letzten Jahren ist die Zahl der illegalen Einwanderer dank jährlicher Zuwächse von 500.000 bis 850.000 auf 7 bis 20 Millionen gestiegen (12 Millionen ist eine allgemein akzeptierte Zahl) und die Rufe nach Begrenzung des Zustroms über die Grenze werden lauter. War dies in der Vergangenheit meist der Ruf nach mehr Grenzpatrouillen, so ist es mittlerweile der Ruf nach einem durch Informationstechnologie zu einer Barriere aufgerüsteten Zaun oder einer Mauer.

Die unter Präsident Bill Clinton ins Leben gerufene *Operation Gatekeeper* (Operation Torhüter) machte in Kalifornien den Anfang und verdreifachte die installierten Bewegungssensoren am Westende der Grenze und führte das IDENT-System ein, mit dem Wiederholungstäter über eine Datenbank identifiziert werden sollten. Ein Abgleich mit Strafregistereinträgen für Ausländer ist ebenfalls Bestandteil des Systems. Ähnliche Projekte gibt es noch an vielen anderen stark frequentierten Abschnitten der Grenze mit Namen wie *Operation Hold-the-Line* (Operation Dranbleiben) in Texas und *Operation Safeguard* (Operation Absicherung) in Arizona.

Spätestens seit dem 11. September 2001 ist die Grenzsicherung zu einer Aufgabe nationaler Priorität gewachsen, da die relativ offene Grenze zu Mexiko nun als potenzielles Einfallstor für Terroristen gesehen wird:

> *First, America's air, land, and sea borders must provide a strong defense for the American people against all external threats, most importantly international terrorists but also drugs, foreign disease, and other dangerous items.*
> *Die primäre Aufgabe der Luft-, Land- und Seegrenzen von Amerika muss die Verteidigung der amerikanischen Bevölkerung gegen alle externen Bedrohungen sein, vor allem gegen internationale Terroristen, aber auch gegen Drogen, fremde Krankheiten und andere gefährliche Dinge. (http://www.whitehouse.gov/, Securing America's Borders Fact Sheet, 25.01.2002)*

Im März 2002 wurde der *Smart Border Action Plan* (Aktionsplan Intelligente Grenze) in Kraft gesetzt, von dessen 22 Punkten sechs explizit auf technologische Maßnahmen abzielen:

- Flugdatenübermittelung ähnlich dem Verfahren zwischen den USA und der EU,
- kompatible Datenbanken zwischen den Grenzbehörden und Geheimdiensten der USA und Mexikos, um im Bedarfsfall Informationen schnell und einfach austauschen zu können,
- elektronischer Austausch von Zollinformationen,
- elektronische Sendungsverfolgung für Waren im Transitverkehr,
- Technologietransfer, um Mexiko mit High-Tech wie elektronischen Containersiegeln und elektronischen Nummernschild-Lesern auszustatten sowie
- Videoüberwachung der Eisenbahn-Grenzübergange.

Im Jahr 2005 definierte die US-Grenzkontrollbehörde den Einsatz sogenannter *Smart Border*-Technologie als eine ihrer fünf Hauptaufgaben zum Schutz der US-amerikanischen Grenzen und machte damit klar, dass der Einsatz von moderner Technologie integraler Bestand der Grenzkontrolle sein wird. Mit der *Secure Border Initiative* machte Präsident George W. Bush die zentrale Rolle moderner Technologie, insbesondere Informations- und Kommunikationstechnologie, für die Sicherung der Grenze zu Mittelamerika klar.

> *We're launching the most technologically advanced border security initiative in American history.*
> *Wir starten gerade die am weitesten technologisch fortgeschrittene Initiative zur Grenzsicherung in der amerikanischen Geschichte. (Präsident George W. Bush in seiner Rede zur Lage der Nation vom 15.05.2006)*

Und einige dieser Technologien werden bereits eingesetzt. Im Tucson-Sektor der Grenze befindet sich das neue Lagezentrum der Grenzschützer in einem neuen, teuren Glasbetonbau. Der Kontrollraum ist mit 25 Videobildschirmen ausgestattet und vernetzt Informationen, die von den Bewegungssensoren, Kameras und den zwei unbemannten Drohnen kommen, die entlang dieses 400 km langen Abschnitts der Grenze stationiert sind. Kameras und Bewegungssensoren sind über das selbe Kontrollzentrum steuerbar, so dass der Beamte vor dem Bildschirm leicht

Abb. 1: Mit High-Tech versuchen die USA illegale Einwanderer vom Überqueren der Grenze abzuhalten

einen Blick auf das Gebiet werfen kann, in dem ein Bewegungssensor Alarm schlägt.

Die Vorschläge für neue Grenzsicherungstechniken reichen von Infrarotkameras auf Trucks, die sich vom Beifahrer per Joystick steuern lassen, über die Vernetzung sämtlicher Kameras in einem Grenzabschnitt, um anschließend mit Bilderkennungssoftware Menschen ausfindig zu machen, bis hin zu einer Kette von Heißluftballons, um darüber ein Netzwerk zum Übertragen der Sensorinformationen über Hunderte von Kilometern möglich zu machen. Es winken hier Verträge zur Grenzsicherung im Gesamtwert von 2 Milliarden Dollar, und so scheint der Kreativität keine Grenze gesetzt.

Doch neben der Hurra-Stimmung macht sich selbst im Lager der Befürworter einer strikten Absicherung der Grenze etwas Katerstimmung breit. Im April diesen Jahres stürzte eine der unbemannten Drohnen ab, die zur Grenzsicherung in Arizona eingesetzt wurde. Die Drohne vom Typ *Predator B* (Jäger B) sollte in 10 bis 15 km Höhe über die Grenze fliegen und war mit High-Tech-Kameras ausgestattet, die selbst durch Wolken hindurchsehen können. Nachdem das Kontrollzentrum Kontakt zur Drohne verloren hatte, stürzte sie am 25. April in der Nähe der Grenzstadt Nogales in Arizona ab. Das nach dem 11. September in Gang gesetzte *Integrated Surveillance Intelligence System* (ISIS) scheiterte an der mangelnden Integration verschiedener Komponenten – so sollten Kameras mit Sensoren gekoppelt

Christoph Dankert

Christoph Dankert (24) studierte Informatik an der Universität Frankfurt und der University of Waterloo in Kanada. Er arbeitet seit Januar 2006 als Unternehmensberater in New York und beschäftigt sich beruflich mit Finanz- und Krankenversicherungsthemen. Privat interessiert er sich insbesondere für das Spannungsverhältnis zwischen Privatsphäre und Schutz vor Bedrohungen durch den Staat.

werden, um automatisch in Richtung eines Sensoralarms gerichtet zu werden. Im Endeffekt kostete dieses Programm weit mehr als ursprünglich geplant.

Allen Skeptikern zum Trotz wurde dieser Vertrag am 20.9.2006 an Boeing vergeben und sieht die Installation eines *virtuellen Zauns* durch ein Netzwerk von 1.800 Kontrolltürmen mit Kameras, Bewegungsmeldern und Radar entlang der Landgrenzen der USA vor – ein Großteil entlang der mexikanischen Grenze.

T. J. Bonner, Präsident des *National Border Patrol Council* und Vertreter der 11.000 Grenzschutzbeamten, glaubt nicht an eine technologische Lösung des Einwanderungsproblems. Er sieht die Beamten schon jetzt überfordert und glaubt, dass man vielmehr die Ursachen angehen muss, die die USA so attraktiv für illegale Einwanderer machen:

> *As long as we're not cracking down on the employers, less of the number of cameras or fences that you have.*
> *So lange wir nicht bei den Arbeitgebern hart durchgreifen, werden die Menschen weiterhin über die Grenze kommen, ganz egal, wie viele Kameras oder Zäune wir haben werden.*

Das ist selbst Präsident Bush klar, doch mangels einer politischen Einigung um das Problem der illegalen Einwanderer setzen die USA zunächst auf die technologische Karte.

Paul Wagstaff

Bridging the Digital Divide

Options for Action

Die revolutionsähnliche Entwicklung der Informationstechnik (IT) betrifft alle Länder und doch gibt es im Nutzungsmaß und in der Nutzungsart gewaltige Unterschiede zwischen einzelnen Ländern und Regionen. Es ist heutzutage ausgeschlossen, am Welthandelsgeschehen teilzunehmen, ohne einen Zugang zur Informationstechnik zu haben, aber Entwicklungsländer stehen vor vielen Hürden, bevor sie Informationstechnik adaptieren und nutzen können. Der Begriff Digital Divide bezieht sich auf die Kluft zwischen den Ländern, die Informations- und Kommunikationswerkzeuge wie Computer und Internet effektiv nutzen können, und jenen, denen dies bislang nicht möglich ist.

A previous paper (FIfF-Kommunikation 3/2006, p. 28) described the main technical, social, economic and political barriers that contribute to the Digital Divide in Less Developed Countries (LDCs). Many of the barriers can only be removed through action by national governments and international agencies, like the ITU. This paper concentrates on activities that can be undertaken by individuals, companies, associations and NGOs working in IT in the West to help reduce the Digital Divide.

Introduction

Why should computer professionals in the West be concerned about the "Digital Divide"? There are important humanitarian reasons for bridging the digital divide, but there are also good business reasons: the poor are a market. Few companies understand how to reach this market, but those who do understand rapidly dominate the market. A few examples: European-based Telecommunication Companies almost lost the African cellular market to South African companies through poor understanding of the markets, something similar has happened to a European car manufacturer which once dominated Africa. For almost 30 years most non-luxury cars and pick-ups in East Africa were Peugeots but I have not seen a Peugeot in East Africa for many years. Peugeot has lost a market that it once dominated to the Japanese car manufacturers. Currently Telecommunication Companies in East Africa are replacing their European switches with Chinese Huawei switches – which are cheaper to buy and easier to maintain by local technicians.

Very few people in LDCs can afford $1,500 computers but the potential market for cheap computers, at less than $300 with low power requirements, is huge. The potential for broadband internet access via cables (copper or glass) is limited but the number of potential customers for slower but cheap and reliable wireless connections is as large as the demand for cheap computers.

International Action

The ITU has assumed the role of coordinating international activities to bridge the digital divide. The ITU organised the World Summit on the Information Society (WSIS), which has gone through several phases: Geneva, December 2003, and Tunis, November 2005. Many of the initiatives supported by ITU and its member states and organisations are listed in the ITU/WSIS Golden Book [1][1], which is partly intended to measure how far member states / organisations have gone in achieving the commitments made at the two WSIS. As the ITU / WSIS is a multilateral organisation the Golden Book initiatives tend to reflect activities by the multilateral agencies (UN, World Bank, EC, etc), bilateral donors, governments and large international companies, though some NGO initiatives are also listed. Though these initiatives are welcome, they will not open all the barriers to uni-

versal access to ITC. Activities by a Communications Ministry to promote ITC will have only limited success if the Ministry is reluctant to support free and fair competition in the telecommunication sector, and other barriers need action by individuals in the IT industry – like web site design. This paper focuses on small-scale activities that can be carried out by individuals, associations and NGOs interested in Bridging the Digital Divide.

Awareness

Probably the most important activity is to spread awareness of the problems and potentials of the Digital Divide within the IT industry. This costs very little but could produce very useful results. Some examples:

Web site design

If your web site takes 5 minutes to download via a slow Internet connection few people in LDCs will be able to access it. Solution: offer an alternative version of your web sites without the animated graphics, video clips, photos, etc. Can you reduce the number of pages that a visitor to your site has to open to get information from your site? If a customer has to download more than 5 web pages to access your information or buy your product the connection may have disconnected before the customer can make the purchase! Have you used file compression for any pages that can be downloaded?

Software design

Can your software work on old, slow computers, old operating systems (OS) or Linux? Could you produce a "light" version of your software for slower processors, limited memory and old OS? Can you provide software documentation in other languages, or use simplified English? Can your software work with wireless or VSAT devices? If your software requires an Internet connection, can it cope with limited bandwidth, slow speeds, and disconnections?

Hardware design

Can your hardware work with wireless or VSAT devices, or slow dial-up connections? How does your hardware cope with voltage fluctuations, dust, and high humidity? Could your hardware run directly from 12V DC? Many power supply problems would disappear if all IT equipment used 12/24V DC! How simple is the documentation? Can your hardware be installed by someone with limited English skills? Can your hardware and drivers work with old OS, slow processors and Linux? Can you modify existing technologies to make them more suitable for developing countries or support the development of entirely new technologies?

Technical / Industry Associations

Are you a member of a technical or industry association? Can your association help to remove barriers to the use of technology by, for example, promoting "Type Approval" and equipment standardisation within your industry?

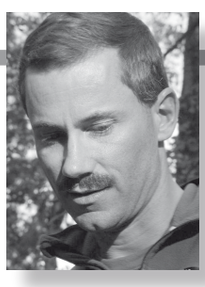
Courses

If you are a Lecturer / Course Director could you make your courses available to students in LDCs over the Web? Can your course material be accessed with a slow, unstable internet connection? Do you use file compression for downloading course material?

Membership of Networks involved in IT and Development

There are several networks specialising in IT and development issues. Through these networks members can share information, encouraging the development of cheap, affordable computers, peripherals and internet access; promote the use of open source software to reduce costs; and lobby for government policies to encourage the private sector to supply IT equipment; education and training policies; support for IT infrastructure; availability of software, and fair copyright and piracy laws. Some suggestions:

1. E-learning: The Commonwealth of Learning, *www.col.org*
2. IT and development: One World Digital Opportunity Network: *www.digitalopportunity.org*
3. IT and development: The Communication Initiative: *www.comminit.com*



Paul Wagstaff

Paul Wagstaff is a Rural Development Consultant with 14 years experience of struggling to use information technology in rural East Africa and Nepal. He has worked for British, German and Austrian NGOs, the European Union and government ministries in developing countries. His most recent work has been developing Market Information Systems (MIS) to enable small-holder farmers in Uganda to access data on crop prices and market demand.

4. IT and development: *www.digitaldividenetwork.org*

5. IT and development: Association for Progressive Communications (APC), *www.apc.org*

Internships in LDCs

Develop an Internship program to enable computer science students, computer education students and interested IT professionals to work for a short period (4-8) weeks in an LDC as part of a 5-year program. The internship program would help students to understand the realities of the Digital Divide, as well as directly helping to overcome some of the problems of the Digital Divide. The internships could be in a range of projects:

a) Secondary schools and secondary level colleges teaching basic IT skills (word processing, spreadsheets, internet, emails) to students and teachers.

b) Tertiary level colleges (universities, vocational and professional training institutes) teaching professional software skills to students and lecturers: CAD, database design, Linux, accounting software, network administration, GIS, etc.

c) Special education. Improving access to ITC technology for those with special needs (software and hardware for the blind, physically disabled, etc.).

d) Building the capacities of educational institutes to maintain their own ITC equipment and networks.

e) Building the capacities of the private IT sector by working with local computer technicians and small IT companies to exchange skills in computer maintenance and technology and develop IT Consultancy Services.

f) Increasing awareness of the opportunities provided by ITC through small projects with development projects, cooperatives, special interest groups (for example groups for the disabled, orphans, women, etc) and small business. These projects could include setting up community Telecenters, setting up office networks, installing wireless technology, designing databases, converting to open source software, setting up e-business software, converting to electronic bookkeeping, etc.

g) Cooperation with other development organisations. Too many computers donated to development projects remain in boxes because there is no one to install the equipment, or the equipment breaks down and is not repaired, so many donors have become disillusioned with financing ITC projects. Interns could help to install the equipment and to train local staff in maintenance, with the donor providing the hardware.

Internships in Europe

Arrange for IT professionals from LDCs to spend time working with IT companies in Europe, for example: teaching, software design, hardware design and maintenance, IT journalism, e-business, etc.

Short Courses (*Summer Schools*)

Interested IT professionals from Europe could help to organise short courses in LDCs. These could be short seminars (2-3 days) or longer technical training courses. Some ideas:

1. General seminars on the benefits of open source software for managers.

2. 3 week technical courses on open source software for IT technicians and network managers.

3. Seminars for farmers' cooperatives, women's groups, disabled groups, etc, on the potential for using the Internet for business.

4. 3 week courses on creating commercial web sites for IT consultants, small business consultants and Web Designers, who would then assist cooperatives, etc. to develop commercial web sites.

In order to strengthen local initiatives and to avoid disrupting the local "market", the courses need to be run jointly with local organisations and companies.

Recycling Used Computer Equipment

An ethical program for recycling computers requires decommissioning, certification, storage and testing facilities. It may be possible to develop a partnership with an organisation like Computer Aid International or World Computer Exchange to recycle

Glossary

ITU	International Telecommunications Union
LDC	Less Developed Country
NGO	Non Governmental Organisation
Telecenter	Business that provides telecommunication services for use by the public
VSAT	Very Small Aperture Terminals, a 2-way satellite ground station with a dish antenna that is smaller than 3 meters

computers from German companies (cf. FIfF-Kommunikation 3/2006, p. 32).

Individual projects in LDCs – a few Words of Warning

There are many examples of organisations and individuals from the industrialised countries providing technical and financial support to IT projects in LDCs: setting up computer departments in schools, creating Telecenters, connecting villages with wireless networks, etc. A good example is a project to connect villages in Nepal: *http://nepalwireless.net*. When planning small projects it is vital to learn from the mistakes of the past, but getting the right information is not always easy. Every project described in NGO reports and web pages is a 100% success (!?) but on the ground it is easy to become disillusioned as the failures seem to exceed the successes. Though IT projects are conceived to Bridge the Digital Divide between the West and LDCs, projects can increase the divide within communities: women may miss computer classes because they have to collect firewood, water or look after sick children; fast learning, IT savvy farmers will have a business advantage over the illiterate farmers in the village; boys have plenty of free time to surf the internet but girls have to help with the housework.

FIfF Annual Meeting (Jahrestagung 2006)

Bridging the Digital Divide will be one of the themes for this year's FIfF annual meeting in Bremen (4-5th November), with invited speakers from organisations involved in Bridging the Digital Divide and a forum for discussions. If there is enough interest FIfF will create a permanent working group which will develop specific projects to Bridge the Digital Divide.

FIfF is interested in contacting NGOs, research institutes, consultants and development agencies that may be interested in joining the working group and / or giving a poster presentation of their activities at the FIFF annual meeting. Of special interest are organisations that have experience in the following issues:

- Research on social issues relating to IT and development.
- Research on economic and policy issues related to IT use in developing counties.
- Raising awareness / advocacy of IT issues in international development.
- Supporting ICT projects in developing countries.
- Supporting or designing IT infrastructure projects in developing countries.
- Sending technical IT experts (short or long term) to developing countries.
- Organising internships and work placements for European IT students and volunteers in developing countries.
- Organising scholarships, training courses and exchange programs for IT students and professionals in developing countries.
- Developing hard and software, including telecommunications equipment, suitable for developing countries.
- Developing E-training / virtual training courses for students in developing countries.
- Sending recycled IT equipment to development projects.

1 ITU / WSIS: Golden Book, February 2006, www.itu.int/wsis/goldenbook

Tanja Brühl

Die Privatisierung der Weltpolitik -

die Vereinten Nationen öffnen sich für private Akteure

Lange Zeit fand internationale Politik in und zwischen Staaten statt. Die Staats- und Regierungschefs stellten die Weichen im nationalen wie internationalen Geschehen. Dieses Verständnis von internationaler Politik ist überholt. Neben den Staaten bestimmen heute zunehmend private Akteure die Weltpolitik. Sie beeinflussen die Ausarbeitung, Festlegung und Umsetzung von internationalen Normen und Vereinbarungen. In einzelnen Bereichen setzen sie sogar selbst diese Regeln fest. Wer sind diese privaten Akteure, und welche Ziele haben sie? Lösen sie bestehende Probleme besser? Und welche Folgen hat diese Privatisierung der Weltpolitik für die Legitimität der Entscheidungen?

Die Gruppe der privaten Akteure ist äußerst heterogen. Sie umfasst sowohl kleine, basisorientierte *NGOs (Non-Governmental Organizations)* wie auch große internationale Unternehmensverbände. Somit zählen neben zivilgesellschaftlichen Organisationen auch privatwirtschaftliche Unternehmen zu den privaten Akteuren. Während die einen sich tendenziell freiwillig engagieren und keine Gewinnerzielungsabsicht haben, ist für die anderen gerade die Profitmaximierung das Ziel. Die privaten Akteure haben ganz unterschiedliche, teils auch gegensätzliche politische Ziele, setzen auf unterschiedliche Strategien und haben mehr oder weniger Macht. Gemeinsam ist ihnen, dass sie sich – alle auf die eigene Art und Weise – zunehmend in der Norm- und

Regelsetzung engagieren. Sie tragen dadurch zur „Privatisierung der Weltpolitik“ (Brühl et al. 2001) bei.

Jeder auf seine Art

Private Akteure können versuchen, zwischenstaatliche Aushandlungsprozesse zu beeinflussen, etwa durch Lobbying oder Teilnahme an internationalen Verhandlungen, oder aber sie sind selbst als gleichberechtigte Akteure an der Regelsetzung beteiligt. Private Akteure kooperieren in *Public-Private-Partnerships (PPP)* mit Staaten und/oder internationalen Organisationen und einigen sich dazu auf gemeinsame Regeln. Sie stellen freiwillige oder verbindliche Verhaltensstandards für bestimmte Branchen auf, ohne hierin öffentliche Akteure einzubeziehen (private Regulierung). Während private Akteure bis zu den 1990er Jahren vor allem anstrebten, internationale Vereinbarungen zu beeinflussen, so sind sie seitdem zunehmend direkt in die Regelsetzung einbezogen.

In der internationalen Umweltpolitik tritt die gewachsene Bedeutung der privaten Akteure besonders offen zu Tage. Anfangs setzten auch hier vor allem die Staaten Normen und Regeln fest. Private Akteure, insbesondere NGOs, nahmen zwar als Beobachter an den internationalen Konferenzen teil, hatten jedoch nur begrenzte Einflussmöglichkeiten. In den letzten Dekaden nahm die Zahl der sich engagierenden privaten Akteure deutlich zu, und ihr Handlungsspielraum ist stark gewachsen. Die Gruppe der privaten Akteure setzt sich anders zusammen, da immer mehr Unternehmen auf dem internationalen Parkett die Regelsetzung zu beeinflussen suchen.

Umwelt- und Entwicklungspolitik der Vereinten Nationen

Drei Weltkonferenzen, die die Vereinten Nationen zum Thema Umwelt bzw. Umwelt- und Entwicklungspolitik veranstalteten, zeigen diese Entwicklung: Zum ersten Umwelt-Weltgipfel reisten 1972 einige hundert private Akteure zum Austragungsort Stockholm, um - offiziell als Beobachter angemeldet - die Beschlüsse zu beeinflussen. Zwanzig Jahre später waren in Rio mehr als fünfmal so viele Gruppen anwesend. Während die privaten Akteure in Stockholm häufig als stumme Beobachter mit an den Verhandlungstischen saßen, nutzen sie spätestens seit Rio die Möglichkeit, schriftliche wie mündliche Stellungnahmen abzugeben, also direkt in die vormals zwischenstaatlichen Verhandlungen einzugreifen. Zusätzlich nehmen private Akteure auch noch indirekt Einfluss auf internationale Verhandlungen, indem sie etwa Kampagnen durchführen oder Gegengipfel abhalten. Auch diese Einflussnahme hat generell zugenommen. Den privaten Akteuren ist es durch die direkten wie indirekten Strategien der Einflussnahmen gelungen, einige ihrer Anliegen in den politischen Schlussdokumenten zu verankern. So ist es u. a. NGOs zu verdanken, dass Verweise auf Bevölkerungswachstum und Familienplanung aus der *Agenda 21*, dem umfangreichen Aktionsprogramm zur Nachhaltigen Entwicklung, gestrichen wurden. Industrielle Interessengruppen konnten gar ein eigenes Kapitel in der Agenda 21 verankern, in dem sie als wichtige Akteure bei der Umsetzung des Aktionsprogramms bezeichnet werden.

Die letzte Weltkonferenz der Vereinten Nationen, bei der u. a. Umweltfragen auf der Agenda standen, wertete private Akteure weiter auf. In Johannesburg wurden 2002 erstmals *Public-Private-Partnerships* - u. a. auf Drängen der USA – als offizielles Konferenzergebnis anerkannt. Bis dato wurden nur Vereinbarungen zwischen Staaten als Ergebnis anerkannt, da diese ja eigentlich die Teilnehmer der Verhandlungen darstellten. Die mehr als 200 vereinbarten PPP sind sehr unterschiedlich groß. Welchen Beitrag sie zur Verankerung der nachhaltigen Entwicklung leisten, bleibt abzuwarten.

Das wohl bekannteste Beispiel einer *Public-Private-Partnership* in der internationalen Entwicklungs- und Umweltpolitik stellt die *Weltstaudammkommission* dar. In der Kommission erarbeiteten Vertreterinnen und Vertreter des privatwirtschaftlichen, des zivilgesellschaftlichen und des staatlichen Sektors gemeinsam Richtlinien für den Bau von großen Staudämmen. Die Weltbank und die *Naturschutzorganisation World Conservation Union (IUCN)* initiierten den Regulierungsprozess. Sie reagierten damit auf die seit Mitte der 1970er Jahren anhaltende Kritik am Bau großer Staudämme. Menschenrechts- und Umweltgruppen sowie die vom Staudammbau betroffenen Bevölkerungsgruppen hatten immer wieder auf die sozialen wie ökologischen Folgen von Staudämmen hingewiesen, beispielsweise das Umsiedeln von Tausenden von Menschen oder die Überschwemmung großer Gebiete. Die Weltstaudammkommission sollte die bestehenden Erfahrungen mit Staudämmen systematisch auswerten, um so gemeinsam Normen für zukünftiges Handeln zu entwickeln. Die aus den drei Sektoren zusammengesetzte Weltstaudammkommission legte im November 2000 ihren Bericht vor. Sie kommt darin zum Schluss, dass die Mehrzahl der bisher gebauten Großstaudämme negative soziale und ökologische Folgen mit sich gebracht und ihre Ergebnisse in keinem Verhältnis

Tanja Brühl

Prof. Dr. Tanja Brühl ist Juniorprofessorin für Friedens- und Konfliktforschung an der Johann Wolfgang Goethe-Universität in Frankfurt am Main. Ihre Forschungsschwerpunkte sind: Vereinte Nationen, Weltordnungspolitik und internationale Umweltpolitik.

zu den Erwartungen gestanden hätten. Für den Bau weiterer Staudämme legte die Kommission Prioritäten und Richtlinien fest, die insbesondere die Interessen der von den Staudämmen betroffenen Menschen schützen sollen. Diesen liegen zentrale Werte zugrunde, wie Gerechtigkeit, partizipatorische Entscheidungsfindung und Nachhaltigkeit. Allerdings hapert es mit der Durchsetzung.

Private Normen

Rein private Regulierungsansätze, in die Staaten oder internationale Organisationen gar nicht eingebunden sind, gibt es erst seit einigen Jahren. Ihre Zahl nimmt freilich enorm zu. Die privaten Regulierungen umfassen erstens firmeneigene Verhaltenskodizes (*Codes of Conduct*), mit denen sich Unternehmen dazu verpflichten, bestimmte soziale und ökologische Mindeststandards in ihrem Betrieb einzuhalten. Zweitens gibt es sektorale Verhaltensstandards, die unter Beteiligung von Gewerkschaften oder NGOs ausgearbeitet wurden. Ein Beispiel hierfür ist die Zertifizierung von Holzproduzenten durch den *Forest Stewartship Council (FSC)*. Umweltorganisationen, Gewerkschaften, Waldbesitzer und die holzverarbeitenden Industrie einigten sich 1993 auf Prinzipien und Kriterien, die beim nachhaltigen Holzabbau einzuhalten sind. Unternehmen, die diese Kriterien einhalten, verleiht der FSC ein Siegel, das von diesen beim Verkauf des Holzes werbewirksam eingesetzt werden kann. Diese private Regulierung kam u. a. deshalb zustande, weil sich die Staaten nicht auf eine gemeinsame Waldpolitik einigen konnten, sie ist freiwillig. Ein Nachteil ist, dass inzwischen nicht zertifizierte Unternehmen dem FSC-Siegel ähnliche Markenzeichen nutzen.

Welchen Beitrag diese Regelungen für die Umwelt leisten, ist umstritten. Auf der einen Seite heben Befürworterinnen und Befürworter der neuen Regelungen, darunter viele Unternehmen, die Flexibilität der neuen Regulierungsformen hervor. Da starre Rahmenbedingungen fehlen, könnten die privaten Akteure der jeweiligen Situation angemessen Normen und Regeln umsetzen und dabei aus Fehlern lernen. Kritikerinnen und Kritiker betonen dagegen, dass viele privat-öffentliche wie auch private Regulierungen sehr allgemein gehalten seien, so dass sie gar keine konkreten Verhaltensregeln enthielten und eher Werbezwecken dienten. Häufig stellten sie nur eine Doppelung von sowieso bestehenden (völker-) rechtlichen Vereinbarungen dar, teils würden diese in privaten Regelungen sogar abgeschwächt. Zudem fehlten unabhängige Mechanismen, um das Verhalten der Akteure überwachen und ggf. eine Verhaltensänderung bewirken zu können.

Schätzt man die Legitimität der Regelungen ein, so kommt man wiederum zu einem uneinheitlichen Bild: So kann man argumentieren, dass eine zunehmende und direkter werdende Beteiligung von privaten Akteuren an Norm- und Regelsetzungsprozessen deren Legitimität erhöht. Schließlich sind dann die von den Regelungen Betroffenen zugleich Regelsetzer bzw. zumindest direkt in die Verfahren einbezogen, so dass die Legitimationsketten kürzer werden. Dies lässt aber außer Acht, dass nicht alle privaten Akteure über dieselben Möglichkeiten der Einflussnahme und Beteiligung an Aushandlungsprozessen verfügen. Zivilgesellschaftliche Organisationen aus Entwicklungsländern haben generell weniger Partizipationsmöglichkeiten als transnationale Unternehmen, die in der OECD-Welt angesiedelt sind. Die unterschiedlichen Beteiligungsmöglichkeiten zeigen sich auch daran, dass zivilgesellschaftliche Akteure in PPP häufig in der Minderheit oder überhaupt nicht vertreten sind. Außerdem verfügen sie über weniger Ressourcen als die Unternehmen. Unternehmen sind der Gesellschaft keine direkte Rechenschaft schuldig, was ihre demokratische Legitimität in Frage stellt. Es lässt sich zwar argumentieren, dass die Konsumentinnen und Konsumenten das Verhalten der Unternehmen ggf. durch Konsumboykotte steuern könnten, Verbrauchereinfluss ist aber von mehreren Faktoren abhängig: Wie hoch ist der Anteil der Stoffe in den Endprodukten? Ist er sehr gering und in vielen verschiedenen Produkten versteckt, lässt sich kaum ein Boykott durchsetzen. Sind die Produkte Luxusartikel, auf die man leicht verzichten kann, oder unverzichtbarer Bestandteil des Alltags? Sind die Produzenten bekannt, und haben sie einen Ruf zu verlieren?

Die Privatisierung der Weltpolitik ist also eine zweischneidige Entwicklung. Zukünftig gilt es, ihre negativen Seiten einzudämmen und hierbei insbesondere die demokratische Basis wie auch die Umsetzung der bestehenden Regelungen sicherzustellen.

Literatur:

Brühl, Tanja; Debiel, Tobias; Hamm, Brigitte; Hummel, Hartwig; Martens, Jens (Hg.) 2001: Die Privatisierung der Weltpolitik. Entstaatlichung und Kommerzialisierung im Globalisierungsprozess, Bonn: Dietz Verlag.

Brühl, Tanja; Feldt, Heide; Hamm, Brigitte; Hummel, Hartwig; Martens, Jens (Hg.) 2004: Unternehmen in der Weltpolitik, Politiknetzwerke, Unternehmensregeln und die Zukunft des Multilateralismus, Bonn: Dietz Verlag.

Kerkow, Uwe; Martens, Jens; Schmitt, Tobias 2003: The Limits of Voluntarism. Corporate Self-Regulation, Multistakeholder Initiatives, and the Role of Civil Society, Bonn: WEED.

Ute Twisselmann

IT Architecture Landscapes in the Context of Multinational Processes

In an international corporation exist few business processes not supported by IT applications. The landscape of these IT applications has usually grown over time and resembles a complex 'zoo'.

Reasons for Changing IT Architecture Landscapes

The complexity and diversity in this IT landscape result in ineffective process flows, time consuming and error prone data transfers and non transparent decisions. This causes a lot of costs and obstructions for operating model changes and process optimization. Other factors increasing the pain are:

- Mergers and acquisitions
- Linking and unification of processes across country and business area lines
- Increased cross-area requirements (i.e. transfer from development to production)
- Outsourcing or offshoring of selected business areas

From IT Architecture To Business-Oriented Architecture

All these factors normally force the restructuring of the IT landscape into a business-oriented architecture – an IT architecture optimized to fulfill the services as prioritized by business needs. There are a lot of technical issues when designing and implementing such an architecture, which are not the topic here. Beyond these technical aspects the main issues are of political and organizational nature or have their roots in company culture. Examples where non technical issues are dominating are:

- Smooth transitions between business areas or IT applications require: Integration of various applications used by different business areas into one IT architecture via middleware solutions, and the introduction of data standards enabling the data exchange in such an integrated environment.
- Creation of corporation wide standards, decision rules or corporate wide business processes need common agreement and careful change management.
- Outsourcing or offshoring decisions require new prioritizations of IT areas and services.

Generally the basic functional requirements and high service level needs are already defined on business level when the IT projects start. A lot of detailed agreements are necessary during the analysis phase of the IT project:

- Details of workflow and role definitions (on IT application level)
- Detailed data contents
- User interfaces
- Business impacts of IT architecture

Examples for the business impacts of an IT architecture are:

* Will the selected architecture fit the needs in five years? Data volumes might increase. IT application might be rolled out into other areas of the world. Security aspects must be observed to keep the trust of customers and business partners.
* To find a solution optimally supporting the business needs requires a common understanding of weaknesses and strength of existing architectures. A business case for selected solutions must be provided.
* Laws on data protection and data security rules must be observed in the application and architecture design.

Ute Twisselmann

Dr. Ute Twisselmann arbeitet zur Zeit als Senior Consultant im Bereich *Strategy and Change for Product Development in Automotive Industries* bei IBM Global Business Services. Ihre Tätigkeit bei IBM begann sie 1989 in der Produktentwicklung in Böblingen, wo die Kooperation mit anderen IBM Entwicklungsabteilungen weltweit zum täglichen Geschäft gehört. Sie hat in vielen internationalen Projekten gearbeitet, auch, aber nicht nur im IT-Bereich.

Challenges to the Project Management

All this needs international and cross-area agreements and decisions. A project team working on a restructuring of an IT landscape must be able to identify the demand of agreements and decisions as well as the stakeholders. The interests and goals of the stakeholders need to be addressed. Decision requests are usually formulated to the project leader who normally is responsible for getting answers in time from the domain departments. Nevertheless the project manager of the IT project is responsible for structuring these requests and keeping track of them. Careful stakeholder analysis, risk management and continuous agreement with the stakeholders is needed on how to react on delays.

Cultural Challenges and Diplomacy

Some agreements needed to progress in the project as planned are difficult to get. Reasons might be insufficient agreement on prioritization from the various stakeholders, incomplete decision hierarchy in the project organization, intercultural differentials or legal issues.

Examples for items that might affect an IT project are:

* Labor law: In the United States it is less of a problem to track working results of an individual than in Germany where the 'Betriebsrat' has to be involved.

* Change resistance: Department 'A' uses data source 'x' and department 'B' uses data source 'y'. Both departments are not willing to change their policy for an integration of data pools.

* Different time zones: Working in different time zones needs exact planning of project team communication.

* Different expertise levels: Skill levels and daily experiences differ in the various cultures. East European employees might for instance need additional training in certain PC or application skills. For instance a few years ago the use of CAD systems was not so common in Russia than in Europe or USA.

* National standards: Double byte character support must be planned for Japan or China.

* Infrastructure: In some areas of the world the technical or organizational infrastructure might be instable. For instance electricity supply may fail occasionally. Such risks influence technology decisions and achievable service levels of IT services.

The Development to an Expert

These examples show that beside the application and mastery of appropriate methods (i.e. Service Oriented Architecture) skills outside the traditional IT or computer science education are needed. Examples of such skills are:

- Knowledge about the business domain of the customer
- Handling of different working cultures
- Ability to create a financial analysis
- Conflict resolution and other communication skills
- Project management experience

Only some abilities can be trained theoretically:

- Project management methods become more and more part of engineering studies.
- Financial analysis methods can be acquired by an additional MBA study
- Data protection and IP laws: At least the project leader must be sensitive to possible legal issues and contact the legal departments for clearance.
- Data security solutions are a core part of computer science education.

Other skills can be accomplished by experience only:

- Recognition of differences in the working culture of a customer and appropriate reactions can only be learned by working at different customer locations and experiencing different working cultures.
- Conflict resolution can partially be trained but also needs a lot of practice.
- Basic knowledge about the business domain of the customer can be learned theoretically – but the specific situation of the customer can only be observed and handled in the direct project situation. This often requires high flexibility and analytic skills. Normally this requires consistent project assignment in one customer area or to be a member of a company's IT department.
- Leadership experience needs strong personal development in practice.

The main responsibility for gaining the optimal expertise lies at each computer scientist. He or she must address individual needs in expertise. On the other hand companies not offering a good mixture of theoretical education possibilities and mentoring practical experience will have problems getting the optimal mix of skills needed to complete projects successfully. These needs might become strategic issues in the near future when young skilled professionals become rare because of demographic development and increased complexity in expertise requirements.

Lesen -
Neues für den Bücherwurm

Stefan Hügel

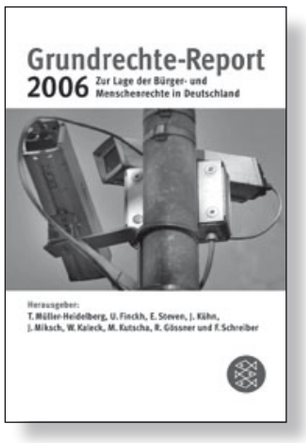
Grundrechte-Report 2006

Zur Lage der Bürger- und Menschenrechte in Deutschland

Der Mensch, der bereit ist, seine Freiheit aufzugeben, um Sicherheit zu gewinnen, wird beides verlieren.
Benjamin Franklin

„Mehr Freiheit wagen" – das ist die Absicht unserer Bundesregierung, wie Bundeskanzlerin Merkel zu Beginn ihrer Amtszeit erklärte.

Zum zehnten Mal bereits ist nun der Grundrechte-Report erschienen, der von Vertreterinnen und Vertretern verschiedener Organisationen herausgegeben wird, die sich die Verteidigung freiheitlicher Bürgerrechte zum Ziel gesetzt haben. Als alternativer Verfassungsschutzbericht konzipiert lässt er ahnen, dass Regierungen und Behörden in Deutschland mehr Freiheit wohl tatsächlich als Wagnis empfinden.



Die Schwerpunkte der letzten zehn Jahre haben sich dabei im Wesentlichen nicht verändert: „... es geht unverändert um Besorgnis erregende Entwicklungen und Übergriffe von Polizei und Nachrichtendiensten, um Verletzungen des Demonstrations- und Versammlungsrechts, um die überhand nehmende Überwachung und damit Verletzung des Grundrechts auf informationelle Selbstbestimmung, um Einschränkungen der Meinungs- und Pressefreiheit, um Asyl-, Ausländer- und Flüchtlingsrecht, um die Trennung von Staat und Kirche, um die vom Grundgesetz geforderte Friedensstaatlichkeit der Bundesrepublik Deutschland und um die Auswirkungen europäischer Politik und Maßnahmen auf die Bürger- und Menschenrechte." *(Seite 14)* Nur §20 GG beansprucht größeren Raum – die darin geforderte Sozialstaatlichkeit wird zunehmend ausgehöhlt.

Die Herausgeberinnen und Herausgeber gehen von der Grundthese aus, „... dass ernsthafte Gefahren für unseren freiheitlichen, demokratischen Rechtsstaat mit seinen Bürger- und Menschenrechten weniger ausgehen von so genannten Verfassungsfeinden und verfassungsfeindlichen Bestrebungen, sondern in erster Linie vom Staat und seinen Institutionen, und daher der Schutz der Verfassung nicht etwa in den Händen der Verfassungsschutzbehörden liegt, sondern Aufgabe der Bürgerinnen und Bürger ist *(Seite 14)*."

Diesem Ziel verpflichtet haben die Autoren – orientiert an den Grundrechtsartikeln unserer Verfassung – eine Reihe von Beispielen zusammengestellt.

Die meisten der behandelten Themen gingen im letzten Jahr durch die Presse – der Fall *Khaled el Masri* findet sich beispielsweise gleich zu Beginn. Auch die Einbürgerungspraxis in Baden-Württemberg (mit ihrem diskriminierenden Gesprächsleitfaden), die Gewissensfreiheit von Bundeswehrsoldaten (der Fall *Florian Pfaff*, vgl. FIfF-Kommunikation 3/2005) und die Aufhebung von Freiheitsrechten im Rhein-Main-Gebiet anlässlich des Besuchs von US-Präsident Bush werden behandelt.

Die Gesetzgebung der deutschen Parlamente ist ebenfalls Thema – wurden doch in der jüngsten Vergangenheit einige Gesetze vom Bundesverfassungsgericht für verfassungswidrig erklärt. Beispiel dafür ist der „große Lauschangriff".

Mittendrin findet sich auch ein positiver Beitrag: 2005 wurde ein Informationsfreiheitsgesetz auf Bundesebene beschlossen. Wenn man sich hier auch mehr wünschen würde, ist es doch ein Schritt in die richtige Richtung.

Vor dem Band sei zunächst gewarnt: Er erzeugt keine gute Stimmung. Das Buch ist auch nicht unparteiisch – das soll es auch gar nicht sein. Es lässt viele derjenigen Ereignisse nochmals Revue passieren, die hinsichtlich der weiteren Entwicklung unseres Rechtsstaats zu Besorgnis Anlass bieten. Es sind möglicherweise auch solche dabei, die man im Trubel der Medienberichterstattung überhaupt nicht oder nur am Rande wahrgenommen hat.

Wichtig ist das Buch besonders in einer Zeit, in der – folgt man der veröffentlichten Meinung – die Akzeptanz staatlicher Freiheitseinschränkungen im Namen der Sicherheit stetig steigt. Hierin liegt eine große Gefahr – das Buch weist deutlich auf die Konsequenzen hin.

Denen, die sich solcher Gefahren bewusst sind, zur Bestätigung, den anderen zur Überprüfung ihrer Sichtweise, ist die Lektüre des Bandes unbedingt zu empfehlen.

Till Müller-Heidelberg, Ulrich Finckh, Elke Steven, Julia Kühn, Jürgen Micksch, Wolfgang Kaleck, Martin Kutscha, Rolf Gössner, Frank Schreiber (Hg.): Grundrechte-Report 2006. Zur Lage der Bürger- und Menschenrechte in Deutschland. Frankfurt am Main: Fischer Taschenbuch-Verlag, 2006. ISBN 3-596-17177-6

Sebastian Jekutsch

Whistleblowing

Whistleblowing ist zum Beispiel Folgendes: Ein Metzgergeselle verliert Material in einem Wald, das den Arbeitgeber belastet. Ein Pilzsammler findet die Dokumente und übergibt sie der Polizei. Die Polizei ermittelt und deckt dabei einen umfangreichen Betrugsfall auf. So geschehen beim *Gammelfleisch*-Skandal im September in Bayern. Whistleblowing ist aber auch dieses: Dem Metzgergesellen wird fristlos gekündigt, seine ehemaligen Kollegen bedrohen ihn, Gerüchte kommen auf über eine unerfüllte Liebe zur Tochter des Geschäftsführers. Nur der Staatsanwalt lobt ihn, und unausgesprochen dankt ihm vermutlich ein großer Teil der Bevölkerung.

So warnt auch Rohde-Liebenau in seiner Broschüre „Whistleblowing" über die ungeahnten Folgen eines falsch geplanten Heldentums oder übersteigerten Berufsethos und mahnt besonnenes Vorgehen an. Hinweisgeber – so die offizielle Übersetzung des auch in der FIfF-Kommunikation schon etablierten Begriffs *Whistleblowing* – sollten alle Möglichkeiten einer internen Diskussion ausnutzen, bevor gibt es keinerlei rechtliche Unterstützung für externes Whistleblowing, im Gegenteil: man macht sich schuldig im Sinne des Betriebsgeheimnisses. Zu einer Kultur des Ja-Sagens und Wegsehens sollte dies aber keineswegs führen. Und wenn sich Arbeitnehmer gar selbst strafbar machen würden oder die Arbeitsbedingungen unzumutbar sind, bleiben nicht viele Möglichkeiten.

Rohde-Liebenau setzt vor allem auf Betriebsvereinbarungen zur „internen Risikokommunikation", d.h. zu betrieblichen Vereinbarungen, die internes Hinweisgeben fördern, um den Gang nach draußen zu vermeiden. Dies sollte auch, ja vor allem im Sinne des Arbeitgebers sein. Die Mittel sind anonyme Briefkästen, Abweichungsmöglichkeiten vom Dienstweg, Rückmeldungspflicht und Schutz vor Benachteiligungen. Die vorliegende Broschüre – dies wird auch aus dem Klappentext und der Herausgeberin Hans-Böckler-Stiftung deutlich – wendet sich vor allem an den Betriebsrat und hilft ihm in erster Linie bei der Erstellung solcher Vereinbarungen (ein Mustertext ist dabei). Sie hilft aber auch bei der Durchführung von Beratungsgesprächen mit Kolleginnen und Kollegen, die sich dem Betriebsrat anvertrauen, und enthält direkte wertvolle Hinweise für die unsicheren und zweifelnden Arbeitnehmer, z. B. eine halb-reale Fallgeschichte und eine Checkliste. Sogar ein Kapitel für das Management ist vorhanden, um es von einem offenen Risikomanagement zu überzeugen. Auf Besonderheiten z. B. der IT-Branche geht die Broschüre leider nicht ein.

So ist die Broschüre vor allem interessant für die Beschäftigtenvertreter, weniger für den Gesellen mit Gewissensbissen. Aber auch dieser wird für einige der Hinweise dankbar sein.

Björn Rohde-Liebenau: Whistleblowing – Beitrag der Mitarbeiter zur Risikokommunikation, edition der Hans Böckler Stiftung 159, Düsseldorf 2005, 82 Seiten, ISBN 3-86593-036-0, 10 Euro

Dagmar Boedicker

Human Rights in the Global Information Society

Ein sehr interessantes Buch für alle, die Interesse an den Menschenrechten und ihrer – tatsächlichen oder ausbleibenden – Umsetzung in der Informationsgesellschaft haben! Die Autorinnen und Autoren aus Nichtregierungs-Organisationen auf drei Kontinenten behandeln alle wesentlichen Themen, die die vernetzte und global kommunizierende Weltgemeinschaft beschäftigen: Es geht um Informations- und Meinungsfreiheit, Vereinigungsfreiheit und Partizipation und um Gleichberechtigung und Entwicklung. Zeitlicher Ausgangspunkt ist der letzte Weltgipfel über die Informationsgesellschaft *(World Summit on the Information Society - WSIS),* den die Autoren konsequent mit der *Allgemeinen Erklärung der Menschenrechte* der Vereinten Nationen (VN) und den Entwicklungszielen der VN *(Millenium Development Goals - MDG)* zusammen denken, beschreiben und weiter entwickeln.

Die enge und gleichrangige Verbindung von Menschenrechten, Demokratie und Entwicklung wäre Voraussetzung für eine friedliche Welt. In den Beiträgen wird sie unter anderem den Herausforderungen gegenüber gestellt, die sich aus diversen Bedrohungsszenarien ergeben und scheinbar danach rufen, Menschenrechte einzuschränken, um Sicherheitsbedürfnisse, wirtschaftliche Entwicklung und allgemein Ruhe zu befördern. Der technische Fortschritt der Kontroll- und Überwachungstechnik seit September 2001 hat das Potenzial, Meinungs-, Informations- und Versammlungsfreiheit ernsthaft zu beschädigen. Die Verbreitung und Konvergenz von IKT (Informations- und Kommunikationstechnik) kann Frieden oder Unfrieden verbreiten, sie kann aufklärerisch und demokratisch oder als Verblendung und zur Volksverhetzung wirken. Und natürlich ist die digitale Kluft auch weiterhin ein Problem, von dessen Lösung wir weit entfernt sind.

Wer sich vorbereitend mit den Menschenrechten beschäftigen möchte (neulich ergab eine Studie haarsträubende Defizite bei diesem Thema in Deutschland): *www.ohchr.org/english/about/hc/iondex.htm*. Es könnte Sie überraschen, wie viele es gibt, denn die VN-Generalversammlung hat sie mit ihren Erklärungen 1984 (Recht der Völker auf Frieden) und 1986 (Recht auf Entwicklung) präzisiert. Ihre Interpretation und Anwendung sind keineswegs unumstritten. Das Buch befasst sich im ersten Abschnitt mit der Meinungsfreiheit, Informationsfreiheit und dem Schutz der Privatsphäre. Autoren sind Rikke Frank Joergensen zum *Recht, seine Meinung zu äußern und sich zu informieren,* Daid Banisar zum *Recht sich im Informationszeitalter zu informieren,* Kay Raseroka zum *Zugang zu Information und Wissen,* Robin Gross zum *geistigen Eigentumsrecht und der Informations-Allmende,* Gus Hosein zu *Privatheit als Freiheit.*

Im zweiten Teil (Vereinigungsfreiheit, Partizipation und rechtsstaatliche Verfahren) schreiben Charley Lewis über das *Recht auf Versammlung und Organisation im Informationszeitalter,* Hans Klein über das *Recht auf politische Partizipation in der Informationsgesellschaft* und Meryem Marzouki über *Rechtsgarantien zur Durchsetzung des Rechtsstaats.*

Im dritten Teil (Gleichberechtigung und Entwicklung) behandeln Mandana Zerrehparvar die *nicht diskriminierende Informationsgesellschaft,* Heike Jensen (sie schrieb über den WSIS in der FIfF-Kommunikation 2/2006) die *Frauenrechte in der Informationsgesellschaft,* Birgitte Kofod Olsen die *Sicherung von Minderheiten-Rechten in einer pluralistischen und „fließenden" Informationsgesellschaft* sowie Ran Greenstein und Anriette Esterhuysen das *Recht auf Entwicklung in der Informationsgesellschaft.*

Als kleinen Auszug aus den durchweg spannenden Beiträgen ein paar Bemerkungen zum Beitrag von Hans Klein (ehemaliger CPSR-Vorsitzender) zur Partizipation: Klein bindet das Partizipationsrecht an die Voraussetzungen einer Staatsbürgerschaft und einer Regierung, womit er einigen ehemaligen oder heutigen Bewohnern des Cyberspace vielleicht die Illusionen raubt. Denn Partizipation kann kein Menschenrecht an sich sein, sie setzt organisierte und etablierte Herrschaft voraus, nur mit dieser lässt es sich um Beteiligung streiten, wie immer diese dann aussehen mag. Klein bezieht sich auch auf Lessig und dessen Hinweis darauf, dass die Politik für eine Informationsgesellschaft nicht von den Politikern gemacht wird, sondern von den Software-Entwicklungsprozessen – in der Gestaltung der Technik. Ein Code kann Verhalten möglich oder unmöglich machen, und er ist damit den Gesetzen vergleichbar, die manches Verhalten erlauben, anderes nicht. Das Problem der Technikgestaltung liegt darin, dass es keine Verfahren, ob traditionell oder neu, gibt, die eine Mitbestimmung regeln. Entscheidungen mit breiter wirtschaftlicher, politischer und sozialer Wirkung werden in geschlossen Normungs-Gremien oder den Chef-Etagen großer Unternehmen gefällt, Zutritt für Bürger verboten. An den Beispielen der *Free and Open Source Software* Bewegung und von ICANN präsentiert Klein zwei Modelle für Partizipation in der Informationsgesellschaft, und in seinen abschließenden Bemerkungen stellt er die Frage, ob wir die Informationsgesellschaft als eine Gesellschaft mit üppigem Informationsangebot aber traditionellen Institutionen betrachten wollen, oder als eine davon abweichende, mit neuen Regeln für die Partizipation, die erst noch zu bestimmen und durchzusetzen wären.

Ran Greenstein und Anriette Esterhuysen kritisieren die verbreitete Auffassung, dass für Entwicklung vor allem die digitale Kluft zu überwinden sei. Schließlich ist sie in erster Linie ein Symptom für die tiefen strukturellen Gräben auf lokaler und globaler Ebene, die Entwicklung bisher be- oder verhindern, und es ist deshalb kaum zu erwarten, dass die Verbreitung einer *Wissensökonomie* zu einer gerechteren Verteilung von Macht und Reichtum führen wird. So sei beim WSIS die Machtfrage nicht gestellt worden, obwohl Machtverteilung und Ungleichheit die wesentlichen Faktoren und damit auch Hindernisse für Entwicklung sind. Armut und Machtlosigkeit würden zwar diskutiert, dafür verantwortliche Individuen, Institutionen, Prozesse oder soziale Verhältnisse aber nicht identifiziert, leider ein häufiges Phänomen bei Abkommen, die im Rahmen der VN von den Regierungen beschlossen werden. 2003 hat deshalb die *Civil Society Declaration* (Erklärung der Zivilgesellschaft) genau diese Aspekte aufgegriffen. Die Autoren des Beitrags bezeichnen es als entscheidende Herausforderung, die wesentlichen Entwicklungshindernisse (sozial, politisch, technisch) zu erkennen und mögliche Strategien zu skizzieren, mit denen sie sich in der Informationsgesellschaft überwinden ließen. Sie betrachten dazu das Recht auf Entwicklung systematisch und kommen zu teilweise überraschenden, nicht immer erfreulichen Beurteilungen. So ist schon die Betrachtung eines Rechts auf Entwicklung von Staaten äußerst problematisch, lenkt sie doch von den innerstaatlichen Verhältnissen ab. Auch die MDGs eröffnen problematische Interessenkonflikte, wenn sie eine verstärkte Zusammenarbeit mit dem Privatsektor und der Zivilgesellschaft fordern (siehe *Die Privatisierung der Weltpolitik*, T. Brühl in diesem Heft).

Gus Hosein beschreibt Privatheit als Freiheit, er bedauert gleich am Anfang seines Beitrags, dass der Schutz der Privatheit in der öffentlichen Diskussion einen geringeren Stellenwert hat als andere politische Themen wie Umweltschutz oder die Abtreibungsdebatte. Man sieht, hier schreibt jemand aus US-amerikanischer Sicht, Hosein kommt aber zu den gleichen Schlüssen wie unser Verfassungsgericht bei seinem Urteil über die informationelle Selbstbestimmung: Wo Privatheit bedroht ist, ist auch politische Freiheit bedroht. Drei Bewegungen beschreibt er (neben den Regierungen) als Feinde der informationellen Selbstbestimmung: Kommunitarier, klassische Feministinnen und den Markt. Die Begründungen sind spannend, und ich würde sie ungern vorwegnehmen. Selbstverständlich widerspricht Hosein der Argumentation, dass das Recht auf Privatheit hinter anderen, grundlegenderen Menschenrechten zurückzustehen habe. Er schildert überzeugend, wie Überwachung und Kontrolle durch das Zusammenwachsen der Kommunikationsmedien erleichtert werden, so dass auch schon die Überwachung nur der Verkehrsdaten ein Vielfaches an Information liefert. Er beschreibt, wie auch die Daten aus vielen Quellen, die bei nahezu allen Aktivitäten einer Person anfallen, darunter auch biometrische, zu diesem Ergebnis führen: „Wenn genügend anscheinend unbedeutende Daten in einer Analyse mit Milliarden von Daten verglichen werden, wird auch das Unsichtbare sichtbar." (Das ist ein Zitat aus dem Werbematerial für *MATRIX – Multistate Anti-TerRorism Information Exchange.)* Sein Fazit ist bedrückend, und seine Warnung vor gesellschaftlichen Weichenstellungen für die Technik deutlich: Sie könnten irreversibel sein.

Viele Themen, kritische Perspektiven, ein hervorragendes Buch! Angenehm ist auch der Index des Buchs, der es zu einem nützlichen Werk für die eigene Arbeit macht.

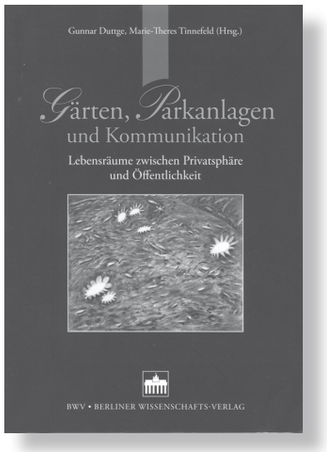
Rikke Frank Joergensen (Hrsg.): Human Rights in the Global Information Society. Massachusetts Institute of Technology 2006. ISBN 0-262-60067-6 (paperback), 16,95 britische Pfund, in englischer Sprache

Dagmar Boedicker

Gärten, Parkanlagen und Kommunikation

Lebensräume zwischen Privatsphäre und Öffentlichkeit

Der Folgeband zu *Privatheit, Gärten und politische Kultur* ist erschienen, wieder ein interessanter Blick auf die ungewöhnliche Beziehung zwischen dem, was uns politisch beschäftigt, und dem, was uns als erholsamer Rückzugsort oder gemeinschaftliches Erleben gut tut.



Privatheit gedeiht nur in der Freiheit – wie Marie-Theres Tinnefeld in ihrem Text *Der Garten Eden* schreibt – und umgekehrt. Sie warnt vor der Verletzung verfassungsrechtlich verbürgter Freiheitsrechte und einem Staat, in dem tendenziell alles und jeder beobachtet werden dürften, weil die Folge ein „allgegenwärtiges, ineffizientes Misstrauen und eine diffuse Angst" wären. Tinnefeld schlägt den Bogen zur Aufklärung und kritisiert „in politisch unsicheren Zeiten eine irrationale Sehnsucht nach Unmündigkeit, und zwar in bewusster Abhängigkeit von einem starken Staat". Ihr Text leitet den ersten Teil des Buchs *Der Garten als Maß für Menschenrechte?* ein. Abgeschlossen wird dieser erste Teil von einem Beitrag, der die Diskriminierung und Ausschließung von Juden während der NS-Zeit untersucht. Hubertus Fischer und Joachim Wolschke-Bulmahn stellen darin aber auch eine „autoritäre Fürsorglichkeit für die gehobenen Klassen" fest, „die zur Fernhaltung der mit den niederen Trieben assoziierten Gruppen führt." Wem würde dabei nicht die allgegenwärtige Videoüberwachung einfallen, mit der *unerwünschte Elemente* heute von öffentlichen Plätzen oder privatem Eigentum wie Einkaufspassagen ferngehalten werden. Die Nazis benutzten dazu Verbotstafeln in Parkanlagen und gelb gestrichene Bänke „nur für Juden". Mich hat dieser Beitrag wieder sehr beeindruckt, weil er deutlich zeigt, wie gern Verwaltungen bereit sind, menschliches Denken und Fühlen auszuschalten, und wie bereitwillig ein beachtlicher Teil der Bevölkerung dieses Verhalten mit trägt oder sogar verlangt.

Die Richterin am Verfassungsgericht Christine Hohmann-Dennhardt eröffnet den zweiten Teil *Öffentlichkeit und Privatheit im Spiegel der Rechtspolitik* mit ihrem Beitrag *Freiräume.* Sie macht deutlich, dass es ohne funktionierende Sozialpolitik keine Freiheit geben kann, „dass Freiheit, um sich entfalten zu können, auch einer materiellen Basis bedarf, dass deshalb ‚jeder Mensch Anspruch darauf hat ... in den Genuss der für seine Würde und die freie Entfaltung seiner Persönlichkeit unentbehrlichen wirtschaftlichen, sozialen und kulturellen Rechte zu gelangen' ..." (Art. 22 der Allgemeinen Erklärung der Menschenrechte). Hohmann-Dennhardt weist darauf hin, dass es längst nicht mehr nur darum geht, „einzelne Informationen über sich zurückhalten zu können, sondern davor bewahrt zu sein, gänzlich durchleuchtet und erfasst zu werden". Die altmodisch klingende Warnung vor dem gläsernen Menschen aus den Achtziger Jahren hat über 20 Jahre danach das Schicksal etlicher Warnungen vor Technikfolgen erlitten: Zunächst halten sie alle für übertrieben, und wenn die Folgen eintreten, haben sich alle schon daran gewöhnt. Um so eindringlicher klingt da der Appell der Richterin, dass es gilt, „gerade in der Informationsgesellschaft[,] der Privatheit ausreichende Breschen zu schlagen, ihr Platz und Freiraum zu erhalten ... Dazu aber bedarf es nicht nur der Rechtsgewährung, sondern auch unserer Wahrnehmung des Rechts auf Privatheit, der Sensibilität jedes Einzelnen zu erkennen, wo ihr Gefahr droht, und sie rechtzeitig zu verteidigen."

Es folgen ein dritter Teil *Brauchen Gärten und Parks neue Übersetzer?* und ein vierter *Welt- und Menschenbilder im Verständnis von Zeit und Raum.* Rainer Erlingers Beitrag *Der elektronische Garten* vergleicht unsere Möglichkeit, überall und jederzeit elektronisch zu kommunizieren, mit einem virtuellen elektronischen Garten. Wir sind nicht mehr an einen geschlossenen Ort gebunden, sondern können in der Öffentlichkeit unter Menschen sein, von denen wir uns dann abgrenzen, um mit anderen Menschen zu sprechen, eine SMS zu schicken oder Mails zu lesen – also ganz privat zu sein. Erlinger vergleicht das mit einer Szene im Faust, in Marthens Garten, in der Marthe sich mit Mephistopheles und Faust sich mit Gretchen unterhalten, obwohl sie in Marthens Garten zu Gast sind. Das geht im Garten, in einem geschlossen Raum wäre es unhöflich.

Auch in diesem Buch wird wieder das Verhältnis zwischen Öffentlichkeit und Privatheit thematisiert, es ist eine rechts- und kulturpolitische Betrachtung für Menschen, die gern auch von weit gespannten und ungewohnten Verbindungen zwischen den Themen lesen.

Gunnar Duttge, Marie-Theres Tinnefeld (Hrsg.): Gärten, Parkanlagen und Kommunikation, Berliner Wissenschafts-Verlag, Berlin 2006. ISBN 3-8305-1172-8, 39,00 Euro

Ingo Ruhmann

Mit einer Tagung „Informatik und Rüstung" am 29. und 30. September in Berlin wurde die im Einsteinjahr 2005 begonnene Auseinandersetzung von Wissenschaft und globaler Sicherheit auch im Informatikjahr 2006 fortgeführt. Der Trägerkreis „Einstein weiterdenken" - bestehend aus AFK (Arbeitsgemeinschaft für Friedens- und Konfliktforschung), DSF (Deutsche Stiftung Friedensforschung), FONAS (Forschungsverbund Naturwissenschaft, Abrüstung und internationale Sicherheit), Natwiss (NaturwissenschaftlerInnen Initiative Verantwortung für Frieden und Zukunftsfähigkeit) *und* VDW (Vereinigung Deutscher Wissenschaftler), *ergänzt um das* FIfF – *richtete mit Unterstützung des* Bundesministeriums für Bildung und Forschung (BMBF) *diese Tagung aus.*

Mit ca. 200 Teilnehmerinnen und Teilnehmern wurden die Erwartungen der Veranstalter klar übertroffen. „Eine vergleichbare Tagung gab es zuletzt vor 15 Jahren. Das Thema Informatik und Rüstung ist aus seinem Dornröschenschlaf aufgewacht und muss jetzt wieder ein Thema der Informatik und ihrer Fachgesellschaften sowie der gesamten Gesellschaft werden", so der Kongressverantwortliche Reiner Braun.

Besonders großes Interesse fand am Eröffnungsabend die Podiumsdiskussion zwischen den „Grands Seigneurs" der Informatik, Prof. Dr. Joseph Weizenbaum und Prof. Dr. Klaus Brunnstein. Weizenbaum warnte, dass die technische Entwicklung der Informatik rasant sei, das Navigationssystem aber nicht genutzt werde. Die heute zivil geprägte Informatik habe ihre wesentlichen Ursprünge im Militärischen. Nun führe der *dual-use* ziviler Entwicklungen, wie das World Wide Web zu neuen Problemen, so Prof. Brunnstein. Es gebe eine unsichere Infrastruktur, die den Cyberwar begünstige. Niemand wolle solche Konflikte, aber „wir müssen heute fragen, wie wir durch bessere Sicherheit einen Cyberwar auf diesen Netzen verhindern können", so Brunnstein.

Joseph Weizenbaum sah die InformatikerInnen in der Verantwortung: „Wir haben kein Recht, Politikern vorzuwerfen, uns in den Krieg zu führen. Wenn wir Informatiker nicht mitmachen, wären Kriege heute unmöglich oder würden ganz anders aussehen." Beide forderten die Informatiker auf, die zunehmende „Gleichgültigkeit" – so Weizenbaum – abzulegen. „Vielen ist es heute schon egal, welche Datenspuren sie hinterlassen und wie die Privatsphäre ausgehöhlt wird", so Brunnstein.

Melissa Ngo, Direktorin der amerikanischen Bürgerrechtsorganisation *Electronic Privacy Information Center (EPIC),* erläuterte anschließend die Folgen von schwächeren Gesetzen und geringerem Interesse an solchen Fragen. Dort verkaufen Datenverarbeitungsfirmen die Daten ihrer Kunden an Betrüger, die mit der elektronischen Identität unbescholtener Bürger Straftaten begehen. Ngo erläuterte ihren Beitrag mit Beispielen zur Videoüberwachung und RFID-Funkchips aus den USA und Deutschland. Die Videoüberwachung ist in Großbritannien und den USA weit verbreitet. Straftaten verhindern kann sie jedoch nicht. Ngo führte mehrere Beispiele an, in denen spezielle, für spezifische Fälle installierte Videoüberwachung auch bei der Ermittlung und Aufklärung erfolglos blieb. Videoüberwachung ist so teuer und so wenig effektiv, dass es sinnvoller wäre, wenn Städte ihre Systeme abbauen würden, um mit den frei werdenden Mitteln Polizisten zu bezahlen. Genau dies tun inzwischen einige Städte in den USA.

Auch Deutschland ist nicht frei von Problemen. Wenn die Wohnung der Bundeskanzlerin Merkel durch eine Videokamera auf einem Museum gegenüber überwacht wird, wie viel Schutz haben dann normale Bürger, fragte Ngo.

Der Samstag begann mit Einleitungsvorträgen für die sechs Arbeitsgruppen. Götz Neuneck gab als erstes einen Überblick über die technologische Entwicklung allgemein und in der Informatik insbesondere und stellte dazu Überlegungen zu den Folgen für die Rüstungsdynamik an.

Neben neuen Techniken, wie der RFID-Technik, dürfe nicht vergessen werden, dass die umfangreichen bestehenden Datensammlungen des Staates und von Unternehmen, wie zum Beispiel im Bereich Telekommunikation, sehr viel interessanter für Sicherheitsbehörden seien, so der stellvertretende Datenschutzbeauftragte des Landes Schleswig-Holstein, Dr. Johann Bizer. Militär in Auslandseinsätzen werde immer mehr mit Polizeiaufgaben betraut – das schließe die Sammlung von Daten über die Bürger ausdrücklich ein. Wer nun über die Bundeswehr im Inland rede, werde daher auch darüber Rechenschaft ablegen müssen, welche Rolle die Bundeswehr beim Zugriff auf zivile Daten erhalten solle.

Der Medienwissenschafter Friedrich Kittler sieht im Computer die Eskalation der Eskalation: die durch Moores Gesetz beschriebene Dynamik der Informatikentwicklung führt nach der Integration des Computers in Rüstungssysteme dazu, dass diese Dynamik nun auch durchschlage auf die Rüstung.

Der Major der Bundeswehr Florian Pfaff beschrieb die diversen vorsätzlichen „Fehler" in der Berichterstattung über die Kriege im Kosovo und nun in Afghanistan, die ihn veranlasst und bestärkt haben, sich den Befehlen zur Entwicklung von technischen Komponenten für den Kosovo-Einsatz zu widersetzen – und damit vor Gericht zu obsiegen. Pfaff sieht die Pflicht jedes Einzelnen, sich zu informieren und zu seiner Verantwortung zu stehen.

In dieselbe Richtung argumentierte FIfF-Vorstand Prof. Hans-Jörg Kreowski, der sein Ziel in der Lehre damit beschrieb, dass er zwar bei Studierenden die Begeisterung für die Informatik wecken wolle, aber dies nicht mit Lügen erzielen wolle.

Das frühere FIfF-Vorstandsmitglied Prof. Friedrich Holl fragte danach, wie es funktionieren könne, Sicherheit durch IT-Einsatz und damit auf der Grundlage von unsicheren Systemen leisten zu wollen. Lösung bieten nicht die technischen Systeme, man müsse dafür hinter die technischen Systeme treten, so Holl.

Die anschließenden Arbeitsgruppen boten durch die Zusammenstellung der Referenten einige ungewohnte Perspektiven. Prof. Kittler, der eine AG mit dem BND-Experten Erich Schmidt-Eenboom gemeinsam bestritt, stellte die Frage, in wie weit asymmetrische Konflikte wie jüngst der Feldzug Israels gegen die Hisbollah nicht eine Abkehr vom technologischen Krieg erkennbar werden lasse. Israel habe modernste Überwachungstechnologien zur Verfügung, aber seit einigen Jahren keine Agenten mehr vor Ort, die Hisbollah greife dagegen auf ein Netzwerk von Informanten zurück, die ohne technologische Hilfsmittel Nachrichten weitergegeben würden. Kittler ergänzte dies mit der Nachrichtenübermittlung in den Konflikten in Afghanistan und im Irak, bei denen die Kämpfer gegen die USA archaische Informationsmittel nutzen, die von den hoch technisierten Amerikanern kaum geortet werden können. Kittler warnte hier aber vor voreiligen Schlüssen. Weder ließe sich sagen, dass der Erfolg dieser Bewegungen darin liege, dass sie mit ihrer altmodischen Kriegsführung von der modernen Technologie gar nicht wahrgenommen werden, noch sei klar, ob das Bild von den mit archaischen Methoden operierenden Gotteskriegern überhaupt stimme. So betrieb die Hisbollah ihren Fernsehsender Al-Manar trotz mehrfacher Bombardierung weiter, konnte den Funkverkehr israelischer Militärs abhören und war mit modernsten Panzerabwehrwaffen ausgerüstet.

Thema des Abschlusspodiums war der Abbau der Bürgerrechte im Zeichen des Sicherheitsdiskurses und die Möglichkeiten, als InformatikerIn zu handeln. Melissa Ngo erläuterte noch einmal die Einschränkungen der Bürgerrechte in den USA nach dem 11.September und machte darauf aufmerksam, in welchem Maße vor allem bei der jungen Generation das Bewusstsein für Privatsphäre an Bedeutung verloren habe. Ähnlich pessimistisch äußerte sich der Mitbegründer des Chaos Computer Clubs, Frank Rieger. Er hält den Kampf um die Bürgerrechte weitgehend für verloren und plädierte für Selbstschutz in Form von Verschlüsselung und anderen Gegenmaßnahmen. Wie solche Gegenmaßnahmen aussehen können, demonstrierte Rena Tangens, eine der Organisatorinnen der BigBrother Awards. Rena Tanges «Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs» hat zahlreiche Projekte gegen Videoüberwachung und für die Kontrolle von RFID-Chips durchgeführt, die zeigen, wie man sich und andere informieren kann und konkret gegen den missbräuchlichen Einsatz von IT vorgehen kann.

Stefan Hügel

FIfF International

Europa wächst zusammen. Immer mehr Entscheidungen und Aktivitäten – politisch, gesellschaftlich, wissenschaftlich – finden heute auf internationaler, mindestens europäischer Ebene statt. Nationale Gesetze setzen oftmals nur noch Richtlinien um, die zuvor in Brüssel beschlossen wurden. Gerade die Informationsgesellschaft, mit dem Internet als technischer Basis, kann nicht auf die nationale Ebene beschränkt bleiben.

In merkwürdigem Gegensatz dazu steht die Tatsache, dass viele öffentliche Debatten – auch und gerade in den Medien – immer noch national stattfinden und die Auswirkungen vorwiegend aus nationaler Perspektive betrachten.

Es gibt aber mittlerweile eine Reihe von Initiativen, die diese nationale Beschränkung überwinden wollen. Bereits 1991 fand die Jahrestagung des FIfF im Rahmen des internationalen Kongresses „Challenges – Science and Peace in a Rapidly Changing Environment“ statt.

Aktuell ist das FIfF insbesondere an zwei dieser internationalen Initiativen beteiligt:

- Das FIfF ist seit zwei Jahren Mitglied von *European Digital Rights (EDRi)*. Hier haben sich inzwischen 25 zivilgesellschaftliche Organisationen aus Europa zusammengeschlossen, die sich hauptsächlich mit Informationsrecht und den Folgen der IKT für die Persönlichkeitsrechte der Bürger befassen.
- Anfang November findet – in der Folge des *Weltgipfels der Informationsgesellschaft (WSIS)* – das *Internet Governance Forum* in Athen statt. Im Rahmen der *ICANN (Internet Corporation for Assigned Names and Numbers)* bilden sich gerade regionale Organisationen, aus denen heraus eine Beteiligung der Zivilgesellschaft an Fragen des Internet Governance geleistet werden soll.

EDRi – European Digital Rights

Zahlreiche Gesetzesinitiativen im Umfeld der Informationstechnik haben ihren Ursprung in den Institutionen der Europäischen Union. Prominentes Beispiel ist die EU-Richtlinie zur Vorratsdatenspeicherung, die eine Speicherung von Verbindungsdaten aus elektronischer Kommunikation für mindestens sechs Monate vorsieht und im Dezember 2005 verabschiedet wurde.

Weitere Themen sind die weiter zunehmende Videoüberwachung, biometrische Pässe und weitere Maßnahmen, die im Rahmen des „Kriegs gegen den Terror“ eingeführt wurden und

werden und teilweise erhebliche Auswirkungen auf die Meinungsfreiheit und andere Bürgerrechte haben.

Um solche Themen europaweit bearbeiten zu können, wurde 2002 EDRi gegründet. EDRi ist ein Verein nach belgischen Recht mit Sitz in Brüssel; seine bisher 25 Mitgliedsorganisationen stammen aus 16 europäischen Ländern.

Am 2. und 3. September 2006 fand in Berlin die diesjährige Generalversammlung statt, in die jede Mitgliedsorganisation Vertreterinnen und Vertreter entsendet. Im Rahmen dieser Versammlung wurden zum einen vereinsrechtliche Themen behandelt – insbesondere Vorstandswahlen und die Aufnahme neuer Mitglieder – und zum anderen inhaltlich-strategische Fragen diskutiert.

Der neue Vorstand besteht aus drei Mitgliedern:

- Meryem Marzouki, *Imagions un Réseau Internet Solidaire,* Frankreich (Vorsitzende)
- Rikke Frank Joergensen, *Digital Rights,* Dänemark (stellvertetende Vorsitzende)
- Andreas Krisch, VIBE!AT – *Verein für Internet-Benutzer Österreichs* (Finanzreferent)

Es wurden vier neue Mitglieder aus Großbritannien, Irland, Italien und Spanien aufgenommen.

Inhaltliche Aktivitäten waren und sind:

- die Kampagne gegen die EU-Richtlinie zur Vorratsdatenspeicherung,
- Beteiligung an Konferenzen, beispielsweise zu den Themen Biometrie, Vorratsdatenspeicherung und Umgang mit illegalen Inhalten im Internet,
- Beteiligung am Weltgipfel der Informationsgesellschaft (2003 in Genf und 2005 in Tunis) und am Internet Governance Forum (November 2006 in Athen).

Im EDRi-gram berichtet EDRi alle zwei Wochen auf seiner Web-Seite (siehe unten) über aktuelle Entwicklungen und Ereignisse im Umfeld digitaler Rechte.

Der zweite Tag der Generalversammlung bestand aus Berichten der einzelnen Organisationen und der Diskussion weiterer Inhalte der EDRi-Arbeit. Die meisten der Mitgliedsorganisationen sind an den (jeweils national organisierten) Big-Brother-Awards beteiligt, bei denen jährlich besondere *Verdienste* beim Abbau von Bürgerrechten prämiert werden. Weitere Themen – auch für die weitere Arbeit des EDRi – sind Fragen der Privatheit (RFID, Anti-Terror-Gesetze, Ausgestaltung der Vorratsdatenspeicherung), Rede- und Meinungsfreiheit (z.B. Filterung von Inhalten im Internet) und Intellektuelle Eigentumsrechte (z.B. Digital Rights Management). Es ist das Ziel, dabei die internationale Vernetzung weiter voranzutreiben und verstärkt zusammenzuarbeiten.

European At-Large Organisation

Für die technische Verwaltung des Internet ist die Internet Corporation for Assigned Names and Numbers (ICANN) zuständig. Sie hat ihren Sitz in Marina del Rey (Kalifornien) und ist durch ein *Memorandum of Understanding* mit dem US-Amerikanischen Handelsminsterium verbunden (damit untersteht sie diesem de facto). Zu ihren Aufgaben gehören (Deutscher Bundestag 2005):

- Verwaltung und Koordinierung der IP-Adressen als oberste Instanz durch die Vergabe von Adressblöcken an regionale Organisationen, die sie dann weiter verteilen.
- Koordination und Weiterentwicklung des Domain-Name-Systems und Entscheidung über die Einrichtung neuer Top-Level-Domains (*.com, *.de, ...).
- Überwachung des Betriebs des DNS-Rootserver-Systems.

In Deutschland ist die DENIC eG – das Deutsche Network Information Center – für die Registrierung von Domainnamen mit der Länderkennung *.de zuständig.

Die Beteiligung der Zivilgesellschaft erfolgt über das *At-Large Advisory Comittee (ALAC),* ein Komitee frei gewählter Anwender-Vertreter, in dem aktuell Annette Mühlberg vom *Netzwerk Neue Medien* (Berlin) den Vorsitz führt. Institutionen können sich als *At-Large-Strukturen (ALS)* registrieren lassen und zu *Regionalen At-Large Organisationen (RALO)* auch grenzüberschreitend zusammenschließen.

Das FIfF ist als ALS registriert und beteiligt sich an der Initiative, eine europäische regionale At-Large-Organisation (EURALO) zu gründen. Das erste Treffen fand unter Beteiligung mehrerer Organisationen aus verschiedenen europäischen Ländern Ende

Stefan Hügel

Stefan Hügel ist Mitglied im FIfF-Vorstand und vertritt das FIfF in der EDRi-Generalversammlung und in der Initiative zum Aufbau einer EURALO. Er ist Informatiker und lebt in München.

Mai in Frankfurt am Main statt; das zweite Treffen, bei dem vor allem die Satzung diskutiert und die Gründung der Organisation vorbereitet wurde, am 17. September 2006 in Berlin.

Ziel ist die Gründung der Organisation im Rahmen des Internet Governance Forum in Athen und anschließend die Unterzeichnung eines Memorandum of Understanding. Ob dieser Zeitplan eingehalten werden kann wird sich zeigen – die Diskussionen über die Satzung sind momentan noch nicht abgeschlossen.

Referenzen

Deutscher Bundestag (2005): Die Regulierung des Internets – Strukturen, Aufgaben und Arbeitsweisen von ICANN, DENIC, CENTR, CORE und ORSN, Ausarbeitung der wissenschaftlichen Dienste des Bundestags, November 2005, www.bundestag.de/bic/analysen/2005/2005_11_281.pdf

European Digital Rights (EDRi): *www.edri.org*

EDRi-gram: *www.edri.org/edrigram*; auf Deutsch: *www.unwatched.org*; EDRi-gram kann man auch abonnieren: mailto: *edri-news-request@edri.org*; Subject: subscribe

Internet Corporation for Assigned Names and Numbers (ICANN): *www.icann.org*

At-Large Advisory Comittee (ALAC): *www.icannalac.org*

Internet Governance Forum (IGF): *www.intgovforum.org*, *www.igfgreece2006.gr*

World Summit on the Information Society (WSIS): *www.wsis.org*

Dagmar Boedicker

Die cleveren Dinge für überall – oder wir im Netz der Dinge?

Neue FIfF-Broschüre zu RFIDs

RFIDs sind weder technisch noch sozial und politisch ein triviales Thema, sie werden uns in Zukunft vielleicht sogar mit ökologischen oder gesundheitlichen Problemen konfrontieren. Das ist die eine Seite, die andere präsentiert ein spannendes Spektrum immens nützlicher Anwendungen. Und weil die reichhaltige Information aus dem Web, teils von interessierter Seite, nach einem kompakten Überblick zu rufen schien, haben wir und andere uns wieder an die Arbeit gemacht, wie schon bei der elektronischen Gesundheitskarte im letzten Jahr.

Wenn Sie also etwas zu den vielfältigen Aspekten dieses Themas wissen möchten, sollten Sie sich diese Broschüre besorgen. Für die Lektüre brauchen Sie keine umfassenden Vorkenntnisse, ein wenig technisches Verständnis ist aber hilfreich. - Wir haben die Veröffentlichungen zu diesem Thema gesichtet und namhafte Autorinnen und Autoren aus verschiedenen Fachgebieten und Institutionen um Beiträge gebeten. Auch FIfF-Mitglieder beschäftigen sich mit dem Thema und haben etwas zu dieser Broschüre beigetragen.

Die Autoren sind

* Uwe Wissendheit und Dina Kuznetsova vom Lehrstuhl für Informationstechnik der FAU Erlangen
* Sarah Spiekermann und Holger Ziekow von der Humboldt-Universität zu Berlin
* Gabriele Spenger von Philips Semiconductors
* Rena Tangens vom FoeBuD e.V.
* L. Humbert (Studienseminare für Lehrämter an Schulen), J. Koubek (Humboldt-Universität zu Berlin), A. Pasternak (Fritz-Steinhoff-Gesamtschule Hagen), H. Puhlmann (Studienseminar am Gymnasium Altdorf)
* Dagmar Boedicker und Michael Riemer vom FIfF e.V.

Es geht um die Varianten der RFID-Technik (ihre physikalisch-technische Grundlagen), um den Stand der Implementierung und die zukünftigen Entwicklungen, eine technische Analyse RFID-bezogener Angstszenarien, kryptographische Methoden auf RFID-Systemen und den Datenschutz allgemein, in dem sich FoeBuD e.V. bereits profiliert hat, Anforderungen an das politische Handeln und darum, wie viel informatische Bildung/ Kompetenz nötig ist, um mit der Entwicklung angemessen umzugehen.

Auch diese Broschüre enthält ein Glossar, damit Sie das technische und gesundheitspolitische Fachchinesisch rund um RFIDs besser überblicken können, und eine kommentierte Liste von Internet-Seiten, damit Sie sich leichter zurechtfinden, wenn Sie selbst weiter suchen wollen.

Wenn Sie sich für diese Broschüre interessieren, können Sie sie zum Preis von 3,50 Euro zuzüglich Versandkosten bestellen bei

FIfF e.V.

Goetheplatz 4

D-28203 Bremen

oder im Buchhandel beziehen, ISBN: 978-3-9802468-6-6

oder kostenlos von unserer Website als PDF-Datei herunterladen: http://www.fiff.de

Ulrike Wilkens

FIfF-Fotowettbewerb 2006

Beeindruckendes gesehen und Bemerkenswertes gezeigt

Anlässlich der FIfF-Jahrestagung 2006 hatten wir einen Foto-Wettbewerb ausgeschrieben. Der Appell „Dank Informatik? - Alles zeigen!“ sollte eine Herausforderung für alle sein, die sich Gedanken über die Auswirkungen der Informatik machen und sich der Frage stellen wollen, ob und wie sich auch die bedenklichen Errungenschaften und ihre Folgen in einem Bild einfangen und darstellen lassen. Als Wettbewerbsbeiträge haben wir uns digitale Fotografien gewünscht - und bekommen:

Bis zum 16. Oktober 2006 sind beim FIfF 110 Beiträge von 19 Teilnehmerinnen und 28 Teilnehmern eingetroffen.

Sie kamen aus Baden-Württemberg, Bayern, Berlin, Bremen, Niedersachsen, Nordrhein-Westfalen, aus dem Saarland, aus Sachsen und aus Thüringen, aus dem Ausland sind Einsendungen aus den Niederlanden, aus der Schweiz und aus der Tschechischen Republik eingegangen.

Informatisch Bemerkenswertes wurde vor der eigenen Haustür entdeckt. So z. B. „Platinen unter Platanen“ in Berlin-Kreuzberg, oder die Dokumentation der technischen Randbedingungen während der Fußball-WM-Achtelfinalpaarung Brasilien gegen Ghana im Dortmunder Westfalenstadion, die zeigen, was die globale Wahrnehmung des lokalen Geschehens erst möglich macht – mit einer überraschenden Ästhetik.

Das Foto mit dem am weitesten entfernten Motiv wurde laut Auskunft des Teilnehmers in Kambodscha aufgenommen – ein Versuch, die „totale Informatisierung der Weltgesellschaft unter den Bedingungen der ökonomischen Globalisierung“ zum Thema zu machen und die daraus resultierenden Widersprüche zu zeigen:

Matthias Krauß, Bremen

„Auf dem Foto nun stehen sich nicht nur zwei gänzlich unterschiedliche Kulturen gegenüber, repräsentiert von dem jungen buddhistischen Mönch Leang und einem recht bekannten Produkt des reichsten Mannes der Welt. Vielmehr erreicht auf diesem Foto ein westliches Kulturprodukt den Mönch in seinem kambodschanischen Alltag, beeinflußt sein Denken und Handeln, schafft neue Realitätsauffassungen, neue Ideale und neue Anforderung an einen sich verändernden lokalen Lebensalltag. Durch solche von internationalen (Medien-)Konzernen initiierte 'Begegnungen', die in den Entwicklungsländern längst Normalität geworden sind, entsteht so zwar keine uniforme Weltkultur, die weltweite Diversität menschlicher Werte, Stile und Praktiken aber gerät in diesem Prozess zunehmend in die Abhängigkeit einer Kultur des globalen Kapitalismus. Dank Informatik." (Jan Boenkost, Lilienthal)

Die verschiedenen Ausdrucksformen, in die die Antworten auf unseren Wettbewerb verpackt wurden, haben uns überrascht und beeindruckt. Oft wurden die Einsendungen begleitet durch Texte, die Auskunft über den Entstehungsprozess des Bildes, den Ursprung der Idee oder den persönlichen Bezug zu kritischen Aspekten der Informatik gaben: Kommentare, Essays, selbst ein Gedicht.

Unsere Preisfrage wurde zum Thema einer Foto-AG an einer Thüringer Schule, woher auch der jüngste Teilnehmer (Jahrgang 1995) kam. Sie hat Menschen am stillen Örtchen zum Nachdenken über die Nummerierung von Klopapierrollenhaltern bewegt, Informatikstudenten vom Schreiben ihrer Diplomarbeit abgehalten, weil sie nun zunächst ihrem Nachdenken über den gläsernen Menschen fotografisch Ausdruck geben wollten - und sie hat Fragen aufgeworfen wie diese:

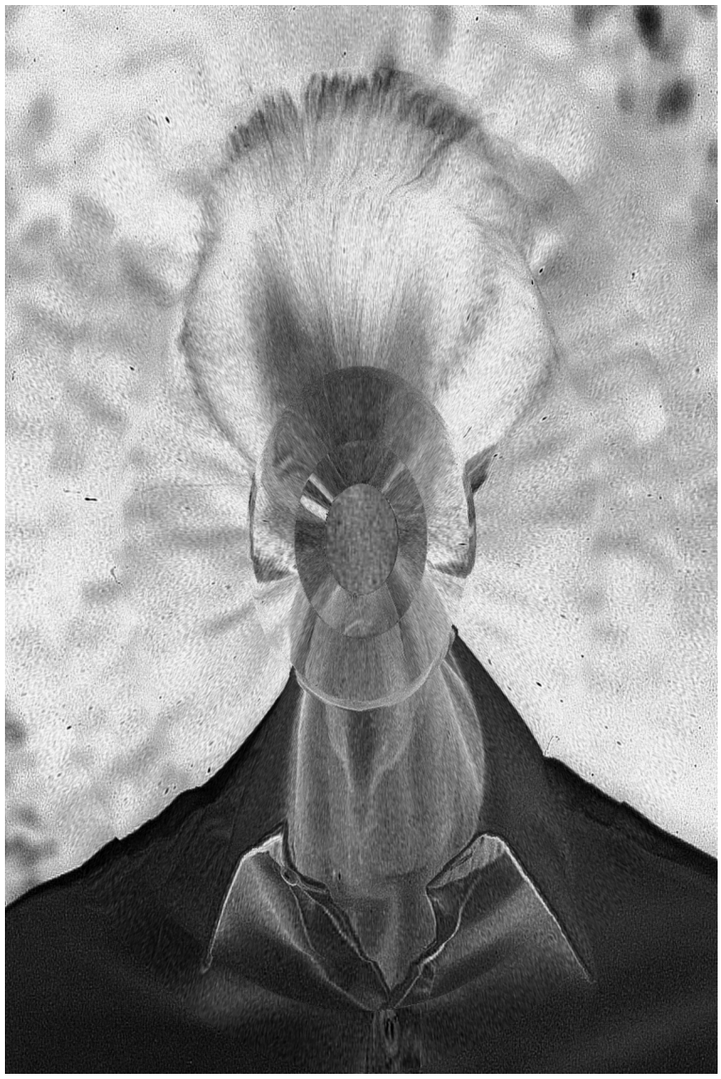
„Wo bleiben Wahrheit, Persönlichkeit und Würde,
wenn alles ‚digital modifizierbar' ist?"
(Fritz J. Schmidhäusler)

Unsere Idee, Anlass zu einer kritisch-kreativen Auseinandersetzung mit dem Motto „dank Informatik" zu geben, hat also viele Früchte getragen. Als Wettbewerbsbeitrag waren digitale Fotografien gefordert. Sie sollten „alles zeigen" – und dies auch für sich allein tun können. Alle Bilddateien wurden anonymisiert und mit Titel versehen an die Mitglieder der Jury weitergegeben: Die Jury musste sich mit Einzelbeiträgen, Fotosammlungen und Bilderstrecken befassen. Die Bandbreite der inhaltlichen und technischen Auslegung unserer Wettbewerbs-Ausschreibung war groß – und die Interpretation der Ergebnisse durch die Jury gewiss nicht immer leicht. Schon die Organisatoren des Wettbewerbs gerieten bei der Sichtung und Weiterleitung der Beiträge oft ins Grübeln:

- Erschließt sich die Aussage dieses Fotos wirklich ohne den beigefügten Kommentar?
- Ging hier nicht eine Idee in den technischen Möglichkeiten ihrer Umsetzung unter?
- Sehen wir wirklich ein Foto, oder beherrscht hier jemand die digitale Fotomontage so perfekt, dass wir selbst nicht mehr entscheiden können, ob wir dem Abgebildeten auf den Grund oder der visuellen Täuschung auf den Leim gehen – dank Informatik!

Die Arbeit der Jury war also gewiss nicht leicht – aber anregend. Die drei Preisträger wurden während der FIfF-Jahrestagung im Rahmen der Ausstellungseröffnung bekanntgegeben:

3. Preis: (111 Euro) (Gen-Fotografie, Fritz J. Schmidhäusler, Mönchengladbach)



„Wo bleiben Wahrheit, Persönlichkeit und Würde, wenn alles ‚digital modifizierbar' ist?"
(Fritz J. Schmidhäusler)

Aus allen Einsendungen hat das FIfF 20 Beiträge ausgewählt, die – inkl. der drei prämierten Arbeiten – in der Ausstellung vom 4. bis zum 13. November 2006 am Flughafen Bremen als Foto-Prints zu sehen waren.

Für die FIfF-Kommunikation haben wir einige Beiträge herausgegriffen, um einen Eindruck von der Vielfalt der Ideen und Umsetzungen zu vermitteln. Einige sehenswerte Fotos fehlen, sie wären im Schwarz-Weiß-Druck der FIfF-Kommunikation nicht richtig zur Geltung gekommen.

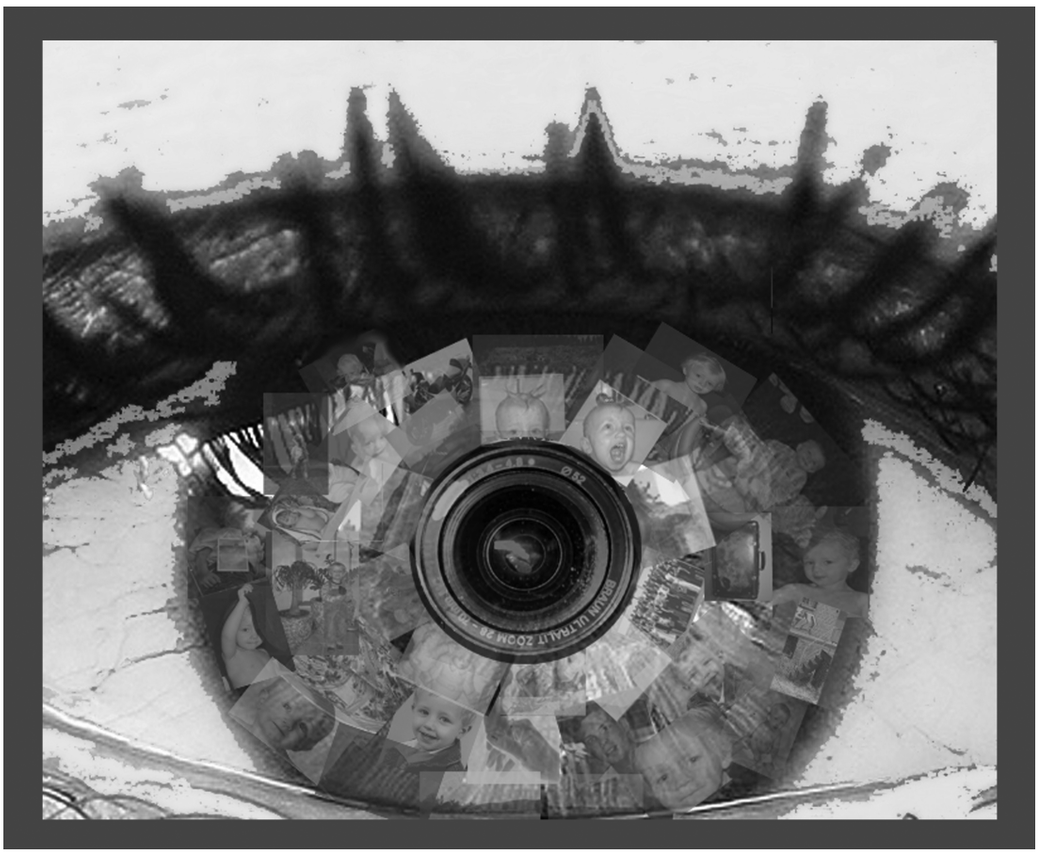
Die prämierten Beiträge sowie weitere Bilder von der Ausstellung finden sich darüber hinaus (natürlich in Farbe) auf den Webseiten des FIfF unter http://fiff.de.

Wir gratulieren den Preisträgerinnen und Preisträgern und danken allen Teilnehmerinnen und Teilnehmern für ihre Beiträge und das Nachdenken über das, was die „andere" Seite der Informatik ausmacht.

Besonderer Dank gilt der Jury für ihr Engagement und die Zeit, die sich alle Mitglieder genommen haben, um das, was mit den Fotos gezeigt werden sollte, auch zu sehen:

* Kurd Alsleben, Netzkünstler und Professor an der Hochschule für bildende Künste, Hamburg,
* Dagmar Boedicker, FIfF, technische Redakteurin, München,
* Carsten Büttemeier, FIfF, früher Layouter der FIfF-Kommunikation (Paderborn),
* Martin Koplin, Medienkünstler und Medienwissenschaftler, Bremen,
* Liane Otholt, Künstlerin, Bremen, und
* Julia Stoll, FIfF, Docent Software Engineering, Fontys Technische Hogeschool Venlo, The Netherlands.

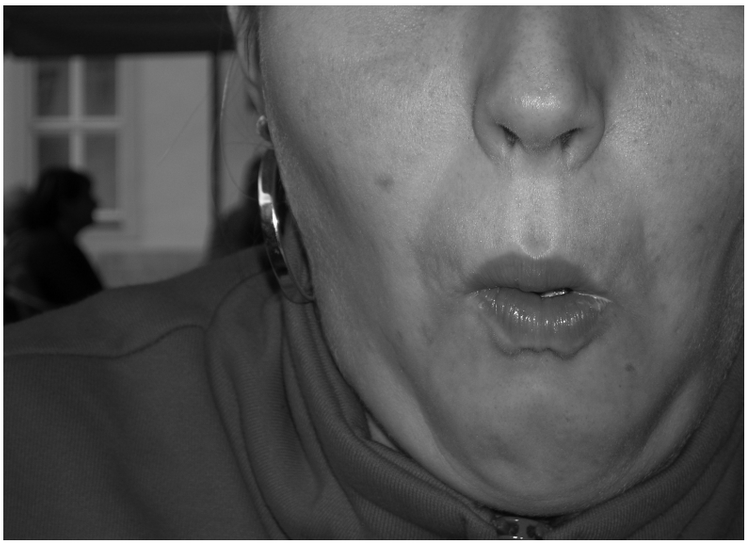
1. Preis: (333 Euro) (Sinnfreie Fotografie, Lukas Eckert, Grenzach-Wyhlen)



2. Preis: (222 Euro) (ohne Titel, Jennifer Pahl, Pr. Oldendorf)

Auch wird immer alles schneller und kurzlebiger doch es gibt auch ein paar Ausnahmen die es langsam angehen lassen und dabei auch noch uralt werden. (Anja Graf, Karlshuld).

ohne Titel (Manfred Krause, Berlin)



Meine, eigentlich hübsche, Freundin, ... wurde ein Opfer des Vollzoom. Mir scheint, er ermöglicht Perspektiven, die eigentlich keiner sehen will. (Maria Thulke, Mauer)

Pixel, Pixel wo kommst du her?
Wo gehst du hin?
Was du da machst, macht das Sinn?
Hast du nicht mehr zu bieten als eins und null?
Das Fühlen und Spüren,
warum bleibst du stumm?
Du dienst uns, bist berechenbar.
Gefühl aber ist anders, Gefühle sind wahr!
(Christian Möller, Leipzig)

...Ich sage: ohne Informatik hätten die Menschen Zeit, komplizierte Dinge zu verstehen und zu sehen, weil sie ihnen nicht von einem Medium genommen würde, das selbst keine Zeit hat, sie zu erklären. Klipps, klipps, klipps. ...
(Nataliya Kovalova, Stuttgart)

thought n sight control
(Karin Demuth, Bremen)

Ob als Teilnehmer, Jury oder Organisations-Team der Jahrestagung 2006 sind wir uns wohl alle einig:

„Wir haben Beeindruckendes gesehen und Bemerkenswertes gezeigt."

Im Netz der Informatik (Martina Kraemer, Gräfelfing)

Videoüberwachung
(Johannes Röhnelt, Sankt Augustin)

Alltagswelt

... Man kann nebenher arbeiten oder nebenher die Kinder erziehen. Einkäufe werden nebenher online bestellt und nach Hause geliefert ...

(Jennifer Neumann, Hannover)

Ulrike Wilkens

Dr. Ing. Ulrike Wilkens ist promovierte Diplom-Informatikerin. Seit November 2001 leitet sie das Multimedia-Kompetenzzentrum an der Hochschule Bremen und ist dort mit dem Aufbau der Koordinierungsstelle für Neue Medien in der Lehre befasst. Schwerpunkt ihrer Arbeit ist die Entwicklung netzbasierter Lernszenarien in ihrer technischen und didaktischen Dimension.

Gerrit Hornung

Ein Jahr neuer Reisepass – quo vadis Biometrie?

Seit dem 1. November 2005 werden in Deutschland neue Reisepässe mit RFID-Chips ausgegeben, auf denen biometrische Daten des Gesichts gespeichert sind. Ein Jahr später rücken die Erweiterung um Fingerabdrucksdaten und die Einführung des neuen Personalausweises näher. Ob die Technik im Massenbetrieb besteht, lässt sich derzeit noch nicht beurteilen – sicher ist aber, dass wichtige rechtliche und politische Fragen bislang offen geblieben sind.

Seit den Terroranschlägen des 11. September 2001 betreiben nahezu alle Regierungen weltweit die Aufnahme biometrischer Daten in ihre Reisepässe. Neben den Sicherheitspolitikern der einzelnen Staaten treiben insbesondere der außenpolitische Druck der USA und die internationalen Standardisierungsaktivitäten der *Internation Civil Aviation Organization (ICAO)* diese Entwicklung voran. Die Europäische Union erließ am 13. Dezember 2004 eine Verordnung mit technischen Vorgaben für die Einführung von Gesichts- und Fingerabdrucksdaten. Mit dem Start am 1. November 2005 war Deutschland unter den ersten Ländern, die die neue Technologie einführten. Der Pass enthält seitdem einen RFID-Chip mit einem komprimierten Volldatensatz des Gesichts. Die Gebühr für die Ausstellung wurde von 26,- auf 59,- Euro (bzw. von 13,- auf 37,50 Euro bei Ausstellung vor Vollendung des 26. Lebensjahres) angehoben. Die alten Reisepässe bleiben für den vollen Zeitraum gültig, für den sie ausgegeben wurden.

Hintergrund: Rechtsgrundlage und technische Funktionsweise

Die Einführung des neuen Reisepasses erfolgte auf der Basis der erwähnten EU-Verordnung. Das geltende deutsche Passrecht erwähnt zwar seit den Änderungen durch das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 biometrische Daten, ist aber nach seinem ausdrücklichen Wortlaut unvollständig und enthält folglich keine hinreichende Ermächtigungsgrundlage. Allerdings finden sich datenschutzrechtliche Vorgaben wie das Verbot einer bundesweiten Datei und ein Auskunftsanspruch der Passinhaber. Die EU-Verordnung, erlassen vom Europäischen Rat in Form des Rates der Innenminister, verfolgt – ausweislich Erwägungsgrund Nr. 2 – das Ziel, „höhere, einheitliche Sicherheitsstandards für Pässe und Reisedokumente zum Schutz vor Fälschungen festzulegen. Zugleich sollen auch biometrische Identifikatoren in die Pässe oder Reisedokumente aufgenommen werden, um eine verlässliche Verbindung zwischen dem Dokument und dessen rechtmäßigem Inhaber herzustellen". Unter den verschiedenen biometrischen Merkmalen, die hierfür in Betracht kämen, hat sich der Europäische Rat für das Gesichtsbild und den Fingerabdruck entschieden. Er wählte überdies den Weg der europaweit für alle Mitgliedstaaten unmittelbar verbindlichen Verordnung, um eine einheitliche technische Lösung für die verschiedenen europäischen Reisedokumente, Visa und Asylbewerberdateien sicherzustellen.

Der Ablauf biometrische Systeme lässt sich verallgemeinernd wie folgt beschreiben: Zunächst werden im Rahmen des so genannten Enrolments Referenzdaten des Merkmalsträgers gewonnen und gespeichert. Schlägt dies fehl (etwa weil ein Passinhaber ein Merkmal überhaupt nicht oder nicht in hinreichender Ausprägung für die biometrische Authentifikation besitzt), so wird der prozentuale Anteil der fehlgeschlagenen Versuche als *False Enrolment Rate* oder *Failure to Enrol Rate (FER)* bezeichnet. Die Speicherung der Referenzdaten kann in vollständiger Form (Roh- oder Volldaten; so beim Gesichtsbild des neuen Passes) oder als extrahierter Datensatz (so genannte Templates; geplant beim Fingerabdruck) erfolgen. Beim späteren Vergleichsprozess *(Matching)* werden die aktuell erhobenen Daten mit den gespeicherten Referenzdaten verglichen. Dies geschieht beim neuen Reisepass dezentral, also nur mit den auf dem Pass vorhandenen Daten. Aufgrund von Messfehlern, zu geringen

Merkmalsausprägungen und anderen Ungenauigkeiten ergibt sich beim Matching niemals ein eindeutiges Ergebnis; Falschakzeptanzen und -zurückweisungen sind nie ganz auszuschließen. Die Wahrscheinlichkeit einer ungerechtfertigten Zurückweisung wird als *False Rejection Rate (FRR),* die einer ungerechtfertigten Akzeptanz als *False Acceptance Rate (FAR)* bezeichnet. Diese sind voneinander abhängig: eine Reduzierung der einen Rate hat einen – nicht notwendig antiproportionalen – Anstieg der anderen zur Folge.

Die Daten des Passes sind auf einem Mikrochip gespeichert, der über eine RFID-Antenne ausgelesen werden kann. „RFID" wird derzeit regelmäßig als Sammelbezeichnung für eine Vielzahl technischer Anwendung (Logistik, Archivierung, WM-Tickets, Bezahlsysteme in der Gastronomie, Kundenkarten) verwendet. Man muss sich allerdings klarmachen, dass diese Anwendungen lediglich eine Schnittstellentechnologie – nämlich die Datenübertragung mittels Radiofrequenzwellen – gemeinsam haben. Diese verursacht zwar – insoweit verallgemeinerbar – durch die

Möglichkeiten der kontaktlosen Datenübertragung Probleme für Datensicherheit und Nutzertransparenz. Die weiteren Fragen der Datenverwendung hinter der Schnittstelle können aber nur in Bezug auf die einzelne Applikation beantwortet werden.

Verfassungsrechtliche Anforderungen

Aus dem Zusammenspiel des Rechts auf informationelle Selbstbestimmung mit weiteren Grundrechten (insbesondere dem Gleichheitssatz) und allgemeinen rechtsstaatlichen Anforderungen ergibt sich eine Reihe verfassungsrechtlicher Anforderungen an die Verwendung von Biometrie in Identitätspapieren, die hier nur im Überblick behandelt werden kann:

- Die gegenwärtige Fassung des deutschen Passgesetzes ist durch die vorrangige EU-Verordnung teilweise gegenstandslos geworden. Aus dem Grundsatz der Normenklarheit folgt, dass dieser Zustand alsbald zu ändern ist. Notwendig sind außerdem Bestimmungen, die aus verfassungsrechtlicher Sicht zum Schutz der betroffenen Grundrechte erforderlich sind. Diese müssen ausreichend spezifisch und detailliert sein, weil sie einen Ausgleich für die Tiefe des Grundrechtseingriffs darstellen.

- Das biometrische Verfahren muss zum Zweck der Authentifikation geeignet sein, d.h. hinreichend niedrige Fehlerraten aufweisen. Ob dies bei den derzeit eingesetzten Verfahren der Fall ist, lässt sich schwer beurteilen, da bisherige Feldversuche oftmals mit kleinen, nicht für die Gesamtbevölkerung repräsentativen Testgruppen (Vielflieger, Mitarbeiter des BKA) arbeiten. Jedenfalls weist die Gesichtserkennung weitaus höhere Fehlerraten auf als die Erkennung von Iris- oder Fingerabdruck. Für den Einzelnen wird oftmals entscheidend sein, wie mit Abweisungen des Systems umgegangen wird (s.u.).

- Bei der Wahl zwischen Volldatensätzen und Templates sind letztere grundsätzlich vorzuziehen, da sie weniger Informationen über den Passinhaber enthalten und niedrigere Fehlerraten aufweisen. Bei der Gesichtserkennung ist allerdings in absehbarer Zeit nicht mit einer Standardisierung von Templates zu rechnen, sodass diese Anforderung mit praktischen Bedürfnissen kollidiert.

- Zur Gewährleistung des datenschutzrechtlichen Transparenzgebots müssen bei der Verwendung von RFID-Systemen effektive Authentisierungsmechanismen eingesetzt werden, die ein unbemerktes Auslesen verhindern. Der deutsche Pass verfügt in der ersten Erweiterungsstufe über einen „schwachen" Authentifizierungsmechanismus, der den Zugriff auf die Daten nur erlaubt, wenn das Lesegerät über einen spezifischen Schlüssel verfügt, den es aus den – zuvor automatisiert optisch gelesenen – Passdaten berechnet. Als letzte Lösung verbleibt für den Bürger schließlich der Selbstschutz, etwa der Transport des Passes in einer Verpackung, die das vom Lesegerät ausgehende elektromagnetische Feld abschirmt.

- Dieser Mechanismus schützt allerdings nicht gegen ein Auslesen nach Diebstahl oder Verlust. Hierzu sind weitergehende kryptographische Zugriffsmechanismen erforderlich. Deren Effektivität wird allerdings durch das Erfordernis einer weltweiten Verteilung der Zugriffsberechtigungen stark reduziert.

- Unter gleichheitsrechtlichen Gesichtspunkten ist zu fordern, dass biometrische Systeme diskriminierungsfrei implementiert werden. Bei einer dauerhaften oder vorübergehenden Nichteignung zur Authentifikation (z.B. durch Behinderungen oder Erkrankungen) liegt ebenso eine Ungleichbehandlung vor wie dann, wenn das System unterschiedliche Erkennungsleistungen hinsichtlich Merkmale wie Geschlecht, Rasse oder Alter hat. Biometrische Grenzkontrollsysteme sind deshalb ohne effektive Rückfallsysteme verfassungsrechtlich unzulässig. Eine Möglichkeit sind manuelle Nachkontrollen. Diese haben ohne größere zeitliche Verzögerungen oder sonstige Nachteile für die Betroffenen zu erfolgen.

- Die gegenwärtige Rechtslage verbietet – von kleinen Ausnahmen abgesehen – den Gebrauch biometrischer Passdaten im privaten Bereich. Eine Änderung dieser Regelung wäre verfassungsrechtlich akzeptabel, wenn die Freiwilligkeit der Anwendung gesichert wird und eine gegenseitige Authentisierung mit einem Lesegerät erfolgt, welches zuvor zertifiziert wurde. Ein strafbewehrtes Verbot könnte außerdem dem Missbrauch der Daten entgegenwirken.

Verbot bundesweiter Dateien – auf Dauer?

Der neue Reisepass wirft eine Fülle datenschutzrechtlicher und sicherheitstechnischer Probleme auf. Allerdings sind einige der in der letzten Zeit in der Fachöffentlichkeit diskutierten Missbrauchsgefahren bei näherem Hinsehen in beiderlei Hinsicht kaum relevant. So demonstrierte im Sommer 2006 ein deutscher Sicherheitsexperte, dass sich die Daten des neuen Passes mit entsprechendem Aufwand „klonen", also auf ein neues Dokument übertragen lassen. Da im Datensatz allerdings die Gesichtsdaten mit den Namensangaben zusammen elektronisch signiert werden, entsteht so allenfalls ein exaktes Duplikat, das zumindest keine über den Diebstahl eines Passes hinausgehenden Sicherheitsfragen aufwirft. Allgemein gilt, dass aus grundrechtlicher Perspektive die Biometrie solange verhältnismäßig unproblematisch ist, als sie – über die genannten Anforderungen hinaus – ausschließlich in spezifischen, gesetzlich klar umrissenen Einzelfällen (etwa bei der Kontrolle am Flughafen) verwendet wird.

Viel folgenschwerer sind demgegenüber die Folgen zentraler biometrischer Datenbanken. Werden diese eingerichtet, so ergeben sich – unter Berücksichtigung des zu erwartenden technischen Fortschritts biometrischer Verfahren im 1:n-Modus, also bei der Identifizierung von Personen aus großen Referenzmengen – in der Zukunft weitreichende Überwachungsmöglichkeiten. Aus diesem Grund werden einige europäische Länder (z.B. Großbritannien) im Zusammenhang mit der Einführung des neuen Passes entsprechende Datenbanken anlegen, und auch in Deutschland haben sich Politiker und der *Bund Deutscher Kriminalbeamter (BDK)* hierfür ausgesprochen.

Demgegenüber bleibt festzuhalten, dass zentrale *und* dezentrale Datenbanken (etwa bei den Passämtern) für die Verwendung des Passes nicht erforderlich sind. Im Ausland werden zentrale biometrische Register mitunter zur Verhinderung der Vergabe

von Mehrfachidentitäten eingesetzt. Hierfür gibt es in Deutschland wegen des hochentwickelten Meldewesens jedoch keine Notwendigkeit. Bei einer Erweiterung der Pass- und Personalausweisregister um biometrische Daten könnte im Fall einer Neubeantragung auf diese Informationen zugegriffen werden. Hierzu bietet sich aber als milderes Mittel die Neuerhebung an. Diese ist schon aus Gründen der Merkmalsveränderung über die Zeit und wegen der zu erwartenden technischen Veränderungen der Verfahren erforderlich.

Das gegenwärtige Passgesetz verbietet die Einrichtung einer bundesweiten Datei. Diese Regelung ist nach wie vor gültig, da die EU-Verordnung diesen Punkt ausnimmt. Allerdings schweigt das geltende Recht zur Möglichkeit der Speicherung der biometrischen Daten bei den Passämtern. Zwar wird man immerhin das Verbot der zentralen Datei so auszulegen haben, dass auch dezentral-vernetzte Systeme unzulässig sind. Die Erfahrung mit dem Problem des staatlichen Zugriffs auf die Maut-Daten des Unternehmens *Toll Collect* im Sommer 2006 zeigt aber, dass die Beständigkeit rein rechtlicher Datenschutzmechanismen begrenzt ist: Dort planen die Regierungsfraktionen, den Zugriff auf die Daten, der derzeit absolut unzulässig ist, in Zukunft in bestimmten Fällen zuzulassen. Um Ähnliches – und damit den Aufbau einer Datenbank, die von jedem Bürger Zeit seines Lebens ein unveränderbares und zur allgemeinen Überwachung geeignetes Kennzeichen vorhalten würde – hier zu verhindern, besteht nur die Möglichkeit, von Anfang an auch auf die dezentrale Speicherung der Referenzdaten zu verzichten und diese nach der Herstellung des Passes zu vernichten.

Hauptprobleme der praktischen Handhabung

Von den praktischen Problemen der Einführung seien an dieser Stelle nur zwei herausgegriffen, nämlich der Umgang mit einer Abweisung durch das System und der mit funktionsunfähigen Reisepässen.

Wird eine Person durch das biometrische System nicht erkannt, so kann das zwei Ursachen haben: entweder der vorgelegte Pass gehört nicht zu der Person, die ihn vorlegt, oder es handelt sich um eine Falschabweisung. Diese kann unterschiedlichste Ursachen haben: Sensorfehler beim Enrolment oder Matching, Produktionsfehler des Passes, Softwareprobleme, Beschädigungen des Chips, eine zu geringe Merkmalsausprägung des Betroffenen und anderes mehr. Die Zahl der Falschabweisungen wird die der Missbrauchsversuche um mehrere Größenordnungen übertreffen. Aus rechtlicher Sicht, aber auch im eigenen Interesse, müssen deshalb Verfahren für den Umgang mit diesem Problem implementiert werden. Die logistischen Herausforderungen sind nicht zu unterschätzen. Schon Fehlerraten, die für heutige Systeme durchaus ambitioniert sind, verursachen bei der Massenabfertigung verhältnismäßig hohe absolute Fallzahlen. So würde am Frankfurter Flughafen ein biometrisches Kontrollsystem mit einer FRR von 1 % etwa 1.000 Fehlalarme pro Tag produzieren.

Für den Einzelnen wird entscheidend sein, welche Art von „Sonderbehandlung“ die Verhaltensanweisungen der Behörden für den Abweisungsfall vorsehen. Wenn etwa lediglich ein oder mehrere weitere Authentifizierungsversuche vorgesehen werden und eins von mehreren positiven Resultaten zum Passieren ausreicht, entstehen keine gravierenden Probleme. Gleiches gilt, wenn eine manuelle Nachkontrolle so zügig erfolgt, dass es nicht zu größeren Verzögerungen kommt. Nicht zu rechtfertigen wäre es angesichts der zu erwartenden Zahl von Falschabweisungen, jeden Betroffenen einer umfangreichen Zusatzkontrolle hinsichtlich seiner Person oder seines Gepäcks zu unterziehen.

Bislang ungelöst ist das Problem des Umgangs mit defekten Pässen, deren Defekt nicht äußerlich erkennbar ist. Von Seiten der Bundesregierung verlautete im Dezember 2005, der Reisepass behalte in diesem Fall seine Gültigkeit, und der Inhaber werde „im Rahmen der Grenzkontrolle der bisher üblichen visuellen Kontrolle unterzogen“. In der Tat dürfte es kaum zu rechtfertigen sein, dem Bürger das Risiko aufzuerlegen, einen ungültigen Pass vorzulegen, dessen Funktionsfähigkeit er selbst nicht kontrollieren kann. Hinter dem Statement der Bundesregierung verbirgt sich aber ein Problem, das letztlich Begründung und Sinn des gesamten Projekts in Frage stellen könnte. Wenn nämlich potenzielle Straftäter durch eine nicht erkennbare Zerstörung des Chips der biometrischen Kontrolle entgehen könnten, würden letztlich nur diejenigen kontrolliert, die ohnehin (objektiv) kein Sicherheitsrisiko darstellen. Die verbleibenden Vorteile, die sich im Logistikbereich (schnellere Abfertigung) abzeichnen, könnten weder den mit der Biometrie verbundenen Grund-

Gerrit Hornung

Dr. Gerrit Hornung, LL.M., ist Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) und Wissenschaftlicher Mitarbeiter an der Universität Kassel. Nach dem Studium der Rechtswissenschaften und der Philosophie an der Universität Freiburg und der Absolvierung eines LL.M.-Studiums an der University of Edinburgh promovierte er 2005 über die rechtlichen Anforderungen an Chipkartensysteme, insbesondere den digitalen Personalausweis und die elektronische Gesundheitskarte, und absolvierte sein Referendariat in Hamburg. Er arbeitet schwerpunktmäßig im Datenschutz- und Multimediarecht.

rechtseingriff, noch die durch das System hervorgerufenen Kosten rechtfertigen.

Der europäische Umweg als Muster

Wie erwähnt, wurde die Rechtsgrundlage für die neuen Pässe nicht durch den deutschen Bundestag, sondern durch den europäischen Rat (in Form der Innenminister) beschlossen. Diese Regelungstechnik zeichnet sich als Muster der Einführung neuer hoheitlicher Überwachungsmaßnahmen und -technologien ab; sie wurde etwa durch die Mitgliedstaaten zunächst auch bei der EG-Richtlinie zur Vorratsdatenspeicherung von Kommunikationsdaten angestrebt. Während sich dort allerdings im Ergebnis das EU-Parlament zumindest insoweit durchsetzen konnte, als es eine Verabschiedung im Mitentscheidungsverfahren erstritt, wurde es bei der Verordnung zum Reisepass lediglich angehört und überdies in entscheidenden Punkten durch den Rat überstimmt.

Die Pass-Verordnung ist damit zwar kompetenzrechtlich und auch ansonsten formell ordnungsgemäß zustande gekommen. Dennoch lässt sie an der Legitimität des mit ihr verbundenen Eingriffs in die Grundrechte der Bürger der Europäischen Union zweifeln. Im Vorfeld der Verabschiedung der europäischen Verordnung fehlte nicht nur so gut wie jede öffentliche Diskussion über die Chancen und Risiken der Einführung der biometrischen Daten, sondern es gab auch – soweit ersichtlich – in keinem Mitgliedstaat eine formelle Zustimmung zu der Maßnahme. In Deutschland war der Fortgang der Arbeiten auf der europäischen Ebene zwar Gegenstand verschiedener parlamentarischer Fragestunden, es erfolgte aber keine politische Willensäußerung des Bundestags, der sich im Terrorismusbekämpfungsgesetz die näheren Entscheidungen ausdrücklich vorbehalten hatte. Dieser Vorgang ist ein geradezu prototypisches Beispiel für das so genannte „Demokratiedefizit" der Europäischen Union. Nach der Rechtsprechung des Bundesverfassungsgerichts wird die demokratische Legitimation von Maßnahmen der Union, die in Grundrechte eingreifen, durch die nationalen Parlamente vermittelt, die über die im Rat entscheidenden Minister die Kontrolle ausüben. Dem Europäischen Parlament komme eine unterstützende Funktion zu. Dieser Befund ist verschiedentlich als empirisch nicht haltbar kritisiert worden, weil bei Ratsentscheidungen de facto so gut wie keine Mitsprache der nationalen Volksvertretungen stattfinde. Das gilt auch für den konkreten Fall und wäre umso problematischer, wenn dieser Weg in Zukunft öfter beschritten werden sollte.

Ausblick

Welche der genannten verfassungsrechtlichen und technischen Herausforderungen des neuen Reisepasses entscheidend sein werden, wird erst der Masseneinsatz in der Praxis zeigen können. Gerade der praktische Umgang der Kontrollbehörden mit dem Pass wird eine erhebliche Auswirkung auf die endgültige rechtliche Bewertung haben. Das ist umso wesentlicher, als es sich bei biometrischen Systemen und RFID-Chips um Teile einer neuen Identifizierungsinfrastruktur handelt, die in Zukunft in immer mehr Lebensbereichen (etwa beim neuen, „digitalen" Personalausweis und in weitem Umfang auch im betrieblichen Umfeld) eingesetzt werden wird.

Die grundsätzliche Kritikwürdigkeit des gewählten Regelungsverfahrens ist schließlich überdeutlich. Hierbei handelt es sich zwar um ein allgemeines Problem des europäischen Verfassungsrechts; dieses tritt jedoch am Beispiel der europäischen Reisepässe besonders hervor. Nicht nur, aber auch deshalb sollte die politische und gesellschaftliche Öffentlichkeit die weiteren Implementierungsschritte des neuen Reisepasses kritisch begleiten.

Literatur

Albrecht, A., Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Baden-Baden 2003.

Article 29 Data Protection Working Party, Working Paper 112: Opinion on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, 1710/05/EN, abrufbar unter http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp112_en.pdf, 2005.

Büro für Technikfolgenabschätzung beim Deutschen Bundestag, Biometrie und Ausweisdokumente. Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung. Zweiter Sachstandsbericht, BT-Drs. 15/4000, 2004.

Golembiewski, C.; Probst, T., Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen, abrufbar unter http://www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf, Kiel 2003.

Gundermann, L.; Probst, T., Biometrie, in: Roßnagel, A. (Hrsg.), Handbuch zum Datenschutzrecht. Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003.

Hornung, G., Biometrische Systeme – Rechtsfragen eines Identifikationsmittels der Zukunft, Kritische Justiz 2004, 344.

Hornung, G., Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, 2005.

Hornung, G.; Steidle, R., Biometrie am Arbeitsplatz – sichere Kontrollverfahren versus ausuferndes Kontrollpotential, Arbeit und Recht 2005, 201.

Roßnagel, A.; Hornung, G., Reisepässe mit elektronischem Gesichtsbild und Fingerabdruck. Die EG-Verordnung 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, Die Öffentliche Verwaltung 2005, 983.

Roßnagel, A.; Hornung, G., Biometrische Daten in Ausweisen, Datenschutz und Datensicherheit 2005, 69.

Roßnagel, A.; Hornung, G., Datenschutzrechtliche Anforderungen/Möglichkeiten zur Erfüllung, in: Reichl, H.; Roßnagel, A.; Müller, G. (Hrsg.): Digitaler Personalausweis. Eine Machbarkeitsstudie, Wiesbaden 2005, 106 / 223.

Silke Stokar, innenpolitische Sprecherin der Bundestagsfraktion Bündnis 90 / Die Grünen
28.09.2006: 54. Sitzung des Deutschen Bundestages

Zur Beratung des Antrags der Fraktion Bündnis 90/Die Grünen (Plenarprotokoll 16/54)

Informationspflicht für Unternehmen bei Datenschutzpannen einführen

Sehr geehrte Damen und Herren,

Deutschland war nach dem grundlegenden Volkszählungsurteil des Bundesverfassungsgerichts lange Jahre Vorreiter in Sachen Datenschutz. Einiges davon ist bis heute geblieben. Denken wir nur an die unabhängige Rolle des Bundesdatenschutzbeauftragten. Wir haben hier Standards gesetzt für die europäische Rechtentwicklung.

Allerdings ist unser Datenschutzrecht vielfach schlicht in die Jahre gekommen. So nimmt unser Gesetz noch nicht hinreichend auf, dass eine immer größere Gefahr für das Recht auf informationelle Selbstbestimmung gerade auch von nicht-öffentlichen Stellen ausgeht.

National und international steigt die Zahl der sogenannten „Identitätsdiebstähle". Die Fälle von Kreditkartenbetrug durch die missbräuchliche Verwendung von Identifizierungsdaten nehmen immer größere Ausmaße an. Durch das sogenannte Pishing im online-Banking entsteht pro Jahr ein grob geschätzter Schaden von 4,5 Millionen Euro. Wir wollen sicherstellen, dass Angriffe auf die IT-Systeme von Unternehmen, die mit personenbezogenen Daten arbeiten, umgehend an die Kunden gemeldet werden müssen. Wir brauchen hier mehr Transparenz, wir müssen die Schutzrechte der Betroffenen stärken und Anreize setzen für mehr präventive Datensicherheit in den Unternehmen. Der Markt allein wird dies nicht regeln.

Das deutsche Datenschutzrecht ist hier nicht mehr auf der Höhe der technischen und wirtschaftlichen Entwicklung. Die Benachrichtigungspflichten des § 20 BDSG sowie die damit eng zusammenhängenden Berichtigungsansprüche in § 35 des Bundesdatenschutzgesetzes beinhalten zu viele Ausnahmetatbestände. Obwohl mit der Novelle des Gesetzes nunmehr in § 7 ein eigenständiger Schadensersatzanspruch des Betroffenen besteht, greift auch dieser zu kurz. Die Beweispflicht für Sorgfaltspflichtverletzungen liegt bei dem Betroffenen. Es ist an der Zeit, diesen Umstand zu ändern. Ich sage das ganz offen: Es wäre das Beste, nicht am bestehenden Gesetz herumzuflicken, sondern die weit gediehenen Vorarbeiten für ein völlig neues Datenschutzgesetz aufzugreifen. Ich hoffe sehr auf ein Signal des Bundesinnenministers, hier entschlossen voran zu gehen.

Andere Länder sind beim Schutz der Konsumenten schon weiter. Das gilt in bestimmten Fällen sogar für einzelne Bundesstaaten der USA. Da reibt man sich verwundert die Augen. Während wir etwa bei der Behandlung der Flugdaten europäischer Passagiere oder beim Geldtransfer riesige Probleme mit den Vereinigten Staaten haben, ist Arnold Schwarzenegger hier Wolfgang Schäuble voraus.

Der sogenannte „Security Breach Information Act" des US-Bundesstaats Kalifornien gilt dort bereits seit dem 1. Juli 2003. Wer als Unternehmen geschäftliche Kontakte zu Bürgern dieses Bundesstaats unterhält, muss seine Kunden über Datenschutzpannen sofort informieren. Ist die vertrauliche Behandlung personenbezogener Daten nicht mehr gewährleistet, muss das Unternehmen reagieren, sonst kann es sich sogar schadensersatzpflichtig machen. Diese gesetzliche Neuregelung hat für andere US-Bundesstaaten bereits eine Vorbildfunktion übernommen. In der Praxis haben diese Gesetzeswerke dazu geführt, dass Informationen über solche Verletzungen mehr und mehr öffentlich bekannt gemacht werden.

Wir haben einen Antrag im Bundestag eingebracht, der die Grundgedanken der US-Regelungen aufgreift. Auch bei uns sollen zum Schutz der Verbraucherinnen und Verbraucher hier tätige Unternehmen zu einer umfassenden Bekanntmachung von Datenschutzpannen verpflichtet werden. Wir fordern, dass Unternehmen bei fahrlässigem Umgang mit personenbezogenen Daten ihrer Kunden zivilrechtlich Schadensersatz leisten müssen. Diese Verletzungen ihrer Sorgfaltspflicht gilt für die Erhebung, Speicherung und Verwertung personenbezogener Daten der betroffenen Personen.

Mit einer bloßen Verpflichtung allein ist es aber nicht getan. Das Gesetz sollte - nach einer Übergangsphase - den Datenschutzaufsichtsbehörden auch die Möglichkeit geben, Ordnungswidrigkeitsverfahren für besonders renitente Unternehmen zu verhängen, die grob fahrlässig ihre Schutzpflichten verletzen und ihren Transparenzverpflichtungen nicht nachkommen.

Wir sind davon überzeugt, dass wir hier auch einen wirksamen Beitrag zu Kriminalitätsbekämpfung leisten können, weil mehr Sorgfalt und Transparenz bei den Unternehmen den kriminellen Nutznießern von zu niedrigen Sicherheitsstandards das Handwerk legt. Die Menschen müssen wissen, wann die Gefahr besteht, dass mit ihren Daten Missbrauch getrieben werden kann. Ich erinnere auch hier an die USA, wo solche staatlichen Sanktionen durch die Handels- und Wettbewerbsbehörde *Federal Trade Commission FTC,* die *Federal Communications Commission (FCC)* oder die Bankenaufsicht verhängt werden können.

Ich hoffe, die Regierungsfraktionen zeigen sich in den Fachausschüssen offen für die Debatte dieses neuen Ansatzes. Die Innovation in der Informationsgesellschaft muss einhergehen mit der Modernisierung des Datenschutzrechtes.

Vielen Dank.

Silke Stokar

Innenpolitische Sprecherin der Bundestagsfraktion Bündnis 90 / Die Grünen

Platz der Republik 1 , 11011 Berlin , Tel.: 0 30 / 2 27 - 7 21 22 Fax: 0 30 / 2 27 - 7 68 22

http://www.stokar.de/bundestag/reden/295260.html

Annette Hauschild

Informationsfreiheitsgesetz

Seit dem 1. Januar 2006 ist das „Gesetz zur Regelung des Zugangs zu Informationen des Bundes" (volkstümlich „Informationsfreiheitsgesetz" oder IFG) in Kraft. Es wird eifrig genutzt, aber der von den Behörden befürchtete Ansturm ist bisher nicht eingetreten.

Nach langem, zähem Ringen ist es so weit, das von Bürgerrechtlern, Datenschützern, Umweltverbänden, Korruptionsbekämpfern und Journalisten zuletzt mit der Ausarbeitung eines eigenen Gesetzentwurfs geforderte Recht auf Akteneinsicht für Jedermann ist nun endlich da. Geschaffen wurde es nach mehreren Anläufen von der rot-grünen Bundesregierung im Rahmen der Modernisierung der öffentlichen Verwaltungen, teilweise gegen heftigen und anhaltenden Widerstand der Ministerialbürokratie, insbesondere der Außen-, Verteidigungs- und Wirtschaftsminister. Es sollte demokratische Willensbildung vorantreiben, die Kontrolle staatlichen Handelns fördern und Verwaltungsentscheidungen für Normalbürger transparenter machen. Das in dem preußischen Verwaltungsdenken wurzelnde „Amtsgeheimnis" sollte abgelöst werden durch einen Rechtsanspruch auf Auskunft durch Behörden.

Federführend beim IFG ist der Bundesminister des Innern.

Das Bundes-IFG hat als Vorläufer verschiedene Gesetze: Der Freedom of Information Act (FOIA) in den USA stand Pate, in den meisten Ländern des alten Europa gab es schon ähnliche Gesetze, und in den Jahren zuvor traten auf Bundeslandebene schon ein paar IFG in Kraft. Das älteste in Brandenburg (1998), das zweitälteste in Berlin im Jahr 1999. Mehr als 60 Staaten haben Informationsfreiheitsgesetze, darunter auch Mexico und Indien. Deutschland gehörte in der EU zu den Schlusslichtern.

Großes Interesse bei Privatleuten und Verbänden

Die FDP-Bundestagsfraktion wollte es im Juni dieses Jahres genauer wissen und fragte in einer Kleinen Anfrage erstmals nach dem Stand der Dinge. Laut der Antwort der Bundesregierung (DS 16/2168) gab es bis Juli 2006 schon 420 Anträge allein bei Bundesministerien.

Von diesen 420 Anträgen wurde in 193 Fällen der Informationszugang vollständig und in 30 Fällen teilweise gewährt, 106 Fälle wurden abgelehnt und ein Fünftel befand sich noch in Bearbeitung. Die Bundesbehörden und nachgeordneten Dienststellen waren in dieser Zahl nicht erfasst, so dass die wirklichen Fallzahlen höher liegen dürften. Auch zum jetzigen Zeitpunkt gibt es noch keine vollständige zentrale Erfassung der Fallzahlen bzw. der Fälle.

Jede Behörde bearbeitet die an sie gerichteten Anträge selbst. Berichtspflichten gibt es zwar, aber mit der Einforderung von Berichten und der Erstellung entsprechender Statistiken durch die vorgesetzten Behörden hapert es noch. Der Bundesdatenschutzbeauftragte, Peter Schaar, der als Beauftragter für Informationsfreiheit auch die Funktion eines Ombudsmannes für IFG-Auskünfte hat, will deshalb mit dem Innenministerium einen Lösungsvorschlag erarbeiten.

Keine Übersicht über die Akten

Es gibt auch keine zentrale Aktensammelstelle, wo man rasch und ohne hohe Kosten nachschauen kann, welche Fälle schon beantragt wurden und ob das eigene Anliegen eventuell auch dabei ist. Dies ist im Gesetz auch gar nicht vorgesehen. Schaar regte zwar an, in Zukunft auf den Internetseiten von Bund und Ländern solche Fallsammlungen, Gerichtsentscheidungen und Stellungnahmen bereitzustellen, aber es ist fraglich, ob – angesichts des Personalabbaus in den Verwaltungen – Kapazitäten dafür frei werden.

Daher haben der Bielefelder Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs (FoeBud e.V.) und der Chaos Computer Club (CCC) unter der Internet-Adresse *http://www.befreite-dokumente.de/* eine Aktensammelstelle eingerichtet, bei der man IFG-Akten einstellen und einsehen kann. Dort sind Akten nach Länder- und Bundes-IFG eingestellt. Der Verein bietet an, dass Akten auch in Papierform eingereicht werden können. Noch ist die Anzahl der Akten allerdings sehr beschränkt, gegenwärtig (September 2006) sind erst 11 Akten online und 8 beantragt. Das mag auch damit zusammenhängen, dass viele Antragsteller auf dem Papierweg Akteneinsicht beantragen und diese Sammelstelle nicht kennen. Es ist zu hoffen, dass sie bald breiteren Kreisen bekannt wird.

Die Haltung der Behörden: A-H-A (Ablehnen, Hinhalten, Abkassieren)

Die ersten, prominent gewordenen Fälle zeigten, dass die Behörden durch Hinhalten, restriktive Handhabung und unverhältnismäßig hohe Gebühren versuchen, BürgerInnen von Auskunftsersuchen abzuschrecken. IFG-Beauftragter Schaar hatte im Juni dieses Jahres schon 120 schriftliche Beschwerden vorliegen, weil Ämter sich auf Geschäfts- und Betriebsgeheimnisse oder auch Vertraulichkeitsvereinbarungen mit Dritten berufen. Die Höhe der Gebühren, die zu Beginn des Jahres mehrfach heftig kritisiert worden war, scheint aber nicht so wichtig zu sein, wie anfangs befürchtet. Vor allem ärgert die Antragsteller, dass vielfach Behörden erst gar nicht reagieren und Antwortfristen verstreichen lassen.

Die ersten prominenten Fälle

Die Bundesagentur für Arbeit: Der Wuppertaler Sozialhilfeverein "Tacheles e.V." musste sich das Recht auf Einsicht in interne Dienstanweisungen der Bundesanstalt für Arbeit vor dem Sozialgericht Düsseldorf erstreiten. Das Gericht verpflichtete die Bundesagentur dazu, ihre Verordnungen im Internet zu veröffentlichen. Da die Agentur das Urteil schnell und vollständig umsetzte, erhielt sie mittlerweile sogar Lob von den Datenschützern.

Das Auswärtige Amt hat eigens einen Arbeitsstab Informationsfreiheit eingerichtet. Die Homepage des Auswärtigen Amtes ist die einzige Homepage der Bundesregierung, die eigens ein Formular für Auskünfte nach dem IFG aufweist. Allerdings verlangte das Amt für eine einfache Auskunft zu Visaerteilungsvorschriften 108 Euro.

Die Maut-Verträge: Der Antrag des SPD-Bundestagsabgeordneten Jörg Tauss auf Einsicht in die 17000 Seiten umfassenden Maut-Verträge zwischen der Bundesregierung und dem Betreiberkonsortium Toll Collect wurde abgelehnt, weil Toll Collect seine Zustimmung verweigerte. Das Verkehrsministerium lehnte auch ab, eine Version zu erstellen, welche die Geschäftsgeheimnisse von Toll Collect schützte. Begründung: Das Ministerium habe nicht genug Kenntnisse der betrieblichen Vorgänge von Toll Collect und deren Wettbewerbern, um die relevanten Dokumente aussortieren zu können.

Ebenfalls verweigert wurden die Anlagen eines Gutachtens der Physikalisch-Technischen Bundesanstalt zur Bauartzulassung von *Wahlmaschinen*, da der Hersteller, die Firma Nedap, der Weitergabe dieser Informationen nicht zustimmte. Das Innenministerium forderte 240 Euro für den Aufwand, diese Dokumente auszusortieren.

Agrar-Subventionen: Ein weiterer IFG-Antrag von politischer Brisanz ist zur Zeit noch in der Schwebe: Ein Bündnis von dreißig Organisationen aus den Bereichen Entwicklungspolitik, Umweltschutz, Journalismus und Bürgerrechte versucht, über den Hebel des IFG die Empfänger von EU-Agrarsubventionen zu erfahren. Während die Hälfte der EU-Mitgliedsstaaten die Nutznießer dieses größten Postens im EU-Haushalt öffentlich nennen, hält Deutschland die Empfänger bisher geheim. Dabei geht es um Zahlungen von jährlich sechs Milliarden Euro allein in der Bundesrepublik. Durch die Transparenz-Initiative der Europäischen Kommission wurde aus anderen EU-Staaten bekannt, dass der Löwenanteil der Agrar-Subventionen nicht an die Landwirte geht, sondern großen Lebensmittelkonzernen zugute kommt. Die Initiatoren der deutschen Initiative erhoffen sich dadurch politischen Druck auf die Bundesregierung zur Offenlegung der Empfänger.

Roll Back in Schleswig-Holstein?

Seit dem Jahr 2000 hat Schleswig-Holstein eines der fortschrittlichsten Informationsfreiheitsgesetze (IFG-SH) in Deutschland, das teilweise auch Vorbild für das IFG des Bundes war. Die schleswig-holsteinische Landesregierung versucht nun allerdings, genau das aufzuweichen. Geplant ist vor allem, privatrechtlich organisierte Unternehmen von der Auskunftspflicht auszunehmen. Dies ist besonders vor dem Hintergrund fatal, dass die öffentliche Hand zunehmend ehemals behördliche Leistungen in private Trägerschaft überführt.

Die Landesregierung hat Ende des Jahres 2005 einen Gesetzesentwurf vorgelegt, der die Europäische Umweltinformationsrichtlinie in das bestehende IFG-SH integriert. Dabei hat sie zwar ein Umwelteinsichtsrecht geschaffen, das Verbrauchern weitgehende Rechte einräumt, aber die weiteren Anwendungsbereiche des IFG-SH sollen nun wesentlich restriktiver gehandhabt werden. Die Neufassung sieht vor, dass das fiskalische Handeln, das ist jede Form zivilrechtlicher Tätigkeit der öffentlichen Verwaltungen, *nicht* mehr dem IFG-SH unterliegen sollen. Ausgeklammert werden auch alle privatrechtlichen Verträge und die Tätigkeiten von Firmen, die im Auftrag der öffentlichen Hand agieren. Begründung des Innenministeriums: es bestehe kein Anlass, die wirtschaftlichen Erledigungen der öffentlichen Hand anders als die der Rechtssubjekte des Privatrechts zu behandeln.

Thilo Weichert, Leiter des Unabhängigen Landeszentrums für Datenschutz (ULD) führt dazu in einer Pressemitteilung aus:

Der Entwurf sieht vor, dass der Anwendungsbereich des geltenden Informationsfreiheitsgesetzes (IFG-SH) erheblich eingeschränkt wird. Das fiskalische Handeln der Behörden soll aus dem Geltungsbereich des Gesetzes herausgenommen werden. Damit würde der Bereich herausfallen, der von besonderem Interesse für die Bürgerinnen und Bürger ist. Möchte man ernsthaft die Transparenz und Akzeptanz der Verwaltung erhöhen sowie die politischen Mitgestaltungsmöglichkeiten der Bürger verbessern, dann kann ein Informationsfreiheitsgesetz sich nicht auf das klassische Verwaltungshandeln begrenzen, das in vielen Sektoren durch privatrechtliche Handlungsformen abgelöst worden ist und kontinuierlich weiter wird. Gleiches gilt für die Herausnahme von natürlichen und juristischen Personen des Privatrechts aus dem Anwendungsbereich des Gesetzes. Die Beschränkung der Geltung des Gesetzes auf Beliehene wird nicht der Tatsache gerecht, dass öffentliche Aufgaben in starkem Maße auf Private übertragen werden, die privatrechtlich tätig werden. Keines der bestehenden Informationsfreiheitsgesetze – auch nicht das des Bundes – sieht diese Einschränkungen vor. Es wäre bedauerlich, wenn Schleswig-Holstein im Bereich der Informationsfreiheit vom Vorbild zum Schlusslicht befördert werden würde. Gleichermaßen unverständlich ist, warum die Offenbarung personenbezogener Daten nunmehr pauschal unzulässig sein soll, obwohl das Landesdatenschutzgesetz selbst Ausnahmen zulässt. Die Herausnahme der Abwägungsklausel beim Schutz von Geschäfts- und Betriebsgeheimnissen ist nicht nachvollziehbar. Diese Klausel sieht eine Abwägung zwischen dem Geheimhaltungsinteresse des Unternehmers und dem Offenbarungsinteresse der Allgemeinheit vor. Es ist nicht ersichtlich, warum diese Abwägung nur noch im Umweltbereich Anwendung finden soll, obwohl sie sich im Bereich der allgemeinen Informationen als sachgerecht erwiesen hat. Weder die Erfahrungen mit dem IFG-SH noch eine veränderte Rechtslage rechtfertigen die genannten Gesetzesänderungen. Im Gegenteil: Die Verabschiedung des Informationsfreiheitsgesetzes auf Bundesebene (Bundes-IFG) sowie die (neue) Umweltinformationsrichtlinie zeigen, dass ein Abbau der Informationszugangsrechte nicht zeitgemäß ist. Die Umsetzung der Umweltinformationsrichtlinie auf Landesebene darf nicht dazu führen, dass Grundprinzipien des IFG-SH ohne Begründung gestrichen werden. (http://www.datenschutzzentrum.de/informationsfreiheit/stellungnahme-060216.htm)

Deshalb hat der Südschlesische Wählerverband SSW einen eigenen Gesetzesentwurf vorgelegt (Landtags-Drucksache 15/3653), der diesen Gefahren gegensteuern soll. Am 20. September fand eine Anhörung des Innen- und Rechtsausschusses im Kiel zu diesem Thema statt, auf der die Landesregierung zwar einerseits bestärkt wurde in dem Vorhaben, das Umwelteinsichtsrecht in das bestehende IFG-SH zu integrieren, sich jedoch scharfe Kritik von Datenschützern, Umweltverbänden und Journalisten zu ihrer Flucht ins Privatrecht anhören musste. Die Entscheidung im Landtag steht aber noch aus. Man darf gespannt sein.

Informationsfreiheit in den Bundesländern

Der Grundsatz der Transparenz für die öffentliche Verwaltung gilt mittlerweile in acht Bundesländern: nach Brandenburg und Berlin Ende der 90er Jahre kamen Schleswig-Holstein seit 2000, NRW seit 2004 hinzu, und in diesem Jahr treten das Saarland, Bremen, Hamburg und Mecklenburg-Vorpommern dem IFG-Club bei.

Offensichtlich ist, dass die Bundesgesetzgebung den Ländergesetzen wieder Schwung verliehen hat, bedauerlicherweise aber lehnen sich die nun an die recht restriktive Fassung des Bundes-IFG an, insbesondere was die weit gefasste Definition der Ausnahme- und Ablehnungsgründe betrifft, erklärt das Netzwerk Recherche, der Verband investigativer Journalisten. Das Hamburger Gesetz geht aber noch darüber hinaus. So z.B. wird Akteneinsicht nur bei abgeschlossenen Verfahren gewährt, nicht bei laufenden. In Bayern gibt es noch kein IFG, da die CSU sich weiterhin sträubt, aber das „Bündnis für Informationsfreiheit" hat schon einen Entwurf erarbeitet. Auch in weiteren Ländern liegen Entwürfe vor. In Sachsen lehnte der Landtag im Jahr 2005 den Entwurf eines Informationszugangsgesetzes ab. Auch Niedersachsen sieht nach wie vor keinen Bedarf für ein entsprechendes Gesetz, und Rheinland-Pfalz hatte im Jahr 2003 einen Gesetzesentwurf der Opposition abgelehnt. In Hessen, dem ehemaligen Stammland des Datenschutzrechtes, gibt es einen neuen Anlauf der Opposition.

Weitere Informationen zur Geschichte, Anwendungsbereich, etc. gibt es im Internet (letzter Zugriff: 5.10.2006) unter:

- http://217.160.60.235/BGBL/bgbl1f/bgbl105s2722.pdf, der Gesetzestext im Bundesgesetzblatt

Annette Hauschild

Annette Hauschild ist Journalistin und Rechercheurin mit den Schwerpunkten investigative Recherche und Wirtschaftskriminalität. Sie war früher Aktivistin gegen Rüstungsexporte, u.a. Anfang der 80er Jahre Mitbegründerin und Koordinatorin der BUKO-Kampagne „Stoppt den Rüstungsexport".

- http://de.wikipedia.org/wiki/Gesetz_zur_Regelung_des_Zugangs_zu_Informationen_des_Bundes
- http://www.befreite-dokumente.de, die Aktensammlung des FoeBud und des CCC
- http://recherche-info.de/kategorie/informationsfreiheitsgesetz
- http://www.datenschutzzentrum.de/material/recht/infofrei/infofrei.htm, der Text des IFG-SH
- http://www.freedominfo.org/
- http://www.datenschutzzentrum.de/presse/20060220-ifg.htm, die Homepage des Unabhängigen Datenschutzzentrums Schleswig-Holstein
- *http://www.heise.de*, die Magazine des Heise-Verlages

Teile dieses Beitrages wurden bereits veröffentlicht in „M", der medienpolitischen ver.di-Zeitschrift.

Kordula Kugele, Martina von Gehlen

„Jede Frau, die überlebt in einem technischen Studiengang, macht zwei anderen die Türe auf"

Ergebnisse der Online-Befragung ehemaliger Teilnehmerinnen der Informatica Feminale Baden-Württemberg 2001-2005

Die Informatica Feminale Baden-Württemberg ist eine Sommerhochschule für Frauen in der Informatik. Zielgruppe der Veranstaltung sind Studentinnen in technischen Studiengängen der Hochschulen des Landes, die Informatik als Haupt- oder Nebenfach studieren. Die Wochen- und Halbwochenkurse, die Workshops und Vorträge, Ringvorlesungen sowie Podiumsdiskussionen der Veranstaltung ergänzen das fachliche Hochschulangebot der (informations-)technischen Studiengänge. Die einwöchige Sommerhochschule findet im jährlichen Wechsel an der Hochschule Furtwangen und der Universität Freiburg statt. Die baden-württembergische Informatica Feminale motiviert Frauen in ihrem Selbstverständnis in technischen Studiengängen und Berufen durch eine fachliche Qualifizierung auf hohem Niveau. Das Lernen unter Frauen auf der monoedukativen Sommerhochschule bietet darüber hinaus eine Plattform zur Vernetzung der Teilnehmerinnen und der Dozentinnen.

Das Netzwerk *Frauen.Innovation.Technik (F.I.T)* besteht seit Februar 2001. Es wird vom Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg finanziert und ist an der Hochschule Furtwangen an der Fakultät Maschinenbau und Verfahrenstechnik angesiedelt. Das Netzwerk F.I.T organisiert die Informatica Feminale Baden-Württemberg, die inzwischen bereits sechs Mal stattgefunden hat, und begleitet die Sommerhochschule wissenschaftlich. Darüber hinaus motiviert das Netzwerk F.I.T mit vielfältigen Projekten und Aktivitäten Schülerinnen und junge Frauen für ein Studium technischer und naturwissenschaftlicher Berufe und fördert die Vernetzung der verschiedenen Zielgruppen.

F.I.T ist in ein großes Maßnahmenpaket des Bundes und der Länder eingebunden, das die Chancengleichheit von Frauen erhöhen soll. Frauen sind in den ingenieurwissenschaftlichen und naturwissenschaftlichen Studiengängen nach wie vor unterrepräsentiert. Ein Frauenanteil von 18% im Fach Informatik (Statistisches Bundesamt 2004) zeigt, dass sich immer noch wesentlich weniger Frauen als Männer für diese Zukunftsberufe entscheiden. Die Studienabbruchquote unter den Informatikstudierenden liegt deutlich höher als die in den Ingenieurwissenschaften. Sie beträgt in der Informatik 38% an Universitäten und 39% an Fachhochschulen (männliche und weibliche Studierende zusammen, eine geschlechtsspezifische Analyse liegt leider nicht vor). In den Ingenieurwissenschaften brechen an Universitäten 28% und an Fachhochschulen 11% der Studentinnen ihr Studium ab. Die niedrige Abbruchquote an Fachhochschulen ist vor allem durch einen relativ niedrigen Studienabbruch im Fachbereich Architektur bedingt, dessen Studiengänge besonders von Frauen nachgefragt werden. (HIS Studienabbruchstudie 2005).

Aufgrund des niedrigen Frauenanteils im Informatikstudium und anderen ingenieurwissenschaftlichen Fächern wie Maschinenbau und Mechatronik in Baden-Württemberg besteht Handlungsbedarf. Informatikerinnen, Ingenieurinnen und Naturwissenschaftlerinnen werden auf Grund des demographischen Wandels und des jetzt schon aktuellen Mangels an hoch qualifizierten Arbeitskräften in diesen Bereichen dringend gebraucht und können mit sehr guten Verdienstmöglichkeiten rechnen. Wie die in der Überschrift zitierte Äußerung einer befragten Studentin verdeutlicht, sind spezifische Angebote für Studentinnen aus Naturwissenschaft und Technik vor diesem Hintergrund auch in Zukunft unerlässlich.

Ziele der Teilnehmerinnen-Nachbefragung

In den Monaten März und April 2006 wurde eine Online-Befragung ehemaliger Teilnehmerinnen der Informatica Feminale Baden-Württemberg (IF BW) durchgeführt. Neben standardisierten Fragen zum Ankreuzen hatten die Umfrageteilnehmerinnen die Möglichkeit, ihre Bewertungen durch offene Antworten zu ergänzen. Insgesamt nahmen 126 Frauen an der Befragung teil. Damit beteiligten sich knapp 30% aller angeschriebenen ehemaligen Teilnehmerinnen, deren E-Mail Adressen zum Befra-

gungszeitpunkt noch gültig waren. Da die Teilnahme an der IF BW zwischen einem und fünf Jahren zurückliegt, ergibt sich in dieser hochflexiblen Gruppe ein erheblicher Schwund an gültigen E-Mail Adressen, es konnten nur noch 456 ehemalige Teilnehmerinnen per E-Mail erreicht werden.

Die Online-Befragung ergänzt die quantitativen und qualitativen Evaluationsinstrumente, die bisher zur Qualitätssicherung der Sommerhochschule eingesetzt wurden. Ziel dieser Befragung ist eine Bewertung der Veranstaltungsteilnahme im Rückblick. Fragen nach dem Nutzen für Studium und Beruf, Fragen des Wissenstransfers und der Vernetzung standen im Vordergrund. Dieser Untersuchungsansatz ist deshalb besonders interessant, weil eine Teilgruppe der Befragten das Studium bereits abgeschlossen hat und im Berufsleben steht und somit die Teilnahme an der baden-württembergischen Informatica Feminale im Hinblick auf den Berufseinstieg und den Praxisbezug bewerten konnte.

Ergebnisse der Befragung

Derzeitige Beschäftigung und Studienabschluss der Befragten

Mit 24% ist der Anteil derjenigen Umfrage-Teilnehmerinnen recht hoch, die die baden-württembergischen Informatica Feminale mehrfach (zwei- bis viermal) besucht hatten. Auf die Frage nach der derzeitigen Beschäftigung gaben 51% der Befragten an, erwerbstätig zu sein, 40% studierten noch. 57% der Befragten hatten ihr Studium zum Befragungszeitpunkt abgeschlossen. Davon hatte die Hälfte einen Studienabschluss in einem informationstechnischen Fachgebiet, ein Viertel in den Ingenieur- und Naturwissenschaften und ein weiteres Viertel in anderen Studienrichtungen.

Gesamtbewertung

Für 94% aller Befragten war die Teilnahme an der baden-württembergischen Informatica Feminale im Rückblick eine wertvolle oder sehr wertvolle Erfahrung. Ein ebenfalls sehr hoher Prozentsatz, nämlich 83%, beurteilte das Lernen unter Frauen positiv. Eine Teilnehmerin formulierte dies folgendermaßen: *„Ich habe mich immer wohl gefühlt auf der IF. Die Atmosphäre dort war richtig gut. Wenn ich es zeitlich unterbringe, komme ich gerne wieder. Das Rahmenprogramm (Vorträge und Workshops) hat mich auch immer sehr angesprochen."* Die sehr hohe Zustimmung zu diesem monoedukativen Angebot spiegelt sich auch darin wider, dass 83% der Befragten sich vorstellen können, wieder an der Informatica Feminale Baden-Württemberg teilzunehmen.

Nutzen der Fachkenntnisse und Bewertung der Fachkurse

Wie bereits frühere Befragungen ergaben, stellt der Wunsch zum Erwerb informatikrelevanter Fachkenntnisse ein wesentliches Moment der Teilnahmemotivation dar. Der beschriebene positive Gesamteindruck drückt sich auch in der guten Bewertung der Fachkurse aus. Wie Abb.1 verdeutlicht, nutzen zwei Drittel der Befragten die erworbenen Fachkenntnisse häufig oder gelegentlich. Immerhin noch ein Fünftel nutzt sie selten, und nur 10% nutzen die erworbenen Fachkenntnisse nicht. Damit kann gesagt werden, dass der Wissenstransfer von der baden-württembergischen Informatica Feminale in den Studien- und Berufsalltag für die weit überwiegende Anzahl der Teilnehmerinnen gelingt.

Abb. 1: Nutzen der Fachkenntnisse

Von besonderem Interesse war bei dieser Befragung, wie die Inhalte und die Qualität der Fachkurse beurteilt wurden und inwieweit sie den Erwartungen der Teilnehmerinnen entsprachen. Wie Abb. 2 verdeutlicht, wurde die Aktualität der Fachkurse mit 94 % Zustimmung als besonders positiv beurteilt. Von 83% der Befragten wurde das Verhältnis zwischen Lernerfolg und Zeitaufwand als gut eingeschätzt. Ebenfalls 83% Zustimmung erfuhr die Frage nach dem Praxisbezug. Jeweils 80% beurteilten die Kurse als eine wertvolle Ergänzung zum Studienalltag und sprachen ihnen eine hohe fachliche Qualität zu. Diese insgesamt sehr positive Resonanz drückt sich auch darin aus, dass drei Viertel aller Befragten ihre thematischen Erwartungen an die baden-württembergische Informatica Feminale als erfüllt ansahen.

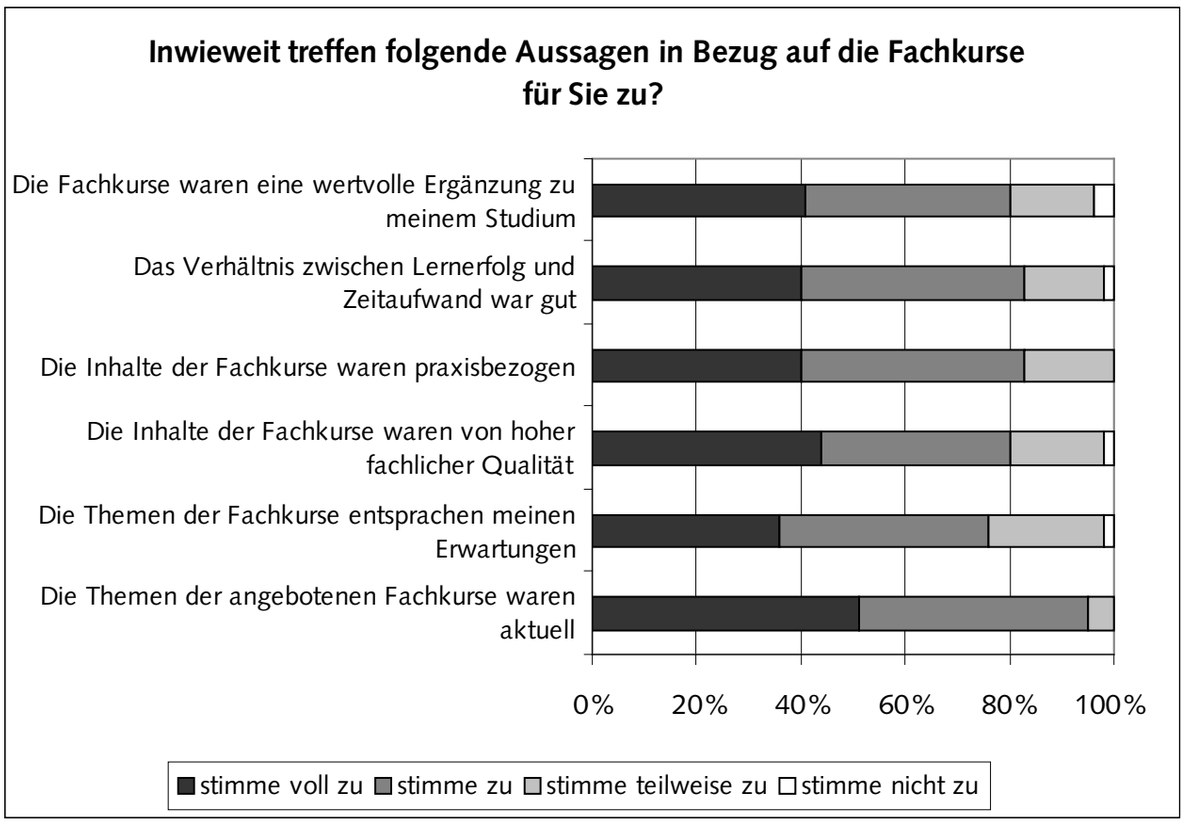


Abb. 2: Bewertung der Fachkurse

Auf die Frage „Was haben Sie aus der Teilnahme/den Teilnahmen an der Informatica Feminale BW in ihren beruflichen oder Studienalltag mitgenommen?“ sollten die Befragten die Bedeutung ihrer Teilnahme an der Sommerhochschule für Beruf und Studium näher erläutern. Die offene Frage erfuhr eine hohe Resonanz, die sich in einer großen Bandbreite unterschiedlicher Aussagen ausdrückt. Wie aus folgender Auswahl der Zitate ersichtlich wird, steht der Erwerb von Fachkenntnissen eindeutig im Vordergrund: *„meine in dem Kurs erworbenen Fachkenntnisse setze ich in meinem Studium um, wo ich meine Programme (software) richtig testen kann“; „für das Studium war die Erfahrung wichtig“; „für das anschließende Masterstudium waren die Kurse sehr wertvoll“; „Interesse am Programmieren steigt“; „Inhalte helfen nach dem Studium weiter“; „der Einblick in verschiedene Themengebiete hat mir geholfen mein Studium in einem größeren Kontext zu sehen“*. Darüber hinaus wurde bei manchen Teilnehmerinnen das Interesse für interdisziplinäre Fragestellungen und Gender-Themen geweckt: *„Kontakte mit frauenspezifischen Themen“* und das Zutrauen in die eigenen Fähigkeiten gestärkt: *„mehr Vertrauen im Umgang mit dem PC“*. Und nicht zuletzt stieg bei manchen Befragten die *„Inspiration“*. Zusammenfassend lässt sich feststellen, dass alle diese Faktoren einen wichtigen Beitrag für den Berufs- und Karriereweg leisten.

Wie aus Abb. 3 ersichtlich wird, trägt das vielfältige Angebot der Sommerhochschule darüber hinaus zum Erwerb wichtiger Schlüsselqualifikationen bei. Circa die Hälfte aller Befragten gab an, nach der Informatica Feminale Baden-Württemberg mehr Spaß im jeweiligen Arbeitsgebiet und wichtige Schlüsselqualifikationen, Soft Skills sowie Selbstbewusstsein erworben zu haben. Immerhin noch mehr als ein Drittel der Befragten ist mutiger geworden und bringt sich stärker in Arbeitsgruppen mit ein. Zusammengefasst kommen diese Erfahrungen in folgender Aussage zum Ausdruck: *„Die wertvollste Erfahrung ist die Zusammenarbeit mit Frauen, ich bin selbstbewusster geworden. Am Ende des Semesters habe ich sogar ein Projekt unserer Studiengruppe geleitet. Vor der Teilnahme an der Informatica Feminale konnte ich mir in dieser Richtung nichts vorstellen.“*

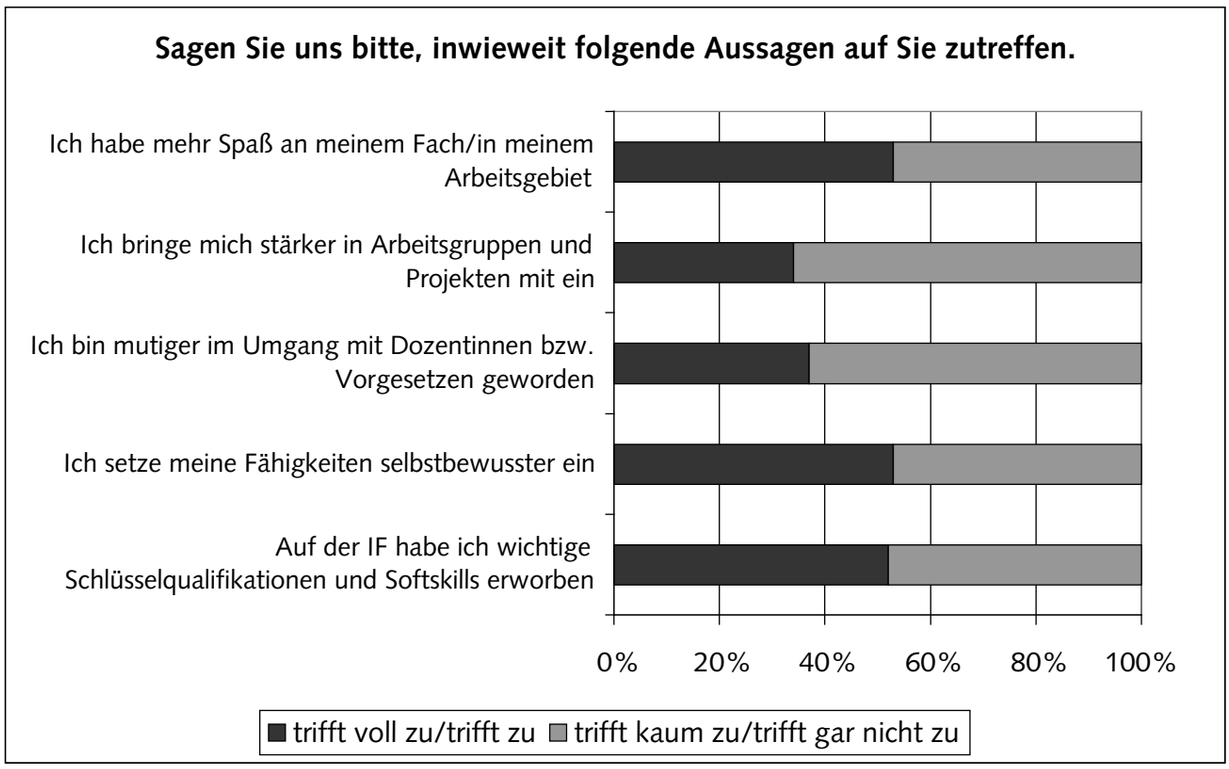


Abb. 3: Bedeutung der erworbenen Schlüsselqualifikationen und Soft Skills für Studium und Beruf:

Netzwerkbildung

Als wichtiges Ziel gehört zum Konzept der Informatica Feminale Baden-Württemberg die Vernetzung der Teilnehmerinnen untereinander. Aus diesem Grunde wurde die Frage gestellt, ob noch Kontakte zu Teilnehmerinnen und Dozentinnen bestehen. Immerhin knapp die Hälfte aller Befragten gab an, Kontakte zu anderen Teilnehmerinnen zu pflegen. Zu den Dozentinnen hatte noch etwa jede sechste Teilnehmerin Kontakt. Diese Ergebnisse verdeutlichen, dass monoedukative Veranstaltungen einen Rahmen bieten, in dem Kontakte geknüpft werden, die nicht nur kurzfristig, sondern längerfristig bestehen.

In diesem Zusammenhang ist auch die Frage interessant, ob zusätzlich zur baden-württembergischen Informatica Feminale weitere monoedukative Veranstaltungen besucht wurden. Die Auswertung ergab, dass ca. ein Viertel der Befragten neben der baden-württembergischen Sommerhochschule die *Informatica Feminale* in *Bremen* und die *Ditact* in *Salzburg* besucht hatte.

Studienabbruch vermeiden

Ein weiteres Ziel der Informatica Feminale ist die Vermeidung von Studienabbrüchen. Auch wenn angesichts der geringen Fallzahlen für diese Frage Repräsentativität nicht in Anspruch genommen werden kann, zeigt die Auswertung doch, dass die baden-württembergische Informatica Feminale in der Lage ist, einen wichtigen Beitrag zur Vermeidung eines möglichen Studienabbruchs zu leisten. Von 74 Befragten, die während der IF studiert hatten, gaben immerhin 24 (35%) an, dass sie schon einmal erwogen hatten, das Studium abzubrechen. Aus dieser Gruppe wiederum wurden 10 Studentinnen, das sind 42 Prozent, durch die IF motiviert weiterzustudieren. Eine Erhöhung der Studienmotivation kommt nicht nur der einzelnen Studentin zu Gute, sondern hat weiter reichende Wirkungen, wie das Zitat einer ehemaligen Teilnehmerin im Titel verdeutlicht: *„Jede Frau, die überlebt in einem technischen Studiengang, macht zwei anderen die Türe auf"*.

Diskussion der offenen Antworten

Auf die Frage nach der Bedeutung der IF-Teilnahme für Beruf und Studienalltag wurden mehr als 80 positive und lobende Aussagen gemacht. Die Zitate hierzu können aus Platzgründen nicht alle wiedergeben werden, jedoch soll an dieser Stelle stellvertretend eine Teilnehmerin zu Wort kommen: *„Für mich war besonders wertvoll, dass ich mein Wissen und meine Fähigkeiten in einem Bereich vertiefen konnte, der an meiner Universität kaum Aufmerksamkeit gewidmet wird. Da dieses Gebiet auch gleichzeitig mein Studienschwerpunkt ist und ich in diesem Umfeld die Diplomarbeit schreibe, hat es mir recht viel gebracht."* In vielen Zitaten wurde hervorgehoben, dass die Vernetzung mit anderen Frauen aus Naturwissenschaft und Technik den Teilnehmerinnen der Sommerhochschule viel bedeutet. Folgendes Zitat macht dies deutlich: „*Neben dem erworbenem Fachwissen insbesondere ein Netzwerk und die Zuversicht, nicht mehr als Frau in der Informatik eine ‚Exotin' zu sein."*

Neben den Fachkursen machte das vielfältige Angebot, z.B. die Ringvorlesungen und die Monoedukation das *Besondere* der Sommerhochschule aus: *„Das Lernen unter Frauen war eine sehr intensive, neue Erfahrung. Sehr interessant fand ich auch die Ringvorlesungen, die Mut dazu machten, sich auch einmal in andere Bereiche hineinzuwagen. Ich zehre auch heute noch*

von der Veranstaltung. Immer wenn ich daran zurückdenke, geht's mir gut!" Neben der überwältigenden Zustimmung übten vier Teilnehmerinnen Kritik. Zwei kritisierten, dass ihre Erwartungen und das Angebot nicht zusammenpassten, weil der Kurs nicht dem erwarteten Schwierigkeitsgrad entsprach. Eine Teilnehmerin fand, dass Frauen generell versuchten das Lerntempo niedrig zu halten, damit alle den Stoff verstünden. Dies stünde im Widerspruch zu einer leistungsorientierten Gesellschaft. Auf der anderen Seite äußerte sich eine andere Teilnehmerin zur selben Thematik dahingehend, dass für sie der unterschiedliche Wissensstand sehr bereichernd gewesen sei. Eine einzige Teilnehmerin fühlte sich ungerechtfertigt schlecht benotet.

Viele Teilnehmerinnen sahen einen positiven Zusammenhang zwischen ihrer Teilnahme an der baden-württembergischen Informatica Feminale und ihrem Berufseinstieg bzw. ihrer Karriere. Erwähnt wurde in diesem Zusammenhang auch immer wieder, dass die Dozentinnen wichtige Vorbilder auf dem eigenen beruflichen Weg waren. Folgendes Zitat stellt die Vorbildfunktion der Dozentinnen deutlich heraus: *„Die Podiumsdiskussion bei der IF 2005 über Frauen mit Kind und Karriere hat mir sehr geholfen, andere Frauen kennen zu lernen, die in der selben Situation mit Kind sind. Sie waren eine Art Vorbild und Ermutigung, da sie es trotz Kind geschafft haben, mit guter Organisation, Mut und Beharrlichkeit Karriere zu machen. Es war wichtig, dass sich die Firmen (...) auf der IF persönlich vorgestellt haben. So kann man sich besser ein Bild machen und die Firma als Bewerber in den engeren Kreis der Firmen einbeziehen."* Die Vorbildfunktion der Dozentinnen und Referentinnen kann durchaus eine langfristige Bestärkung der eigenen Motivation zur Folge haben und sich positiv im Berufsleben auswirken: *„Besonders gefallen hat mir der Erfahrungsaustausch und die Hilfe der Teilnehmerinnen untereinander. Auch fand ich die Vorträge immer sehr spannend, bei denen Frauen aus der Praxis berichtet haben. Ich erinnere mich noch an eine Vortragende, die bei Audi gearbeitet hat und dort sehr erfolgreich war. Heute arbeite ich bei S. und muss manchmal noch an diesen Vortrag denken, der sehr viel Selbstbewusstsein und Kraft ausgestrahlt hat (gerade wenn ich einem Meeting mit 20 Männern sitze oder einen Vortrag vor 50 Systemtestern halten muss). Das gibt mir dann auch gleich noch etwas mehr Power und ich ziehe mein Ding durch."*

Unter „Sonstiges" wurden nochmals viele zuvor erwähnte Punkte aufgegriffen. Ganz überwiegend wurde Lob geäußert und der Wunsch nach einer Verbesserung des regulären Studiums an der eigenen Hochschule: *„Die Teilnahme an der Informatica Feminale hat mir sehr viel Spaß gemacht. Es war viel interessanter, als ich erwartet habe. Wenn auch die Vorlesungen an der FH oder Uni genauso gestaltet werden, wäre es viel spannender und effizienter."* Im Hinblick auf zukünftige Wünsche für die Informatica Feminale wurde nochmals die Vielfältigkeit der Angebote als Alleinstellungsmerkmal hervorgehoben. So äußerten viele der Befragten den Wunsch, die gemischte Angebotsstruktur der baden-württembergischen Informatica Feminale zukünftig unbedingt beizubehalten und wenn möglich sogar noch zu erweitern. Neben speziellen Fachkursen wünschten sich die Befragten auch Angebote zu Soft Skills, Coaching, Statistikprogrammen, Frauenpolitik und weiteren interdisziplinären Themenstellungen.

Fazit

Die Ergebnisse der Nachbefragung zeigen, dass der Besuch der Informatica Feminale Baden-Württemberg für die Teilnehmerinnen langfristig von Nutzen ist. Die Teilnehmerinnen profitierten sowohl vom fachbezogenen Angebot als auch von den Ringvorlesungen, Workshops, und Vorträgen sowie dem Rahmenprogramm, dessen Bedeutung für die Vernetzung der Teilnehmerinnen und Dozentinnen nicht hoch genug bewertet werden kann. Als monoedukative Veranstaltung trägt die baden-württembergische Sommerhochschule darüber hinaus dazu

Die Autorinnen

Kordula Kugele M.A. studierte soziale Verhaltenswissenschaften, Soziologie und Erziehungswissenschaft. Als wissenschaftliche Mitarbeiterin war sie in 2006 beim Netzwerk Frauen.Innovation.Technik beschäftigt und wechselte im Oktober 2006 in das EU Projekt ESGI (European Study on Gender Aspects of Inventions- Statistical Survey and Analysis of Gender Impact on Inventions) an der Hochschule Furtwangen. Frau Kugele hat zwei erwachsene Kinder und eine 13-jährige Tochter. Kontakt: kug@hs-furtwangen.de

Martina von Gehlen ist seit 2001 wissenschaftliche Mitarbeiterin im Projekt Netzwerk Frauen.Innovation.Technik. Sie ist verantwortlich für die Konzeption, Durchführung und wissenschaftliche Begleitung der jährlichen Sommerhochschule. Martina von Gehlen studierte Geoökologie an der Universität Bayreuth und war 5 Jahre in der Umweltberatung tätig, wo sie u.a. Lehrgänge und Seminare für Umweltbeauftragte organisierte. Sie hat einen Sohn. Kontakt: vge@hs-furtwangen.de

Kontakt Netzwerk Frauen.Innovation.Technik (F.I.T) Baden-WürttembergHochschule Furtwangen, Jakob-Kienzle-Straße 17, 78054 Villingen-Schwenningen

www.netzwerk-fit.de

bei, einen möglichen Studienabbruch zu vermeiden und die Motivation für ein informations-technisches oder naturwissenschaftliches Studium zu erhalten oder zu steigern.

Ausblick

Das Konzept der Informatica Feminale Baden-Württemberg ist ein Erfolgsmodell, das sich über Jahre hinweg bewährt hat. Die Sommerhochschule, deren Konzept von der Bremer Informatica Feminale übernommen wurde, hat in den sechs Jahren des Bestehens ein eigenes Profil entwickelt und als monoedukative Sommerhochschule mittlerweile einen festen Platz bei den Studentinnen in technischen Studiengängen im Süden Deutschlands eingenommen.

Literatur

Heublein, Ulrich; Schmelzer, Robert; Sommer, Dieter (2005): Studienabbruchstudie 2005. Hochschul-Informations-System (HIS) Kurz-Information. Hannover

Dietrich Meyer-Ebrecht

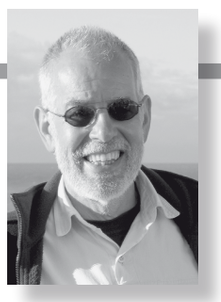
Versteckte Computer und ihr unerwarteter Eigensinn

Marco Polo — der Name verheißt Abenteuer. Sofort verlieben wir uns in Erwartung vieler schöner Reiseabenteuer in dieses kleine, feine Campmobil der Marke mit dem Stern, ausgestattet mit allem Komfort, den Stadtmenschen auch auf fernen Reisen und in romantischer Natur nicht missen möchten. Nicht zu reden von den vielen unauffälligen elektronischen Heinzelmännchen für nützliche und nicht immer notwendige Funktionen: Eine kaum überschaubare Anzahl von Bordcomputern, in vornehmer Zurückhaltung Steuergeräte genannt, verhindern das Blockieren der Bremsen, stabilisieren die Fahreigenschaften, optimieren das Triebwerk, kurbeln Fenster rauf und runter, bringen die Sitze in die gewünschte Position oder lassen die Innenbeleuchtung augensympathisch auf– und abdimmen. Und hin und wieder erhalten wir auch Software–Updates für einzelne dieser Steuergeräte. Die begleitet dann beispielsweise so ein Kommentar: „Die Sitzbank könnte vielleicht nicht mehr aus der Liegestellung hochkommen." Richtig, ist bereits passiert, und da habe ich einfach den Stecker gezogen und wieder gesteckt. – „Sehen Sie, da haben Sie die Software neu initiiert." Ach, ich dachte, das wäre einfach nur ein Schalter. „Aber, aber, heute doch nicht mehr ..."

Beruhigend, wie wir durch so einfache Maßnahmen auch im Auto mit der Technik immer auf der Höhe der (Nach–) Entwicklung bleiben. Wie viel leichter lebt es sich doch heute für die Entwickler dieser Komponenten. Sie müssen die allerletzten, am mühsamsten aufzuspürenden Fehlerquellen nicht mehr sofort ausmerzen. Es ist nicht mehr das halbe Fahrwerk auseinander zu bauen, wenn etwa ein sicherheitsproblematisches Lager ausgetauscht werden muss. Servicecomputer kurz andocken und fertig.

Das wahre Abenteuer begann eines Morgens in der Garage. Der Druck auf den Schlüssel — passt dieses Wort eigentlich noch für den Handschmeichler, der die Türen auf wunderbare Weise bereits auf zehn Schritte Entfernung entriegelt? — wurde auch nach mehrfacher und nach*drücklicher* Wiederholung nicht durch freundliches Blinken und das ersehnte schmatzend–einladende Geräusch der Zentralverriegelung erwidert. Ratlos steht der Zeitdruckgeplagte vor verschlossenen Türen. Hätte ich mir doch vorher das 500 (!) Seiten starke Manual schon einmal durchgesehen, insbesondere das Kapitel „Was tun, wenn …". Im Handschuhfach liegt es griffbereit — aber die Türen bleiben verschlossen. Der Anruf in der Werkstatt bringt Rat: Es gebe da so einen (altmodisch–mechanischen) Notschlüssel ... Der ist schon nach Kurzem unter Abbrechen eines Fingernagels aus dem Plastikteil alias Autoschlüssel herausgepult, und er passt in ein (ebenfalls altmodisch–mechanisches) Schlüsselloch in der Beifahrertür. Leider ist der Marco Polo nur eine Handbreit von der Garagenwand geparkt (er ist halt ein bisschen breiter). Aber irgendwie lässt sich dieses Problem mit einigem akrobatischen Geschick lösen. Was endlich zu der Entdeckung führt, dass die Starterbatterie leer ist, so leer, dass sich nicht einmal der Schlüssel im Zündschloss drehen lässt. Wieso eigentlich, weder Licht noch irgendein anderer Verbraucher waren in der Nacht eingeschaltet?

Also den netten Nachbarn um Starthilfe bitten. Immerhin, das gelingt ohne Umstände, und schon produziert der Diesel wieder munter schnurrend seine Partikel. Dann aber irritieren merkwür-



Dietrich Meyer-Ebrecht

Dietrich Meyer-Ebrecht war von 1984 bis 2004 Inhaber des Lehrstuhles für Messtechnik und Bildverarbeitung an der RWTH Aachen. Davor war er Forschungsgruppenleiter im Philips Forschungslaboratorium Hamburg. Als Emeritus ist er auch weiterhin tätig auf seinem Forschungsschwerpunkt *Computer Vision,* angewendet speziell in der Medizin.

dige Ungereimtheiten auf den Anzeigen des digitalen Multifunktions-Instruments, und die elektrischen Fensterheber wollen auch nicht mehr. Nun gut, ich muss sowie in die Werkstatt, denn die Ursache der spontanen Batterie-Entladung muss gefunden werden. Ein solches Ereignis könnte das Erwachen nach einer lauschigen Nacht an einem einsamen schwedischen Waldsee zu einem wahren Abenteuer machen.

Die Diagnose gelingt dank Diagnosecomputer schnell: Die Batterie habe die Tiefentladung nicht heil überstanden, und der Fremdstartvorgang habe drei der Bordcomputer, Verzeihung: Steuergeräte, zerschossen — „nun ja, da können schon mal Spannungsspitzen auftreten". Wie das? Haben die Entwickler vergessen, die zugegebenerweise empfindliche Computerelektronik gegen ein paar Volt Überspannung zu schützen? Oder mussten auch hier ein paar Cent für die zusätzlich erforderlichen Bauelemente gespart werden? Langwieriger gestaltet sich die Ursachenforschung. Auch nach mehreren Tagen eifrigen Messens und Beobachtens kommt nur die Vermutung auf, dass die Starterbatterie wohl schon vorher defekt gewesen sein musste. Mit neuen Steuergeräten, frischer Starterbatterie und der tröstlichen Bemerkung, dass da wohl mehrere Umstände ungünstig verkettet waren, nehme ich das Gefährt wieder in seinen täglichen Gebrauch.

Vorsichtshalber lasse ich ab jetzt einen Respektabstand zwischen Garagenwand und Beifahrertür, was sich bereits nach kaum zwei Wochen auszahlt: Batterie über Nacht wieder leer! Statt Starthilfe diese Mal eine geladene Ersatzbatterie geordert. Wieder sorgsames Durchmessen und langwierige Beobachtung in der Werkstatt. Diesmal sei die Zweitbatterie defekt — aber keine Erklärung der nächtlichen Entladung der Starterbatterie. Es könne schon mal vorkommen, dass eines der Steuergeräte spontan erwache und Gebläse, Scheinwerfer oder ähnliches einschalte, aber welches und wann? Man könne ja in diese viele Computertechnik nicht mehr hineinschauen. Ja, gibt es denn keine Hotline beim Hersteller? Schon, aber die könnten auch oft nicht weiterhelfen, das „hätten sie noch nie gehabt, das dürfte eigentlich nicht passieren…". Nach einer Woche würden die Hotliner wieder in der Werkstatt anrufen, um sich zu erkundigen, wie man den Fehler gelöst hätte.

Um mich in meiner Besorgnis etwas aufzuheitern, erzählt mir der Mechaniker noch die Geschichte von dem Fahrer der Nobellimousine, die sich mitten in fremder Stadt nicht mehr starten lassen wollte. Die herbeigerufene Pannenhilfe konstatiert ratlos, dass es wohl ein Computerproblem sein müsse und damit wisse man nicht Bescheid. Den Experten bekommt man immerhin schon nach einigen Runden in den Warteschleifen der Hotline zu fassen. Er lässt sich das Problem kurz schildern und empfiehlt dann mit nicht zu verbergendem Westcoast-Akzent, die Fenster herunterzulassen (...?!) — ja, jetzt wieder hochfahren und ein neuer Startversuch: Der Motor startet unerwartet! Wie denn das? fragt der Fahrer verblüfft „Well, das machen wir immer so: Windows runterfahren und wieder hochfahren, dann läuft wieder alles …"

Das klamme Gefühl, mit dem ich mein Gefährt von jetzt an abends abstelle, erweist sich auch schon nach wenigen weiteren Wochen als Vorahnung: Zum dritten Mal streikt die Batterie. Diesmal hat die Werkstatt Erfolg. Sie ortet das problembringende Steuergerät. Ein Austauschgerät ist umgehend beschafft und eingebaut, und in gehobener Stimmung fahre ich nach Hause. Halt — was war denn nun eigentlich der Fehler? Wie war das noch einmal mit den Unwägbarkeiten von Softwarefehlern? Ich glaube, ich warte noch, bis ich mich auf den Komfort computerüberwachter Abstandhaltung und automatische Spurhaltung einlasse. Wenn ich an die Zeiten zurückdenke, als ich meine Pannen unterwegs mit richtigem Werk–Zeug beheben konnte ...

Barbara Wiesner

Versteckte Informationen in elektronischen Dokumenten

Ein studentisches Projekt im Fachbereich Informatik und Medien an der Fachhochschule Brandenburg

Versteckte Daten sind sowohl Metadaten wie Autor, Titel, Stichwörter, Erstellungsdatum als auch versteckte Informationen wie Kommentare, Bearbeitungshistorie und dergleichen mehr. Mit dem Aufdecken dieser versteckten Daten hat sich eine Gruppe Studierender an der Fachhochschule Brandenburg im Rahmen eines studentischen Projektes unter der Leitung von Prof. Dr. Barbara Wiesner beschäftigt.

Die Idee zu diesem Projekt kam durch die Lektüre des Aufsatzes von Byers [4]. Byers untersuchte 100.000 MS Word Dokumente, die er nach einem Zufallsprinzip aus dem Web ausgewählt und herunter geladen hatte. In allen fand er versteckte Texte. Die meisten waren uninteressant, aber einige davon waren durchaus als sehr kritisch einzustufen. Versteckte Daten findet man nicht nur in Microsoft Word Dokumenten. Insofern befassten sich die Studierenden in diesem Projekt auch mit anderen Formaten.

Microsoft Word Dokumente

Den Verfassern von Microsoft-Office-Dokumenten ist oftmals nicht bewusst, welche Vielzahl an Informationen ein Dokument über sie verrät. Einen sehr guten Überblick, welche versteckten Daten man in Microsoft Office Dokumenten finden kann und welche Risiken damit verbunden sind, findet man in der Bitform Fallstudie [17]. Wir haben diese Informationen in einer Tabelle „Risiko von Metadaten und versteckten Informationen in Microsoft Office" in deutscher Sprache zusammengestellt, die wir bei Interesse gerne zur Verfügung stellen.

Auch Microsoft ist sich der Thematik bewusst und stellt auf seiner Homepage Anleitungen zum Schutz von persönlichen Daten für den Office-Nutzer zur Verfügung [15]. Allerdings sind diese Hinweise nicht ausreichend, um alle versteckten Informationen zu entfernen. Wie Microsoft selbst zugibt, sind hiermit nur „persönliche Daten" zu entfernen. Dazu zählen lediglich einige Dokumenteigenschaften wie Autor, E-Mail-Eigenschaften und Firma.

Die folgenden Programme dienen zum Anzeigen von verborgenen Informationen in Microsoft-Word-Dokumenten. Sie wurden getestet und mit einander verglichen.

- Bitform Discover [2]
- DocScrubber [6]
- WorkshareProtect [21]

Die Tests wurden an einem Dokument durchgeführt, das ein Kommilitone aus dem Internet herunter geladen hatte. Die untenstehende Tabelle 1 zeigt die Anzahl der angezeigten Informationen pro Tool.

Bitform Discover analysiert Informationen mit höchsten Risikostufen wie Bearbeitungshistorie und Outlook-Eigenschaften. Des Weiteren zeigt Bitform mittlere Risikoelemente wie Druckerinformationen und Benutzernamen an. Zusätzlich präsentiert dieses Tool Dokumenteigenschaften mit geringem Risiko wie Titel, Erzeugungsdatum, Druckdatum und Speicherdatum.

WorkshareProtect zeigt die meisten Veränderungen in der Bearbeitungshistorie (hohes Risiko) an, jedoch fehlen hier die ausführlichen Outlook-Informationen. Das Tool vernachlässigt z.B. Name, E-Mailadresse sowie Subject der E-Mail. Aus dem mittleren Risikobereich analysiert WorkshareProtect den Benutzernamen, aber nicht die Druckerinformationen. Auch im Bereich des geringen Risikos gibt es wesentlich weniger erkannte Details als bei Bitform Discover.

Bei DocScrubber fehlen gänzlich die Angaben zur Bearbeitungshistorie, E-Mail-Eigenschaften und Druckerinformationen. Aus dem mittleren Risikobereich analysiert es lediglich den Benutzernamen. DocScrubber entdeckt im geringen Risikobereich ähnlich viele versteckte Daten wie WorkshareProtect. Es werden jedoch weitaus mehr statistische Eigenschaften als bei WorkshareProtect angezeigt, leider aber keine zusammenfassenden Eigenschaften.

Außer mit derartigen Tools kann man sich mit beliebigen Hex-Editoren beispielsweise WinHex [19] verborgene Informationen anzeigen lassen.

Im Folgenden werden drei Tools vorgestellt, mit denen verborgene Daten wieder entfernt werden können. Diese wurden getestet und miteinander verglichen. Dabei wurde dasselbe Dokument verwendet wie zuvor.

- DocScrubber [6]
- ezClean [8]
- Office-Add-In [13]

Die Abbildungen 1 bis 3 zeigen das jeweilige Resultat der Tests.

Wenn man sich die Auswertungen hinsichtlich der Anzahl der entfernten Daten anschaut, kann man den Eindruck gewinnen, dass aus den drei untersuchten Programmen DocScrubber das Beste ist. Beim genaueren Hinsehen fällt allerdings auf, dass die entfernten Informationen verschiedene Risikoklassen besitzen. Analysiert man nach diesem Aspekt, so ist das Office-Add-In das beste Tool, da es die hoch riskanten sowie die mittel riskanten Informationen vollständig entfernt bzw. durch allgemeine

Element	Risiko	Anzahl Bitform	Anzahl Workshare	Anzahl DocScrubber
Bearbeitungshistorie		25	56	0
Outlook Eigenschaften		4	0	0
Druckerinformationen		6	0	0
Benutzername		1	1	1
Dateieigenschaften Statistik		19	5	10
Dateieigenschaften Zusammenfassung		10	4	0
Dateieigenschaften Inhalt		1	1	1

Tab. 1: Anzahl der angezeigten Informationen pro Tool

Bezeichnungen ersetzt. Ebenso positiv ist, dass es nur wenige, gering riskante Informationen im Dokument zurück lässt.

DocScrubber beseitigt zwar viele Informationen mit geringem Risiko wie Erzeugungsdatum, letztes Druckdatum, letztes Speicherdatum und letzter Verfasser, hinterlässt aber alle vom Verfasser gemachten Änderungen und E-Mail-Informationen, also viele hoch riskanten Informationen.

ezClean entfernt zwar diese, löscht aber keine mit mittlerem Risiko. Die Anzahl der entfernten Informationen geringen Risikos liegt zwischen denen der beiden anderen Tools.

Das Tool „Bitform Secure SDK“ von Bitform Technology Inc. zum Entfernen versteckter Daten, also das Werkzeug, das die von „Bitform Discover“ entdeckten Daten entfernt, stand für Testzwecke leider nicht zur Verfügung. Es wird inzwischen von Stellent Inc. unter dem Namen „Outside In Clean Content SDK“ vertrieben.

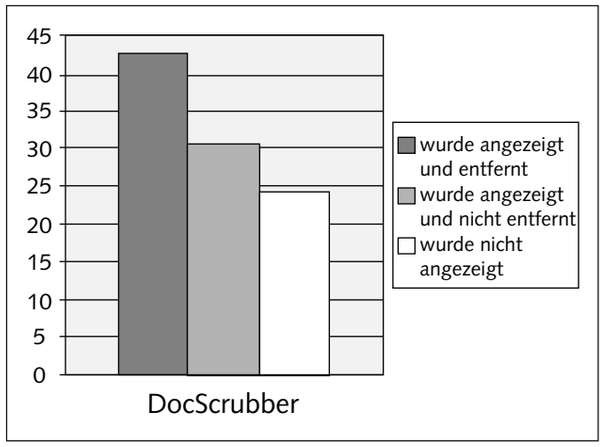


Abb. 1: Testergebnis für DocScrubber

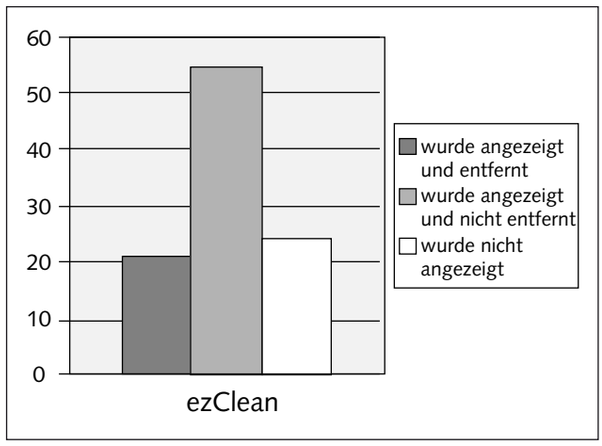


Abb. 2: Testergebnis für ezClean

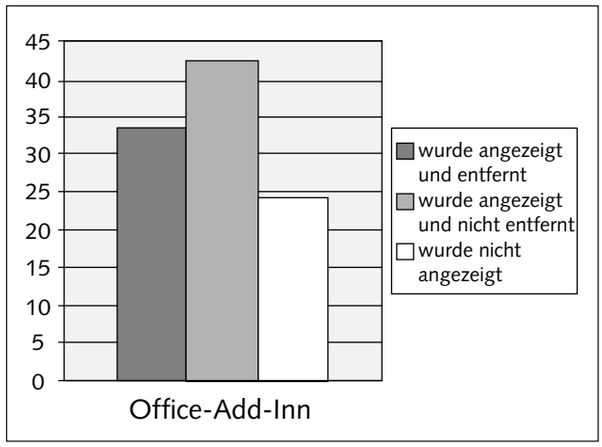


Abb. 3: Testergebnis für das Office-Add-In

Dokumente im Portable Document Format (PDF)

PDF ist ein beliebtes Format zur Weitergabe von nicht mehr änderbaren Dokumenten. Es ist aus Postscript hervorgegangen und wird zunehmend auch im professionellen Druckgewerbe eingesetzt.

Aufbau von PDF-Dateien

Eine PDF-Datei besteht aus einer Sammlung von Objekten. Diese Objekte sind nummeriert und werden durch das Paar obj … endobj geklammert. Sie repräsentieren dabei die einzelnen Elemente des Dokumentes. Die Anordnung der Objekte im Dokument wird dabei in der Querverweistabelle beschrieben. Sie enthält eine Liste der Objekte mit ihren jeweiligen Startpositionen innerhalb der Datei [10].

In PDF-Dokumenten können Metadaten und Versionen gefunden werden. Metadaten sind zum einen die „normalen“ Informationen wie Autor, Titel, Verfasser, Erstelldatum. Außerdem können mithilfe der Extensible Metadata Platform (XMP) individuelle Metadaten hinzugefügt werden. Acrobat Professional zeigt nicht alle Metadaten, die in einem PDF-Dokument gespeichert sind. Öffnet man ein unverschlüsseltes PDF-Dokument mit einem Text-Editor, können alle Metadaten im Klartext ausgelesen werden. So findet man zum Beispiel die XMP-Metadaten unter dem Tag <x:xmpmeta> ... </x:xmpmeta>. Man kann so an Informationen gelangen, die sonst verborgen geblieben wären.

Wird ein PDF-Dokument mit einer digitalen Unterschrift versehen und im nachhinein verändert, so lässt es Acrobat zu, zwischen den einzelnen Versionen umzuschalten. Dies geht nur im Acrobat Professional über die Reiter „Unterschrift auswählen … Unterschriebene Version anzeigen“; der Acrobat Reader bietet diese Funktion nicht. Ist ein PDF-Dokument nicht unterschrieben, bleibt einem die Umschaltung zwischen den einzelnen Versionen verwehrt. Die Änderungen sind aber dennoch abgespeichert, da Acrobat beim Speichern lediglich ein Update an die bereits vorhandene Datei anhängt [10]. Gelingt es, dieses

Update zu entfernen, was möglich sein sollte, erhält man wieder die Vorgängerversion. Erst bei Datei, Speichern unter... bereinigt Acrobat sämtliche Dateistrukturen und schreibt eine komplett neue Datei ohne Updates.

Fehler bei der Konvertierung von Word-Dokumenten nach PDF

Bei der Konvertierung von Word-Dokumenten nach PDF können durch den Nutzer Fehler gemacht werden. Im Folgenden werden einige davon vorgestellt.

Durch das Gleichsetzen der Hintergrundfarbe mit der Textfarbe eines beliebigen Absatzes (Black Text Methode) kann in Word ein Textauszug unlesbar gemacht werden. Nach der Konvertierung des Word-Dokumentes nach PDF kann der Text jedoch wieder sichtbar gemacht werden. Dazu kopiert man zunächst den entsprechenden Textauszug und fügt ihn in ein neues, leeres Word-Dokument ein. Nun wird der Text markiert und die Hintergrundfarbe zurückgesetzt. Der verdeckte Text ist nun wieder lesbar.

Bei der White Text Methode wird umgekehrt die Schriftfarbe an den Dokumenthintergrund angepasst. Der Vorteil gegenüber der Black Text Methode ist, dass dies für den Nutzer nicht sofort erkennbar ist. Er hält dies eher für einen absichtlichen Absatz als für einen versteckten Text. Die Rückführung zum Klartext ist wie bei der Black Text Methode.

Objekte wie Grafiken, Bilder und ähnliche kann man in Office Dokumenten verstecken, indem man sie mit einem entsprechenden großen leeren Bild überlagert. Dadurch sind sie nicht mehr sichtbar. In der entsprechenden PDF-Datei ist das Bild dann nicht zu sehen. Der Acrobat Professional bietet die Möglichkeit „Alle Bilder exportieren". Damit werden nun alle enthaltenen Bilder (JPEG, TIFF, GIF,...) aus dem PDF-Dokument extrahiert und in einem Ordner gespeichert, wo sie dann eingesehen werden können.

Die NSA hat eine Anleitung ins Netz gestellt [11], wie man Word-Dokumente unter Beseitigung aller Metadaten nach PDF konvertieren kann ohne dabei vertrauliche Informationen zu übernehmen. Lediglich die verschiedenen Versionsstände werden weiterhin gespeichert. Richtet man sich nach dieser Anleitung, vermeidet man mögliche Fehlerquellen, die sich in der Vergangenheit als durchaus brisant herausgestellt haben.

Dokumente im Rich Text Format (RTF)

RTF [20] wurde 1987 von Microsoft eingeführt. Sein Zweck war es, den Austausch von Textdokumenten zwischen Textverarbeitungsprogrammen verschiedener Hersteller zu ermöglichen. Das Format ist proprietär, aber die Spezifikation wurde von Anfang an von Microsoft offen gelegt, um anderen Herstellern die Implementierung zu ermöglichen.

Das RTF-Format wird gemeinhin als sicher eingestuft, weil in diesem Format keine Makros abgespeichert werden und damit keine Makroviren verbreitet werden können, und weil seine Spezifikation offen gelegt ist. Es wird deshalb oft für die Veröffentlichung und den Austausch von elektronischen Dokumenten empfohlen [16]. Es ist weltweit eines der am meisten eingesetzten Formate zur Verbreitung von Dokumenten. So listet Google aktuell knapp 600.000 RTF-Dokumente allein in der .com-Domain.

Technische Eigenschaften und versteckte Informationen

Viele offene Dokumentformate speichern die Daten in einer XML-Struktur, also in einer Markup-Sprache. RTF-Dateien sind prinzipiell ähnlich aufgebaut, benutzen jedoch eine geringfügig andere Notation als XML. So sind die Funktionen der RTF-Tags nicht immer klar zu erkennen, vor allem, da diese teilweise dynamisch erzeugt werden. Die Textinformationen sind dennoch in Klartext lesbar.

An Metadaten enthalten die RTF-Dokumente zunächst die üblichen, d.h. Informationen über den Benutzer und über das Dokument selbst. RTF kann zusätzlich die Bearbeitungshistorie speichern. Die Option der Änderungsnachverfolgung kann insofern kritisch sein, da viele Dokumente für die Veröffentlichung, zum Beispiel im Internet, aus bereits vorhandenen Papieren erstellt werden, in denen nicht für die Öffentlichkeit bestimmte Informationen einfach gelöscht werden. Bei eingeschalteter Änderungsnachverfolgung werden diese Daten dennoch im Dokument gespeichert, meist ohne Wissen des Anwenders. Diese Änderungen sind im RTF sogar im Klartext im Dokumenten-Quellcode lesbar.

Auch bei RTF-Dokumenten gibt es die Möglichkeit Text einfach mit nicht transparenten Bildern zu überdecken, um zum Beispiel Namen zu „schwärzen". Im RTF wird der darunter liegende Text immer mit abgespeichert und kann somit leicht wieder sichtbar gemacht werden.

Analyse von RTF-Dokumenten aus dem Internet

Einen Großteil der praktischen Arbeit während des Projekts nahm die Durchführung eines Feldversuchs ein. Vorlage und Ideengeber dafür war der Aufsatz von Simon Byers über potenzielle Schwachstellen in Dokumentformaten. Diesen Versuch wollten wir mit RTF-Dokumenten wiederholen. Dazu wurde die Technik ausgenutzt, gelöschten Text mit dem „\deleted"-Tag zu markieren. Die Durchführung des Versuchs bestand aus mehreren Phasen:

1. **Akquirierung der Dokumenten-Links:** Hierzu wurde bei Google nach RTF-Dokumenten gesucht und die Links dann gespeichert. Um die Links für die weitere Verarbeitung speichern zu können, musste der Zugriff auf die Suchmaschine über eine von Google bereitgestellte API erfolgen. Aufgrund der Eigenheiten der Google-Engine kann man nur in bestimmten Domains nach Dokumenten suchen, ohne Einschränkungen durch Suchwörter zu machen. Die Wahl fiel dabei vor allem auf sicherheitskritische Domains, unter anderem .gov .mil .navy.mil .usaf.mil sowie die Militärdomains Großbritannien, Japans, China, Russlands und Frankreich sowie die Domain der deutschen Bundesregierung. Insgesamt konnten fast 12.000 Links gesammelt werden.

2. **Download der Dokumente:** Hierzu wurde ein Tool erstellt, welches die in der ersten Phase gespeicherten Links auswertete und die eigentlichen RTF-Dokumente herunter lud. Diese Phase war technisch die einfachste, dauerte jedoch Aufgrund von Serverfehlern und ähnlichem am längsten. Knapp 85% der Links waren gültig, und so konnten fast 10.000 Dateien mit einem Gesamtvolumen von 1,2 GByte herunter geladen werden.

3. **Parsen der Dokumente nach versteckten Informationen:** Hierzu wurde ein Programm geschrieben, welches die Dokumente nach \deleted-Tags durchsuchte und den eingebetteten Text in eine CSV-Datei speicherte.

4. **Auswerten der erhaltenen Informationen:** Zuletzt wurde die CSV-Ergebnisdatei ausgewertet. Das Format hätte eine genaue statistische Auswertung erlaubt, welche jedoch nur mit einem größeren Versuchsumfang sinnvoll gewesen wäre.

Die Auswertung der CSV-Ergebnis-Datei war sicherlich der spannendste Moment des Projekts. Nach anfänglicher Skepsis, eventuell keine versteckten Informationen zu finden, was immerhin als Ergebnis bedeutet hätte, dass RTF trotz theoretischer Schwachstellen generell sicher ist oder sicher gehandhabt wird, wurden wir schließlich nach Durchlauf aller Dateien doch fündig. In insgesamt 120 Dateien wurde gelöschter Text gefunden. Das sind bei 10.000 untersuchten Dateien immerhin 1,2%. Interessanter war allerdings die Tatsache, dass in 50% der Dateien mit versteckten Informationen diese in nicht unerheblicher Menge vorhanden waren. So konnten aus sicherheitskritischen Dokumenten aus Militär-Domains Adressen und Namen gelesen werden, welche nicht für die Veröffentlichung bestimmt waren. Aufgrund des Zeitmangels war eine umfassendere Analyse leider nicht möglich, dennoch konnten wir aufzeigen, dass RTF nicht zu 100% sicher ist bzw. nicht immer sicher gehandhabt wird.

Dokumente im Open Dokument Format (ODF)

ODF [14] ist ein XML-basiertes Dateiformat zur Speicherung und zum Austausch von Dokumenten. Es wurde zur generellen Verwendung durch Programme eines Office-Paketes wie Textverarbeitung und Tabellenkalkulation entwickelt. Der Umgang mit Diagrammen und Präsentationen ist ebenfalls möglich. Dabei ist es nicht auf ein bestimmtes Office-Paket beschränkt, sondern wurde als offener Standard ausgelegt, der die Nutzung durch beliebige Office-Pakete ermöglicht.

Technischer Aufbau und versteckte Informationen

Eine ODF-Datei ist in der Regel eine Ansammlung von mehreren Dateien und Ordnern, die jeweils bestimmte Aufgaben übernehmen und nach dem ZIP-Standard komprimiert werden. Überwiegend sind das XML-Dateien. Der Einsatz von XML erleichtert die Verarbeitung und Klassifizierung der enthaltenen Informationen. Dadurch wird eine strikte Trennung von Inhalt, Gestaltung und Metadaten erreicht. Es besteht die Möglichkeit, einzelne Dateien innerhalb des Archivs zu bearbeiten.

Auch im ODF sind Informationen, die bei der Erstellung des Dokumentes anfallen, Bestandteil des Dokumentenformates. Diese sind nicht direkt im Text sichtbar. Besonders problematisch sind Daten, die automatisch gespeichert werden, aber auch bei der optionalen Speicherung kann durch unsachgemäße Handhabung viel Schaden hervorgerufen werden. Auf welche Eigenschaften des Open-Document-Formates man dabei achten sollte, wird im Folgenden näher erläutert.

Metadaten werden in der Datei „meta.xml“ gespeichert. OpenOffice.org stellt diese Metadaten innerhalb der Dokumenten-Eigenschaften dar. Diese sind über das „Datei“-Menü zugänglich. Unter „Allgemein“ finden sich Information über das Dokument und seinen Herstellungsprozess. Diese lassen sich dort auch auf ihre Anfangswerte zurücksetzen. Besondere Beachtung verdient die Einstellung „Benutzerdaten verwenden“. Sie erlaubt es dem Nutzer zu entscheiden, ob für die Erstellung des Dokuments und für weitere Änderungen ein Benutzername mitgespeichert wird. Dabei wird jedoch eine eventuell eingeschaltete Änderungsaufzeichnung nicht berücksichtigt. Diese speichert unabhängig die jeweiligen Urheber der Änderung.

Änderungsaufzeichnungen finden sich bei OpenOffice.org im „Bearbeiten“-Menü unter „Änderungen“. In den Untermenüpunkten lässt sich einstellen, ob Änderungen aufgezeichnet werden. Die Entscheidung, ob eine Änderung akzeptiert oder verworfen wird, fällt unter dem Untermenüpunkt „Akzeptieren oder Verwerfen“. Hier werden alle Änderungen mit Zeitpunkt und Benutzer aufgelistet. Ein Dokument enthält erst dann mit Sicherheit keine aufgezeichneten Änderungen, wenn die Liste der Änderungen keinen Eintrag enthält. Die aufgezeichneten Änderungen werden in der Datei „content.xml“ mitgespeichert.

Unabhängig von der Änderungsaufzeichnung besteht auch die Möglichkeit, verschiedene Versionen eines Dokumentes zu speichern. Dazu wird in OpenOffice.org im „Datei“- Menü der Eintrag „Versionen“ benutzt. Alle Versionen werden innerhalb des ODF-Dokumentes im Ordner „Versionen“ gespeichert. Dabei wird eine Datei „VersionX“ erstellt, wobei das X für eine fortlaufende Nummer der Version steht. Die Datei „VersionList.xml“ enthält Metadaten zur Zuordnung aller Versionen eines Dokumentes. Sie wird nur erstellt, wenn ein Dokument unterschiedliche Versionen beinhaltet. Ähnlich wie bei Änderungsaufzeichnungen gilt auch hier: Ein Dokument behält seine gespeicherten Versionen, bis diese in der Liste der Versionen gelöscht wurden.

Notizen lassen sich innerhalb eines Dokumentes platzieren. Im OpenOffice.org-Navigator, einer Auflistung aller Elemente des Dokumentes, lassen sich die Notizen auch ändern und löschen. Ähnlich wie bei den Änderungsaufzeichnungen wird eine Notiz in der Datei „content.xml“ gespeichert.

Metadaten, Änderungsaufzeichungen, Versionen und Notizen gehören zu den Elementen eines Dokumentes, die bei der Erstellung nicht direkt im Text sichtbar sind. Sie verdienen daher vor der Veröffentlichung besondere Aufmerksamkeit. Hierzu enthält OpenOffice.org eine Einstellung in den Programmoptionen „Sicherheit“, die es erlaubt, den Benutzer bei bestimmten Aktionen zu warnen. Dies gilt für alle vier vorgestellten Inhaltselemente und lässt sich separat für die Aktionen „Speichern oder Senden“, „Signieren“, „Drucken“ und „PDF-Dateien erzeugen“ festlegen.

Möglichkeiten zur Konvertierung und Weiterverarbeitung von ODF-Dokumenten

Beim Import und Export von ODF zu anderen Formaten werden XML-Filter benutzt, die mit Hilfe von XSL-Transformationen Inhalte verarbeiten. Dabei werden Regeln festgelegt, welche XML-Elemente in welcher Form in der erstellten Datei verwendet werden. Das erlaubt nicht nur die Konvertierung von und zu anderen Formaten, sondern auch Veränderungen am Dokument unter Beibehaltung des Open-Document-Formates.

Im Hinblick auf versteckte Informationen hat das weit reichende Bedeutung. Es ist durch diesen Mechanismus möglich, individuelle Sicherheitsrichtlinien zu schaffen, indem je nach Anwendungszweck bestimmte Inhalte, beispielsweise Notizen, aus den Dokumenten entfernt werden. Die Nutzung dieser Möglichkeit innerhalb der Anwendung erfordert jedoch entsprechend geschulte Benutzer. Es bietet sich daher an, die Überprüfung des Dokumentes vor der Veröffentlichung an zentraler Stelle zu automatisieren und somit die Sicherheit unabhängig vom Verhalten der Benutzer zu machen. Gerade für größere Unternehmen mit bereits vorhandenem Dokumentenmanagement und festgelegtem Workflow vor der Veröffentlichung ist eine Integration denkbar und sinnvoll.

Überlegungen zum Datenschutz

Bei diesem Thema drängt sich die Frage auf, ob Daten aus öffentlichen Dokumenten genutzt werden dürfen, obwohl der Autor keine Kenntnis von ihnen hat. Hier handelt es sich um eine rechtliche Grauzone. Wenn einem Nutzer das Wissen zumutbar ist, dass versteckte Informationen in seinem Dokument vorhanden sein könnten, so ist er für die Erhebung, Verarbeitung und Verbreitung dieser Daten verantwortlich und auch belangbar. Wer schutzwürdige Daten verarbeitet, sollte auch das Wissen besitzen, dies richtig zu tun! Schließlich wird es von ihm auch erwartet.

Wenn nun aber nicht davon ausgegangen werden kann, dass der Nutzer das Wissen besitzt oder die Fähigkeit von ihm verlangt werden kann, diese Daten zum Beispiel zu entfernen, wären die Hersteller der Software zu belangen, da sie den nötigen Informationspflichten nicht nachgekommen sind.

Microsoft zum Beispiel ist dem zuvor gekommen, indem es eine Anleitung veröffentlicht hat, in der auf dieses Problem eingegangen wird [15]. Der Nutzer bekommt zudem eine Warnung, wenn er Dokumente mit der Feature „Änderungen verfolgen" abspeichern will. Auch bei anderen Institutionen findet man Informationen über versteckte Daten in Dokumenten und wie man diese entfernen kann [3] [7] [11].

Ob der ungeschulte Nutzer, dem ohnehin das Wissen um die versteckten Informationen fehlt, zugemutet werden kann, die nicht ohne weiteres auffindbaren Anleitungen zu entdecken, zu verstehen und umzusetzen, ist fraglich. Ebenfalls ist nicht bekannt, ob diese Art der Information ausreichend ist und sich Softwarehersteller so völlig aus der Verantwortung stehlen können. Bis zum Abschluss dieser Arbeit ist keine Rechtsentscheidung bekannt, die diese Frage eindeutig klärt.

Brisante Vorfälle

Dass versteckte Informationen sehr kritisch sein können, zeigen die folgenden Fälle.

- Die New York Times veröffentlichte ein PDF Dokument der CIA, das den Sturz der Regierung Irans im Jahre 1954 beinhaltete. Es handelte sich dabei um ein altes eingescanntes Dokument. Ein übliches Verfahren war es, heikle Textpassagen einfach mit einer schwarzen Box zu übermalen. Das Ergebnis war jedoch, dass das Dokument immer noch die Originaldaten enthielt, was schließlich jemand nutzte und die eingeschwärzten Namen Beteiligter veröffentlichte und das so geänderte Dokument im Internet verbreitete [5].

- Ein freier Journalist fand 2002 anhand der herunter geladenen Kurzfassung der Metrorapid-Machbarkeitsstudie heraus, dass wesentliche Textpassagen kurz vor der Veröffentlichung gelöscht wurden. So wurden aus 172 plötzlich 192 Stehplätze pro Zug und kritische Textpassagen wie „Große Trassen-

Die Autoren

Foto:
Heike Schulze,
Brandenburg

Prof. Dr. Barbara Wiesner war bis vor kurzem Professorin für Datensicherheitstechnologie an der Fachhochschule Brandenburg. Inzwischen ist sie im Ruhestand.

An dem Projekt beteiligte Studierende:

Joanna Skowronska, Janette Wehner (Microsoft Word Dokumente)
Kai Frentzel, Torsten Müller (Dokumente im PDF-Format)
Marek Lode, Martin Weigel (Dokumente im RTF-Format)
Daniel Knapp (Dokumente im Open Dokument Format)
Jan Dreger (Datenschutz, brisante Vorfälle)

abschnitte verlaufen durch Landschaftsschutzgebiete und regionale Grünzüge“ einfach gestrichen [18].

- Ein Professor der Cambridge Universität stellte fest, dass das Dossier der britischen Regierung über Sicherheit und Geheimdienstkräfte im Irak Textpassagen enthielt, die ursprünglich aus einem ganz anderen Text stammten. Eine Analyse der verborgenen Daten ergab, dass das Dossier von 4 Mitarbeitern bearbeitet wurde, die daraufhin schnell identifiziert werden konnten. Nach weiterer Analyse stellte sich heraus, dass noch weitere Texte von Veröffentlichungen, teilweise aus dem Jahr 1997, kopiert wurden. Lediglich Mengenangaben und Textpassagen wurden geändert, um Aussagen zu verdeutlichen. Letztendlich wurden unerlaubt weit über 90% des Dossiers aus urhebergeschützten Veröffentlichungen verwendet, ohne die Zustimmung der eigentlichen Autoren [9].

- Ein Untersuchungsbericht zu den Vorkommnissen im Irak, bei dem der Geheimdienstmitarbeiter Nicola Calipari getötet wurde und unter anderem zwei italienische Staatangehörige verletzt wurden, wurde von den offiziellen Behörden der USA im Sommer 2005 ins Netz gestellt. Unter anderem enthielt er nähere Informationen zu der Befreiung der Italienerin Giuliana Sgrena. In diesem Bericht waren Textstellen geschwärzt. Die geschwärzten Texte konnten wiederhergestellt werden. Sie enthielten neben den Namen der verdeckten Ermittler und den näheren Umständen der Befreiung auch Orte, Decknamen und beteiligte Einheiten der Streitkräfte [12].

Resumé

Die Untersuchungen haben gezeigt, dass man versteckte Daten in allen betrachteten Dateiformaten finden kann. Während man sich bei offenen Formaten informieren kann, wo diese Informationen zu finden sind, ist dies bei proprietären Formaten wie z.B. Microsoft Word nicht offen gelegt. Das Auffinden wird damit erheblich erschwert. Doch auch bei den offenen Formaten gehört erhebliches Fachwissen dazu, damit man sicher sein kann, dass keine versteckten Informationen im Dokument vorhanden sind. Es empfiehlt sich daher, z. B. bei der Weitergabe von sicherheitskritischen Word-Dokumenten zumindest ein Programm zum Löschen versteckter Daten einzusetzen oder aber dieses Dokument nach der Anleitung der NSA [11] nach PDF zu konvertieren.

Last not least sei gesagt, dass der deutsche Geheimdienst die Brisanz des Themas inzwischen erkannt hat. Der Bericht des BND zur Bespitzelung von Journalisten wurde veröffentlicht, indem dieses Dokument ausgedruckt und wieder eingescannt wurde. Somit ist es völlig ausgeschlossen, dass Informationen enthalten sind, die nicht für die Öffentlichkeit bestimmt sind [1].

Literatur

[1] Bericht des Sachverständigen Prof. Schäfer zu Aktivitäten des BND gegenüber Journalisten in gekürzter Fassung *http://www2.bundestag.de/bnd_bericht.pdf* (letzter Zugriff: 4.10.2006.)

[2] Bitform Discover: *http://www.bitform.net/products/discover/ (letzter Zugriff: 4.10.2006.)*

[3] BSI (Bundesamt für Sicherheit in der Informationstechnik), M 4.64 Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen *http://www.bsi.de/gshb/deutsch/m/m04064.htm* (letzter Zugriff: 4.10.2006.)

[4] Byers, Simon. Information Leakage Caused by Hidden Data in Published Documents, IEEE Security & Privacy. March/April 2004

[5] CIA Document News: *http://www.schneier.com/crypto-gram-0007.html*, Original: *http://www.nytimes.com/library/w orld/mideast/041600iran-cia-index.html* Dokument: *http://cryptome.org/cia-iran-all.htm* (letzte Zugriffe: 4.10.2006.)

[6] DocScrubber: *http://www.docscrubber.com/* (letzter Zugriff: 4.10.2006.)

[7] DS (Deutsche Datenschutzzentrum Schleswig-Holstein) *http://www.datenschutzzentrum.de/systemdatenschutz/meldung/sm95.htm* (letzter Zugriff: 4.10.2006.)

[8] ezClean: *http://www.kklsoftware.com/products/ezClean/details.asp* (letzter Zugriff: 4.10.2006.)

[9] Iraq „dodgy dossier“ News: *http://www.casi.org.uk/discuss/2003/msg00457.html* Original: *http://www.computerbytesman.com/privacy/blair.doc* (letzter Zugriff: 4.10.2006.)

[10] Merz, Thomas; Drümmer, Olaf. Die Postscript und PDF Bibel, dpunkt Verlag 2002

[11] National Security Agency. Redacting with Confidence: How to Safely Publish Sanitized Reports Converted From Word to PDF *http://www.fas.org/sgp/othergov/dod/nsa-redact.pdf* (letzter Zugriff: 4.10.2006.)

[12] Nicola Calipari Original: *http://www.macchianera.net/files/rapportousacalipari-noomissis.pdf* Dokument: *http://www.macchianera.net/files/rapportousacalipari.pdf* (letzter Zugriff: 4.10.2006.)

[13] Office 2003/XP-Add-In zum Entfernen verborgener Daten *http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=144E54ED-D43E-42CA-BC7B-5446D34E5360* (letzter Zugriff: 4.10.2006.)

[14] Open Document Format for Office Applications (OpenDocument) 1.0 *http://www.oasis-open.org/committees/download.php/12572/OpenDocument-v1.0-os.pdf* (letzter Zugriff: 4.10.2006.)

[15] Schützen von persönlichen Daten in Word 2003-Dokumenten *http://www.microsoft.com/germany/msdn/library/office/word/SchuetzenVonPersoenlichenDatenInWord2003Dokumenten.mspx?mfr=true* (letzter Zugriff: 4.10.2006.)

[16] Sicheres Austauschformat für elektronische Dokumente: *http://www.redtenbacher.de/rtf/index.htm* (letzter Zugriff: 4.10.2006.)

[17] The Risks of Metadata and Hidden Information. Analysis of Microsoft® Office Files from the Websites of the Fortune 100 *www.stg.srs.com/eds/archive/BitformFortune100Study.pdf* (letzter Zugriff: 4.10.2006.)

[18] Transrapid-Gutachtenmanipuliert?*http://www.heise.de/ct/02/05/041/default.shtml* (letzter Zugriff: 4.10.2006.)

[19] WinHex: *http://www.x-ways.net/winhex/index-d.html* (letzter Zugriff: 4.10.2006.)

[20] Word 2003: Rich Text Format (RTF) Specification, version 1.8 *http://www.microsoft.com/downloads/details.aspx?familyid=AC57DE32-17F0-4B46-9E4E-467EF9BC5540&displaylang=en* (letzter Zugriff: 4.10.2006.)

[21] WorkshareProtect: *http://www.officeinfo.com.au/Products/Workshare/WorkshareProtect.asp* (letzter Zugriff: 4.10.2006.)

Hinweis: Die Produktnamen in diesem Beitrag sind geschützt.

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: 927929
BLZ 250 905 00
IBAN: DE05250905000000927929
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*

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

FIfF-Vorstand

- **Prof. Dr. Hans-Jörg Kreowski (Vorsitzender)** Bremen
- **Dagmar Boedicker (stellv. Vorsitzende)** München
- **Stefan Hügel** München
- **Werner Hülsmann** Konstanz
- **Prof. Dr. Klaus Köhler** München
- **Prof. Dr. Dietrich Meyer-Ebrecht** Aachen
- **Michael Riemer** Bremen
- **Prof. Dr. Joseph Weizenbaum** Berlin

Beirat

Michael Ahlmann (Bremen); **Prof. Dr. Wolfgang Coy** (Berlin); **Prof. Dr. Wolfgang Däubler** (Bremen); **Prof. Dr. Christiane Floyd** (Hamburg); **Prof. Dr. Klaus Fuchs-Kittowski** (Berlin); **Prof. Dr. Thomas Herrmann** (Dortmund); **Prof. Dr. Wolfgang Hesse** (Marburg); **Prof. Dr. Michael Grütz** (Konstanz); **Ulrich Klotz** (Frankfurt); **Prof. Dr. Herbert Kubicek** (Bremen); **Prof. Dr. Hans-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. Britta Schinzel** (Freiburg); **Prof. Dr. Dirk Siefkes** (Berlin); **Prof. Dr. Marie-Theres Tinnefeld** (München); **Dr. Gerhard Wohland** (Waldorfhäslach)

Überregionale Arbeitskreise des FIfF

AK »Videoüberwachung und Bürgerrechte«
Peter Bittner, Humboldt-Universität – Institut für Informatik
Unter den Linden 6 , 10099 Berlin
bittner@informatik.hu-berlin.de

AK »RUIN« (Rüstung und Informatik)
Kontakt über das FIfF-Büro Bremen

Regionalgruppen und regionale Ansprechpartner

Aachen
Prof. Dr.-Ing.
Dietrich Meyer-Ebrecht
Tel. (0241) 89498959
dme@fiff.de

Berlin
Peter Bittner
Humboldt-Universität
Institut für Informatik
Unter den Linden 6
10099 Berlin
bittner@informatik.hu-berlin.de

Berlin
Irina Piens
Schlesische Str.29
10997 Berlin
piens@prz.tu-berlin.de

Braunschweig
TU Braunschweig
Fachschaft Informatik
AStA-Fach
Katharinenstraße 1
38106 Braunschweig

Bielefeld
c/o Angewandte Informatik
Technische Fakultät
Universität Bielefeld
Postfach 100 131
33502 Bielefeld
fiff-bi@TechFak.Uni-Bielefeld.de

Bremen
Prof. Dr. Hans-Jörg Kreowski
Uni Bremen
FB Informatik/Mathematik
Postfach 330 440
28334 Bremen
Tel.: (0421) 218-2956
http://fiff.informatik.uni-bremen.de
fiff@informatik.uni-bremen.de

Darmstadt
Julia Stoll
Heinheimer Str. 29-31
64289 Darmstadt
Tel.: (06151) 71 21 81
julias@acm.org

Erlangen/Fürth/Nürnberg
Klaus Thielking-Riechert
Am Dummetsweiher 9
91056 Erlangen

Freiburg
Prof. Dr. Britta Schinzel
Universität Freiburg
Institut für Informatik und Gesellschaft
Friedrichstr. 50
79098 Freiburg im Breisgau
Tel.: (0761) 203-4953
Fax: (0761) 203-4960
schinzel@modell.iig.uni-freiburg.de

Frankfurt
Ingo Fischer
Dahlmannstraße 31
60385 Frankfurt am Main

Heilbronn
Michael Müller
FH Heilbronn, FB
Max-Planck-Straße 39
74081 Heilbronn
Tel.: (07131) 50 43 64
michael.mueller@fh-heilbronn.de

Jena
Prof. Dr. Eberhard Zehendner
Institut für Informatik
Friedrich-Schiller-Universität
07740 Jena
Tel.: (03641) 946385
Fax: (03641) 946372
nez@uni-jena.de

Kaiserslautern
Harald Weber
Institut für Technologie und Arbeit
Technische Universität Kaiserslautern
Gottlieb-Daimler-Straße / Geb. 42
67663 Kaiserslautern
harald.weber@ita-kl.de

Karlsruhe
Prof. Dr. Thomas Freytag
Weltzienstr. 35
76135 Karlsruhe
Tel.: (0721) 815416 (p)
fiff@thomas-freytag.de

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

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

Konstanz
Ulrich Moser
Schlossstrasse 7
78244 Gottmadingen
Tel.: (07731) 74261 (p)
+41-79-3112051 (d)
fiff-kn@apis-security.com

München
Bernd Rendenbach
Leerbichlallee 19
82031 Grünwald
Tel.: (089) 6410547
Bernd.Rendenbach@web.de

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

Paderborn
Harald Selke
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn
hase@uni-paderborn.de

Stuttgart
Kurt Jaeger
Mezgerstraße 34
70563 Stuttgart
Tel.: (0711) 8701309
(0711) 90074-23
Fax: (0711) 7289041
pi@lf.net

Tübingen
Jochen Krämer
Sand 13
72076 Tübingen
Tel.: (07071) 29-5957

Ulm
Bernhard C. Witt
Reuttier Str. 15
89231 Neu-Ulm
bcw@uni-ulm.de

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

FIfF

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 **20 Euro** jährlich frei Haus abonnieren.
- ❑ dem FIfF etwas spenden.
- ❑ Ich überweise den Betrag auf das **Konto 927929** bei der Sparda Bank Hannover eG, BLZ **250 905 00** oder nutze die internationale Kontonummer **IBAN: DE05250905000000927929** , **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): _____

Ich möchte als Mitglied per Email über Aktionen, Beschlüsse u.ä. informiert werden; meine Email:

_____

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.

Die FIfF-Kommunikation bittet um Beiträge!

Die FIfF-Kommunikation lebt von der aktiven Mitarbeit ihrer Leserinnen und Leser! Interessante Artikel sowie Fotos und Zeichnungen zur Illustration (mit Quellenangaben und Nachdruckgenehmigung) sind immer herzlich willkommen. Die Bearbeitung wird erleichtert, wenn Beiträge elektronisch und zusätzlich auf Papier der Redaktion zugehen. Die Redaktion behält sich Kürzungen und Titeländerungen vor.

Geplante Themenschwerpunkte der nächsten Hefte:

Heft 1/2007
„Heft zur Jahrestagung 2006"
Redaktionsschluss: 4.2.2007

Heft 2/2007
„Gender"
Redaktionsschluss: 4.5.2007

Heft 3/2007
„Visionen"
Redaktionsschluss: 4.8.2007

Daneben sind immer auch Artikel zu aktuellen Themen willkommen. Bitte setzen Sie sich mit der Redaktion in Verbindung:

redaktion@fiff.de oder über die Geschäftsstelle des FIfF e.V.

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

Bürozeiten:
Bitte entnehmen Sie diese der Webseite.

Bankverbindung:
Sparda Bank Hannover eG
Kontoverbindung: 927929BLZ 250 905 00
IBAN: DE05250905000000927929 BIC: GENODEF1S09

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!

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	5 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 20 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Sebastian Jekutsch, Ralf Streibl
Schwerpunktredaktion	—
V.i.S.d.P.	Dagmar Boedicker
FIfF-Überall	In dieser Rubrik der FIfF-Kommunikation ist jederzeit Platz für Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert@mtsf.de.* Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *http://www.fiff.de/regional*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an Claus Stark: *claus@fiff.de*
Layout	Berthold Schroeder
Titelbild	Idee und Gestaltung Dagmar Boedicker und 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.

Schluss FIfF

„Es ist besser, den Wandel in die Hand zu nehmen als den Wandel an der Kehle zu haben.“

Das soll Churchill gesagt haben, und es ist unmittelbar überzeugend. Dummerweise haben unsere Mitglieder dazu nur einmal im Jahr Gelegenheit, bei der Jahrestagung. Den Rest des Jahres beraten sich Aktive und Vorstand und versuchen, im Sinne der Mitglieder Beschlüsse zu fassen, Presseerklärungen rauszugeben, sich da einzumischen, wo es für einen Verein wie das FIfF sinnvoll und notwendig erscheint (und die bescheidenen Arbeitskapazitäten es zulassen). Sind die Äußerungen und anderen Aktivitäten im Sinne der Mitglieder? Nachdem bisher der Vorstand immer entlastet worden ist, waren sie wohl meist ganz in Ordnung, aber schön wäre es vielleicht doch, wenn mensch schon vorher eine Anregung oder eine Kritik anmelden könnte. Oder einen Vorschlag, der zunächst im Kreis des FIfF e.V. bleibt.

Wir stehen natürlich voll hinter der informationellen Selbstbestimmung – aber muss es wirklich sein, dass wir nur von 339 Mitgliedern eine Mail-Adresse haben? Zivilgesellschaft funktioniert eigentlich anders, nicht nur bei weniger IT-kritischen Organisationen ... Wir würden Presseerklärungen gern mal vorab an die Mitglieder schicken. Dabei muss es aber schnell gehen. Journalisten haben nämlich ein paar Tage später schon wieder ein anderes Thema, und wenn etwas uninteressanter ist als die Zeitung von gestern, dann ist es eine abgestandene Presseerklärung. Wir würden gern hören, oder vielmehr lesen, was Ihr oder Sie denn dazu sagt, und die Presseerklärung erst dann rausgeben. Das macht die Organisation zwar für die sowieso schon arg strapazierten Vorstandmitglieder etwas stressiger, aber es wäre es wert.

Ein bisschen mehr Demokratie im Verein wäre schön. Bloß geht das nicht ohne Mail-Adressen. Anja in der Geschäftsstelle würde so einen Mitglieder-Verteiler einrichten und pflegen, es lohnt sich bloß nicht mit den paar Adressen, die wir bisher haben. Und die bundesweite FIfF-Liste ist dafür ungeeignet, die ist für jede und jeden, und es kann nicht sein, dass Entwürfe oder Ideen zur Vereinsarbeit gleich nach draußen an einen Kreis auch unbekannter Menschen gehen.

Wir würden die Mailadressen natürlich nicht offen durch’s Netz schicken sondern als /bcc. Wie wäre es, wenn Du (oder Sie) Dich entschließen würdest, **jetzt** eine Mail an die Geschäftsstelle zu schicken und zu schreiben, dass Du in diesen Verteiler aufgenommen werden und Informationen über Vereinsaktionen, Beschlüsse u.ä. erhalten möchtest? *fiff@fiff.de* ist die Adresse.

Du kannst übrigens beruhigt sein, wir werden die Liste Deiner Mails weder unnötig noch ungebührlich aufblähen. Für das Erste haben wir keine Zeit und für das Zweite sind wir zu wohlerzogen.

Dagmar Boedicker, für den Vorstand

Geeignete Texte für den SchlussFIfF bitte mit Quellenangabe an Claus Stark (Adresse siehe Impressum) senden.