H 7625

FIfF Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

24. Jahrgang 2007 Einzelpreis: 5 EUR

4/2007 - Dezember 2007

Datensammelwut

ISSN 0938-3476

• Marketing-Märchen • Software-Engineering in Äthiopien • Solving the E-Waste Problem •

FIfF Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Titelbild: Resignation
C. Antonius, Berlin, photography@berlin.de
Beitrag zum FIfF-Fotowettbewerb 2006

inhalt

Inhalt

Ausgabe 4/2007

03 Editorial
- Dagmar Boedicker

Rund um die Jahrestagung 2007

05 Bielefeld – Hauptstadt des Datenschutzes
Tagungen von DVD, FoeBuD und FIfF am 12./13. Oktober 2007
- Stefan Hügel

09 Bielefelder Erklärung wider Überwachungs- und Datensammelwahn
- Presseerklärung vom FIfF, DVD und FoeBuD

10 Bericht des FIfF-Vorstands
- Hans-Jörg Kreowski

13 Kampagne gegen Datensammelwut
Überregionale Arbeitsgruppe gegründet
- Werner Hülsmann

14 AG FIfF-Kommunikation
auf der Jahrestagung 2007
- Dagmar Boedicker

15 FIfF-Kommunikation: Schlechtes Gewissen oder Ruhekissen - Leserbrief
- Jens Woinowski

Rubriken

16 Lesen - Neues für den Bücherwurm

20 Fachschaften - Bericht von der 35,0. Konferenz der Informatik-Fachschaften

51 Impressum

52 SchlussFIfF

Aktuelles

21 Solving the E-Waste Problem
- Pia Grund-Ludwig

23 Markt, Lügen und Video
Wie man einen Kurs in Forschungsmarketing ohne Sinnkrise übersteht
- Lorenz M. Hilty

24 Software-Engineering in Äthiopien
- Christiane Floyd

28 Weder Sicherheit noch Recht
- Hans-Georg Wischkowski

Nachschlag

31 Überwachung und Datenschutz –
Politik contra Bundesverfassungsgericht
- Thilo Weichert

36 Der Staat hackt mit
Mehr Sicherheit durch Bundestrojaner?
- Klaus-Peter Löhr

40 Email Privacy in the USA
Warshak v. United States
- Vincent Brannigan

41 Weit entfernt von der Normalität
- Sven Lüders

43 Egon Schäuble
- Petra Pau

44 G8-Gipfel – Schäubles Planspiele werden Realität
- Silke Stokar

46 Das hohe Gut der Menschen- und Bürgerrechte darf nicht angetastet werden!
- Klaus Fuchs-Kittowski

FIfF e.V.

04 Brief an das FIfF
- Hans-Jörg Kreowski

Dagmar Boedicker

Editorial

Im September haben uns die Verhältnisse veranlasst, uns in einem Sonderheft klar und deutlich *Wider den Zeitgeist* auszusprechen. Viele Aktive im FIfF haben Andere angesprochen, von denen sie annahmen, dass die symbolische Debatte gegen den Terrorismus auch bei ihnen einen Nerv berührt hatte. Wir bekamen so viele erstklassige Beiträge aus persönlicher Betroffenheit, Wut und Empörung, dass wir die 28 Seiten, die uns für das Sonderheft nur zur Verfügung standen, mehrmals hätten füllen können. Deshalb kann man die vorliegende FIfF-Kommunikation als Folgeheft dazu verstehen. Auch unsere Beiräte haben sich mit lesenswerten Beiträgen zu Wort gemeldet. – Diese FIfF-Kommunikation enthält aber außerdem Beiträge, die ganz besonders für unsere Mitglieder von Interesse sein dürften: Das FIfF wackelt, aber es hat schon mehr gewackelt als jetzt. Aus der Jahrestagung 2007 dürfte ein gestärktes Team hervorgegangen sein, Berichte darüber gibts hier zu lesen. Die Hauptstadt des Datenschutzes, Bielefeld, hatte am 12. und 13. Oktober aber noch mehr zu bieten.

Die FIfF-Jahrestagung 2007 am 13. Oktober in Bielefeld war wieder eine schöne und interessante Tagung, und bei der Mitgliederversammlung waren diesmal auch einige neue Gesichter zu sehen. Gut, dass sie nicht nur zum Zuschauen, Diskutieren und Wählen gekommen waren, sechs von ihnen haben sich den sechs Mitgliedern aus dem bisherigen Vorstand zugesellt. Damit dürfte die Zukunft des FIfF von einer kreativen Mischung aus neuen Mitgliedern mit unverbrauchten Ideen und erfahrenen Vorstandsprofis mit Reife und Stehvermögen geprägt werden, die nur das Beste erwarten lässt.

Stefan Hügel hat einen ausführlichen Bericht über die beiden Tage in Bielefeld geschrieben, auch über das Jubiläum der Deutschen Vereinigung für Datenschutz (DVD) und die BigBrother Awards (BBA). Die drei Vereine DVD, FIfF und FoeBuD (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs) haben eine gemeinsame Bielefelder Erklärung verabschiedet, die wir in diesem Heft veröffentlichen. Leider hat es nicht geklappt, von der FIfF-Jahrestagung auch die beiden Hauptvorträge von Constanze Kurz und Padeluun zu bringen. Hans-Jörg Kreowski hat aber seinen Bericht liefern können, und zu den Arbeitsgruppen FIfF-Kommunikation und Kampagne gegen Datensammelwut auf der Jahrestagung gibt es kurze Zusammenfassungen. So ist auch diesmal zwar kein vollständiger, aber doch ein Eindruck von unserer Tagung entstanden – immerhin!

Informatik-Fachschaften!

Die neue Rubrik für die Fachschaften wartet auf Inhalte. Wir laden die KIF (**K**onferenz der **I**nformatik-**F**achschaften) in diese Kolumne ein, in der die Probleme des Informatik-Studiums diskutiert werden können und alles, was die KIF für wichtig hält.

... und andere

Ob Lorenz Hiltys Text über eine Forschungs-Marketing-Fabel und wie Lorenz sie empfunden hat, eher zum Lachen oder zum Weinen anregen? – Christiane Floyd öffnet ein Fenster in die Welt, wie wir es uns öfter wünschen würden, was auch für den Beitrag von Pia Grund-Ludwig gilt.

Der *Nachschlag* zur Überwachung enthält kritische Beiträge von Hans-Georg Wischkowski, Thilo Weichert, Klaus-Peter Löhr, Klaus Fuchs-Kittowski, Petra Pau und Silke Stokar, Vincent Brannigan und Sven Lueders. Er ist tatsächlich so lang geworden wie das Sonderheft, das der letzten FIfF-Kommunikation beilag.

In der Rubrik *Lesen* haben wir diesmal vier Rezensionen, zu Bildungsprozessen mit Digitalen Medien, dem Innovationsverhalten deutscher Software-Entwicklungsunternehmen und der Bedeutung von Open-Source-Software in diesem Zusammenhang, und einer Studie zur interdisziplinären Geschlechterforschung.

Und wir haben auch endlich mal wieder einen Leserbrief bekommen! Er gibt eine Meinung in der Debatte auf der Mitglieder-Liste wieder, die allen interessierten Mitgliedern zum Nachlesen zur Verfügung steht.

Dagmar Boedicker

Dagmar Boedicker ist technische Redakteurin und Trainerin für Softwaredokumentation und hat Politikwissenschaft studiert.

Hans–Jörg Kreowski

Brief an das FIfF

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

auf der Mitgliederversammlung des FIfF am 13. Oktober 2007 bin ich für eine dritte Amtszeit als Vorsitzender gewählt worden. Ich möchte mich bei allen, die mir ihre Stimme gegeben haben, für ihr Vertrauen bedanken und hoffe, dass eine Mehrheit der Mitglieder, die nicht in Bielefeld waren, auch so gestimmt hätte. Ich werde nach meinen Möglichkeiten alles daransetzen, die Arbeit des FIfF noch wirksamer werden zu lassen. Eine enge Grenze findet meine Absicht darin, dass ich als Professor für Theoretische Informatik schon gut zu tun habe und zwischen dieser Tätigkeit und dem FIfF-Vorsitz wenig Synergieeffekte auftreten. So bleiben mir für die Arbeit im FIfF rund zehn Stunden pro Woche, was angesichts allen dessen, was zu leisten wäre, schrecklich wenig ist.

Aber ein Vorsitzender allein kann ohnehin kaum etwas bewegen. Es kommt darauf an, wie viel politische Kraft wir alle zusammen im FIfF entfalten. Dazu gehört unter anderem die Arbeit des Vorstands. In den letzten zwei Jahren war er mit neun und nach einem Rücktritt mit acht Mitgliedern klein. Jetzt hat er mit elf Mitgliedern zahlenmäßig und so hoffentlich auch kräftemäßig dazu gewonnen. Besonders erfreulich daran ist, dass die neuen Mitglieder das Durchschnittsalter erheblich absenken und die Zahl der Jüngeren im Vorstand größer ist als die Zahl der Älteren. Aus persönlichen Gründen haben Dagmar Boedicker und Klaus Köhler nicht wieder kandidiert. Für ihre langjährige und maßgebliche Vorstandsarbeit gebührt ihnen besonderer Dank. Beide werden sich weiterhin an den Aktivitäten des FIfF beteiligen. Wieder gewählt wurden Stefan Hügel, Werner Hülsmann, Dietrich Meyer-Ebrecht, Michael Riemer und Joseph Weizenbaum, wobei Stefan als stellvertretender Vorsitzender gewählt wurde. Neu im Vorstand sind Carsten Büttemeier, Andreas Hofmeier, Jens Rinne, Britta Schinzel, Jakob Schröter und Joerg Zeltner. Ich freue mich auf die Zusammenarbeit mit diesem Vorstand in den nächsten zwei Jahren. Ich bitte alle Mitglieder, uns tatkräftig zu unterstützen.

Was die Mitgliederversammlung angeht, möchte ich noch auf zwei weitere Punkte hinweisen. Auf der Tagesordnung stand wie immer auch der Bericht des Vorstands, den ich zu großen Teilen für diese FIfF-Kommunikation auch schriftlich gefasst habe, damit alle Mitglieder nachlesen können, was den Vorstand umtreibt. Der Bericht ist durchaus auch als Fortsetzung dieses Briefes an das FIfF gemeint.

Schließlich soll die *Bielefelder Erklärung wider Überwachungs- und Datensammelwahn* nicht unerwähnt bleiben, die von der Mitgliederversammlung einstimmig verabschiedet worden ist. Die Deutsche Vereinigung für Datenschutz (DVD), die am 12. Oktober ihren 30. Datenschutztag veranstaltete, der Verein zur Förderung des öffentlich bewegten und unbewegten Datenverkehrs (FoeBud), der am Abend desselben Tages seine grandiose BigBrotherAwards-Verleihung durchführte, und das FIfF mit seiner Jahrestagung am folgenden Tag haben das Zusammentreffen in der Ravensberger Spinnerei in Bielefeld zum Anlass genommen, eine gemeinsame Erklärung zu erarbeiten und herauszugeben. In einem der beiden Workshops während der FIfF-Jahrestagung wurde dieser Faden aufgegriffen und überlegt, ob und wie das FIfF eine breit angelegte, längerfristige und phantasievolle Kampagne gegen die Datensammelwut durchführen kann. Wer interessiert ist an der Weiterentwicklung und Umsetzung dieser Idee, möge sich bitte bei mir melden.

Mit fiffigen Grüßen

Hans-Jörg Kreowski

Folien aus der PowerPointParodie: ***In der Datenfalle oder ich habe doch nichts zu verbergen***

Stefan Hügel

Bielefeld – Hauptstadt des Datenschutzes

Tagungen von DVD, FoeBuD und FIfF am 12./13. Oktober 2007

Gleich drei Veranstaltungen fanden am 12. und 13. Oktober in Bielefeld statt: Der Datenschutztag *der* Deutschen Vereinigung für Datenschutz (DVD), *die federführend vom* FoeBuD (Förderverein für den bewegten und unbewegten Datenverkehr) *ausgerichteten* BigBrotherAwards 2007 *und die Jahrestagung 2007 des* FIfF. *Alle hatten den Datenschutz zum Thema – oder vielmehr die Tatsache, dass er oft nicht beachtet und von vielen Akteuren demontiert wird. Zum Abschluss der Veranstaltungen verabschiedeten die drei Organisationen ihre gemeinsame* Bielefelder Erklärung, *nachzulesen in dieser Ausgabe der FIfF-Kommunikation.*

Datenschutztag der Deutschen Vereinigung für Datenschutz (DVD)

Den Anfang machte am Freitag die DVD, die ihr 30jähriges Bestehen feierte. Dazu hatte man prominente Referenten eingeladen – allen voran Burkhard Hirsch, profilierter Bürgerrechtler der FDP, der zum Thema „Datenschutz als Grundrecht" referierte.

Am Anfang wurde das Grußwort von *Peter Schaar*, Bundesdatenschutzbeauftragter, zum 30jährigen Bestehen verlesen. Er gab darin einen Abriss der letzten 30 Jahre Datenschutz, beginnend mit dem ersten Bundesdatenschutzgesetz über das Volkszählungsurteil, durch das die informationelle Selbstbestimmung als Grundrecht begründet wurde, bis hin zum *Großen Lauschangriff* und den Gesetzen in Folge des 11. September 2001. Schaar sieht zwar nicht die Gefahr eines Überwachungs*staats,* doch aber die Entwicklung hin zu einer Überwachungs*gesellschaft,* begünstigt durch das Vordringen der Informationstechnik in alle Lebensbereiche, den Charakter von persönlichen Informationen als Wirtschaftsgut und die immer schnelleren Verarbeitungsmöglichkeiten auch großer Datenbestände. Mangelnden Datenschutz sieht er als eine Form der Dehumanisierung und als Verlust individueller Freiheit.

Thilo Weichert, Leiter des unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, gab zuerst seiner Freude über die erfolgreiche Demonstration *Freiheit statt Angst* gegen die Vorratsdatenspeicherung in Berlin Ausdruck: 15.000 Menschen gingen für den Datenschutz auf die Straße soviel wie seit 1987 nicht mehr.

Er skizzierte dann die Entwicklungen der letzten 30 Jahre, vom Schutz vor Missbrauch personenbezogener Daten, der das erste Bundesdatenschutzgesetz charakterisierte, bis zu den Persönlichkeitsrechten, die seit den 80er Jahren die Diskussion bestimmen. Das Grundrecht auf Datenschutz muss durch juristische und technische Hürden, aber auch durch demokratische Verfahren geschützt werden.

Weichert kritisierte, dass bei der Weiterentwicklung des Datenschutzrechts die Betonung lange Zeit auf Maßnahmen lag und die Formulierung von Zielen vernachlässigt wurde. Dies habe auch zu einer Überregulierung im Detail geführt. Eine Modernisierung des Datenschutzrechts sei unbedingt erforderlich – ein Gutachten dazu, das Ende der 90er Jahre von Garstka, Pfitzmann und Rossnagel erstellt wurde, wanderte freilich zunächst einmal in die Schublade.

Als Herausforderungen für den Datenschutz im 21. Jahrhundert nannte Thilo Weichert die Marktfähigkeit, also die Sicht auf den Datenschutz als Wettbewerbsfaktor, den Zusammenhang des Datenschutzes mit dem Verbraucherschutz und die Auswirkungen von Kartellen (als Beispiel den Zusammenschluss von Google und Doubleclick). Große Bedeutung misst er Datenschutz-Audits mit entsprechenden Gütesiegeln bei.

Die Landesbeauftragte von Nordrhein-Westfalen, *Bettina Sokol,* sieht die Allgegenwart des Computers als große Herausforderung. Der Staat befinde sich auf dem Weg in einen Präventionsstaat, der alle Bürger unter Generalverdacht stelle – durch Maßnahmen wie biometrische Reispässe, die allgemeine Steuernummer, Video- und Telefonüberwachung und die geplante Online-Durchsuchung.

Burkhard Hirsch wies in seinem Vortrag auf den Grundrechtscharakter des Datenschutzes hin. Der Wunsch nach Daten der Bürger sei aber nicht erst mit dem 11. September entstanden – auch vorher gab es hier schon Begehrlichkeiten, sei es zur Terrorbekämpfung, sei es aus wirtschaftlichen Gründen.

Dem häufig vorgetragenen Satz: „Wer nichts zu verbergen hat, hat auch nichts zu befürchten", setzte er entgegen, dass jeder Mensch ein Privatleben habe, das andere nichts angehe. Wer nichts zu verbergen habe, habe wohl auch kein Privatleben – oder zumindest ein äußerst ereignisloses.

Auch auf das Argument, der Staat sei heute nicht mehr der Gegner, vor dem Bürger zu schützen seien, sondern Partner, der seinerseits den Bürger schützen solle, entgegnet er, dass staatliche Macht immer missbraucht werden könne und deswegen Schutzmechanismen notwendig seien. Er wies aber auch auf die Bereitwilligkeit vieler Bürger hin, intimste Details ihres Privatlebens in Blogs oder Talkshows preiszugeben – oft, ohne die Folgen zu bedenken.

Am Ende seiner Rede ging er auf die Ankündigung des Bundesverteidigungsministers ein, trotz klarer Rechtslage – aufgrund des Urteils des Bundesverfassungsgerichts – den Abschuss von Flugzeugen zu befehlen, wenn er eine entsprechende Gefährdungssituation als gegeben ansieht. Hirsch erklärte, dass der Minister in einem solchen Fall nicht nur zurücktreten, sondern vor Gericht gestellt werden müsse. In der Diskussion wurde die Frage gestellt, ob nicht bereits diese Ankündigung einen Straf-

tatbestand darstellen würde; diese Frage konnte im Rahmen des Vortrags aber nicht beantwortet werden.

Nach dem Mittagessen folgte ein Grußwort von *padeluun* vom FoeBuD, der Bundesinnenminister Schäuble dafür dankte, dass seine Politik die beste denkbare Werbung für den Datenschutz sei. Er machte dies am steigenden öffentlichen Interesse für die BigBrotherAwards und die erfolgreiche Demonstration gegen die Vorratsdatenspeicherung fest.

Eine etwas andere Position nahm *Reinhard Fraenkel,* der betriebliche Datenschutzbeauftragte von TollCollect ein. Er kritisierte die verbreitete Ansicht, dass Daten in der Privatwirtschaft stärker gefährdet seien als im öffentlichen Bereich. Unter der Überschrift „Zur Halbwertszeit der Zweckbindung" ging er auf den Schutz der und die Begehrlichkeiten nach den Daten ein, die bei der Mauterhebung auf Autobahnen anfallen. Trotz klarer gesetzlicher Regelungen, die eine strikte Zweckbindung vorsehen, wurde kaum eine Woche nach der Inbetriebnahme des Systems die erste Beschlagnahmeverfügung für die erhobenen Mautdaten erlassen. Dies hat sich seither trotz der eindeutigen Rechtswidrigkeit mehrfach wiederholt – nach seinen Worten ein Skandal. Er selbst hält aber die Öffnung der Zweckbindung in begrenzten Fällen, beispielsweise der Verfolgung schwerer Straftaten, für notwendig, da sich sonst ein moralisches Dilemma zwischen Datenschutz und Täterschutz ergebe. Gleichzeitig wies er den Vorwurf der Vollüberwachung des Straßenverkehrs durch TollCollect zurück – dazu sei das System überhaupt nicht geeignet.

Im zweiten Teil des Vortrags ging er auf die Konsequenzen der Vorratsdatenspeicherung ein, zugespitzt in der These: Durch die Vorratsdatenspeicherung wird der Datenschutz geschleift. Dies begründet er damit, dass durch die Vorratsdatenspeicherung tragende Säulen des Datenschutzes beseitigt werden, wie die Zweckbindung und die schnellstmögliche Löschung nicht mehr für den Erhebungszweck benötigter Daten. Zudem führe die Vorratsdatenspeicherung dazu, dass Profile einzelner Personen angelegt werden können, die über Bewegungsprofile weit hinausgehen und quasi die *soziale DNA* einer Person repräsentieren.

Er kritisierte aber auch einen weitgehenden Abstumpfungsprozess in der Bevölkerung gegenüber Fragen des Datenschutzes. Jeder von uns sei eine Gefahr für den Datenschutz. Fälle wie die Veröffentlichung von Fotos von Personen im Internet oder die Verbreitung von Be- und Verurteilungen von Lehrern müssten bei der Einschätzung und Weiterentwicklung des Datenschutzes berücksichtigt werden. Gleichzeitig kritisierte er die staatlichen Aufsichtsbehörden und Gerichte, die sich in der Rechtsauffassung oft nicht einig seien und gelegentlich die notwendige Kompetenz vermissen ließen. Seine Prognose zur Zweckbindung der Mautdaten: Eine Öffnung mit Richtervorbehalt wird kommen. Auch eine On-Board-Unit für Pkws könnte folgen.

Zuletzt berichteten *Hermann Josef Schwab,* SAP-Datenschutzbeauftragter, und *Sachar Paulus,* Chief Security Officer bei SAP, vom Datenschutz in ihrem Unternehmen und bei seinen Produkten. Sie berichteten von den Datenschutzvorkehrungen bei SAP R/3, die es zwar ermöglichen würden, die gesetzlichen Auflagen zu erfüllen, aber nur mit höherem Aufwand als es bei besseren Datenschutzvorkehrungen in der Software notwendig wäre. Kernaussage ihres Vortrags war der Hinweis, dass SAP letztlich Kundenanforderungen erfülle. Sobald Kunden entsprechende Anforderungen stellen und bezahlen würden, würden auch die gewünschten Datenschutzvorkehrungen in die Software eingebaut. Ohne diese expliziten Anforderungen nicht. Paulus überraschte das Publikum mit der Nebenbemerkung, er wünsche sich etwas weniger zögerliche Prüfungen der Gesetzeslage, wenn beispielsweise eine unmittelbare Gefahr für das Zentrum Frankfurts mit seinen vielen Menschen und Banken drohe.

Mit ihrem Vortrag endete der Datenschutztag.

Verleihung der BigBrotherAwards

Am Abend wurden im gut gefüllten Historischen Saal der Spinnerei die diesjährigen BigBrotherAwards in acht verschiedenen Kategorien verliehen.

Karin Schuler von der DVD hielt die Laudatio auf den ersten Preisträger in der Kategorie *Arbeitswelt:* die Novartis AG, die für ihre Bespitzelung von Mitarbeitern und die damit verbundene Missachtung von deren Persönlichkeitsrechten ausgezeichnet wurde. Novartis' martialische Motivationsrhetorik gegenüber den Mitarbeiterinnen und Mitarbeitern fand besondere Erwähnung: „Kill to win – no prisoners".

Preisträger in der Kategorie *Regional* ist die Behörde für Bildung und Sport der Stadt Hamburg, die ein zentrales Register für Schülerinnen und Schüler aufbaut, das mit dem Melderegister abgeglichen wird. Begründet wird dies mit der Möglichkeit, verwahrlosten Kindern – wie im Fall eines von den Eltern vernachlässigten und letztendlich verhungerten Mädchens – rechtzeitig helfen zu können. Tatsächlich werden durch den Abgleich jedoch Kinder ermittelt, die ohne Aufenthaltserlaubnis in Deutschland leben, mit der Folge, dass ihre Eltern sie aus Angst vor Abschiebung von der Schule nehmen. Dem vernachlässigten Mädchen hätte das Register ohnehin nichts genützt – der Fall war den Behörden bekannt. Dennoch wurde nichts unternommen. Laudator war Alvar Freude.

In der Kategorie *Wirtschaft* würdigte padeluun die Bemühungen der Deutschen Bahn AG, anonymes Reisen immer schwieriger zu machen. Für Reisebüros lohnt sich der Verkauf von Fahrkarten kaum noch, die Reisenden sollen sie am Automaten kaufen und dabei Kreditkartennummern und überflüssigerweise die BahnCardnummer hinterlassen. Für BahnCards werden umfassend Daten erhoben, und in die BahnCard 100 ist sogar ein RFID-Chip integriert. Das Foto auf der BahnCard zu verweigern ist aufwändig.

Große Hotelketten – Hyatt, Intercontinental, Mariott – wurden in der Kategorie *Verbraucherschutz* stellvertretend für viele andere ausgezeichnet für das Anlegen umfassender Datensammlung über ihre Gäste. Im Rahmen des *Customer Relationship Management (CRM)* werden persönliche Daten, aber auch Vorlieben und Verhaltensmerkmale wie die im Hotelzimmer konsumierten Pay-TV-Filme und Produkte aus der Minibar fest-

gehalten. So werden umfangreiche Informationssammlungen angelegt – vorgeblich, um dem Kunden einen besseren Service zu bieten. Um ihre Einwilligung bittet man die Gäste nicht. Rena Tangens vom FoeBuD hielt die Laudatio.

Den Preis in der Kategorie *Technik* erhielt die Karlsruher Firma *PTV Planung Transport und Verkehr AG* für ihr System, das die technische Grundlage für Kfz-Versicherungen auf der Basis *Pay as you drive* bildet. Dazu werden Fahrstrecken und Fahrverhalten per GSM und GPS überwacht und daraus die Versicherungsprämie errechnet. Es ergeben sich Bewegungsprofile der Autofahrer, aber auch die Einhaltung von Verkehrsvorschriften könnte damit kontrolliert – und perspektivisch sogar erzwungen – werden. Laudator war Frank Rosengart vom CCC.

Finanzminister Peer Steinbrück erhielt den Preis in der Kategorie *Politik* für die Einführung der lebenslang einheitlichen Steuer-Identifikationsnummer für alle Einwohnerinnen und Einwohner der Bundesrepublik. Sie entspricht der – vom Bundesverfassungsgericht verworfenen – Personenkennziffer. Die Kennziffer soll bereits Neugeborenen zugeteilt werden und 20 Jahre über den Tod hinaus gelten. Werner Hülsmann vom FIfF hielt die Laudatio.

Die vieldiskutierte Vorratsdatenspeicherung brachte Bundesjustizministerin Brigitte Zypries bereits den zweiten BigBrother-Award – in der Kategorie *Kommunikation* – ein. Zypries ignoriert die Rechtsprechung des Bundesverfassungsgerichts, das 1983 die Sammlung nicht anonymisierter Daten zu unbestimmten oder noch nicht bestimmten Zwecken als verfassungswidrig bezeichnet hat. Wegen dieser bereits zweiten Auszeichnung mit einem BigBrotherAward werden Zypries gute Chancen auf einen *Lifetime Award* eingeräumt. Laudator war Frederik Roggan, Humanistische Union.

In der Kategorie *Verwaltung und Behörden* wurde zuletzt Generalbundesanwältin Monika Harms von Rolf Gössner ausgezeichnet – für die von ihrer Behörde veranlassten Antiterror-Maßnahmen gegen G8-Gipfelgegner, bei denen unter anderem Geruchsproben von Verdächtigen genommen und im Briefzentrum Hamburg systematisch die Post kontrolliert wurde.

Rena Tangens vom FoeBuD hielt die Laudatio
Foto: Peter Ehrentraut,

Zur Überraschung vieler ging der große Favorit leer aus, Bundesinnenminister *Wolfgang Schäuble* wurde in diesem Jahr nicht ausgezeichnet. Man will die Debatte nicht durch Konzentration auf eine Person verengen; vor allem sind aber die Verdienste nicht zu unterschätzen, die sich der Innenminister durch seine überzogenen Forderungen um den Datenschutz erworben hat. Sie wurden von Rolf Gössner in einer *Nicht-Laudatio* ausführlich gewürdigt. Den *Publikumspreis* erhielt Generalbundesanwältin Monika Harms.

Leider glänzten auch diesmal die Geehrten durch Abwesenheit, niemand wollte den Preis entgegennehmen.

FIfF-Jahrestagung 2007 – Datensammelwut

Im grauen Blaumann des Datenverkehrs-Arbeiters und mit RFID-Detektor ausgerüstet eröffnete *padeluun* mit seinem Vortrag die diesjährige FIfF-Jahrestagung. Dabei ließ er nach kurzem *Scoring* vor allem das Publikum zu Wort kommen – in dem er die Frage stellte, wie die Wissenschafts-geprägte FIfF-Gemeinde *gute* und menschliche Elemente in die Wirtschaft und soziale Elemente in die Wissenschaft hineintragen könne. Die Meinungen dazu deckten ein breites Spektrum ab: Von grundsätzlichen Handlungsmaximen – „bei sich selbst anfangen", „mit gutem Beispiel vorangehen", „gesunden Menschenverstand einsetzen" und der Aussage, es sei immer möglich, sich richtig zu verhalten – über Fragen der wissenschaftlichen Herangehensweise – „andere Methoden", „Entwickeln von Metriken für moralisches Verhalten" – bis zu gesellschaftlichen Voraussetzungen – Machtfragen oder die Bedeutung von Verhaltenskodizes in unserer Gesellschaft – wurden viele Aspekte angeschnitten.

Schlüsselfrage ist letztlich die Bildung. Eine gesellschaftliche Sichtweise sei notwendig, bei der man sich *schämen müsse, kein Buch gelesen zu haben*. Grundsätzlich ist mehr Kritik an Fehlentwicklungen erforderlich, hier ist die Wissenschaft – aber nicht nur diese – gefragt.

In zwei *Arbeitsgruppen* wurden danach die Themen FIfF-Kommunikation und Kampagne gegen Datensammelwut behandelt. In der Arbeitsgruppe zur *FIfF-Kommunikation* ging es um nichts weniger als deren Zukunft – sehr wahrscheinlich wird Dagmar Boedicker als Redakteurin ab der Ausgabe 2/2008 nicht mehr zur Verfügung stehen. Es muss also eine neue Hauptredaktion gebildet werden.

Zunächst wurde die Frage diskutiert, wie die FIfF-Kommunikation künftig aussehen soll. Auf der Mitglieder-Mailingliste hatte es Befürworter einer Abschaffung der gedruckten Form der FIfF-Kommunikation und die Herausgabe eine reinen Web-Ausgabe gegeben. Im Gegensatz dazu sprachen sich alle Anwesenden für die Beibehaltung der Print-Ausgabe aus. Sie führe zu einer Bindung der Mitglieder an das FIfF und stelle einen *Anker* dar, der das FIfF sichtbar mache. Auch die periodische Erscheinungsweise und die Strukturierung in Themenheften solle beibehalten werden.

Diskutiert wurden sowohl die Form als auch der inhaltliche Anspruch: Er soll grundsätzlich beibehalten werden, führt aber auch dazu, dass potenzielle Autorinnen und Autoren abgeschreckt werden könnten. Auch der politische Charakter der Artikel wurde

diskutiert. Auch wenn von einer reinen Erscheinungsweise im Web abgesehen werden soll, werden doch einzelne Artikel und Abstracts aller Artikel heute schon im Web publiziert.

Aus der Arbeitsgruppe heraus erklärten sich einzelne Mitglieder bereit, die Redaktion der FIfF-Kommunikation künftig zu übernehmen, so dass sie auch in Zukunft erscheinen kann. (Siehe hierzu auch den Kurzbericht in diesem Heft.)

In der zweiten Arbeitsgruppe wurde eine *Kampagne des FIfF zur Datensammelwut* entwickelt. Dabei wurden Ziele und Forderungen formuliert: Zunächst soll eine solche Kampagne Aufmerksamkeit wecken und dann den Widerstand dagegen deutlich machen. Abgeleitet wurden auch Forderungen, insbesondere die Evaluation von Gesetzen hinsichtlich der zu erwartenden Schäden für Menschen, Gesellschaft und Demokratie. Gesetze sollen ein Verfallsdatum haben und nur verlängert werden, wenn die demokratisch beschlossenen Ziele erreicht sind, ohne parallel in der Gesellschaft inakzeptable Schäden zu verursachen. Auf dieser Basis soll die weitere Kampagne geplant werden.

Den Abschluss bildete der Vortrag von *Constanze Kurz* zum Thema Biometrie. Darin gab sie einen Überblick über die Entwicklungen der letzten Jahre in diesem Bereich. Obwohl die Einführung biometrischer Verfahren meist mit Sicherheitsargumenten – dem *Kampf gegen den Terror* – begründet wird, stehen auch starke wirtschaftliche Interessen dahinter, wie eine Studie der BITKOM zeigt.

Biometrische Verfahren sind für breite Einsatzgebiete vorgesehen. Neben dem biometrischen Pass, der vor allem die öffentliche Diskussion bestimmt, werden sie in Zugangssystemen aller Art genutzt und ihr Einsatz ist in Bankautomaten, Mobiltelefonen, ja fast überall denkbar. In den Hintergrund gerückt werden aber gerne die Probleme, die mit der Technik verbunden sind – Erkennungs- wie Sicherheitsprobleme. Kurz zeigte, wie einfach der Chaos Computer Club beispielsweise Systeme zu Erkennung von Fingerabdrücken umgehen konnte.

Fragwürdig sind die üblicherweise vorgebrachten Argumente Fälschungssicherheit und Terrorbekämpfung. Anfragen im Bundestag ergaben, dass die Anzahl der aufgedeckten Fälschungen bei Pässen, vor denen der verstärkte Schutz erforderlich sein soll, verschwindend gering ist. Bei aufgedeckten Planungen für terroristische Anschläge spielten Reisepässe bisher überhaupt keine Rolle. Auch die *inoffiziell* angestrebte wirtschaftliche Vorreiterrolle für die Herstellung biometrischer Pässe ist fraglich.

Folien von Constanze Kurz

Stefan Hügel

Stefan Hügel ist stellvertretender FIfF-Vorsitzender. Er arbeitet als IT-Berater und lebt in München.

Besonders problematisch wird das Thema, wenn man in die USA blickt. Die dortigen Datenbanken in der Folge des *Patriot Act* enthalten mittlerweile ca. 100.000.000 Datensätze; eine *Watchlist* unerwünschter Personen ca. 3.500.000 Datensätze. Der Abgleich mit dieser Datenbank bei der Einreise führte bisher zu ca. 34.000 Einreiseverweigerungen.

Noch beunruhigender ist in diesem Zusammenhang die DNA-Analyse. Seit 1998 existiert in Deutschland die DNA-Analyse- und Vorsorgedatei, in der DNA-Informationen von verurteilten Straftätern oder aus *freiwilligen* Massenuntersuchungen zur Ermittlung von Straftätern erfasst werden. Mittlerweile enthält auch diese Datenbank ca. 1.000.000 Datensätze; die Forderung nach der – heute noch verbotenen – Analyse von Erbgutinformation wird erfahrungsgemäß nicht mehr lange auf sich warten lassen.

Mitgliederversammlung

Bereits am Samstagvormittag hatte die *Mitgliederversammlung des FIfF* stattgefunden. Neben einer längeren Diskussion über die Situation des FIfF, auch seine schwierigen Finanzen, wurde dieses Jahr ein neuer Vorstand gewählt. Erfreulich war dabei, dass sich eine Reihe neuer Mitglieder zu einer Kandidatur entschlossen haben und gewählt wurden. Das FIfF wird in den nächsten zwei Jahren einen zwölfköpfigen Vorstand haben, bei dem die Arbeit wieder auf mehr Schultern verteilt werden kann als bei den acht Vorstandsmitgliedern der vergangenen Wahlperiode.

Mein persönliches Fazit: Es hat sich auf jeden Fall gelohnt, nach Bielefeld zu kommen. Besonders dadurch, dass man drei Veranstaltungen in unmittelbarer Folge besuchen konnte, gab es ein breites Spektrum von Sichtweisen und Diskussionen zum Thema Datenschutz, die eine gemeinsame Grundrichtung hatten.

Diese Presseerklärung wurde am 14. Oktober 2007 vom FIfF, der DVD und dem FoeBuD verschickt.

Bielefelder Erklärung

wider Überwachungs- und Datensammelwahn

Am 12. und 13. Oktober 2007 wurde Bielefeld zur deutschen Hauptstadt des Datenschutzes. Die Deutsche Vereinigung für Datenschutz (DVD) veranstaltete anlässlich ihres 30-jährigen Bestehens den Datenschutztag 2007. Am Abend desselben Tages verlieh der Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs (FoeBuD) die BigBrotherAwards 2007, die Oskars für Datenkraken. Tags darauf veranstaltete schließlich das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) seine 23. Jahrestagung unter dem Motto „Datensammelwut". Die drei Nichtregierungsorganisationen geben aus diesem Anlass die folgende gemeinsame öffentliche Erklärung gegen den Datensammelwahn und die immer stärkeren Überwachungstendenzen von Staat und Wirtschaft heraus.

Beim Telefonieren und beim Verschicken von SMS und E-Mail, mit jeder Überweisung und mit jedem Gebrauch von Kreditkarten, EC-Karten und Kundenkarten aller Art sowie durch Ausfüllen von ungezählten Online-Formularen hinterlassen die Menschen in Deutschland breite Datenspuren. Viele dieser Datenspuren lassen sich nicht mehr vermeiden, wenn man am politischen, wirtschaftlichen und sozialen Leben teilnehmen will. Das weckt Begehrlichkeiten: Staat und Wirtschaft gehen immer ungenierter mit diesen Daten um, erstellen Kunden-, Bewegungs- und Persönlichkeitsprofile, überwachen, kontrollieren, spähen aus und manipulieren. Die Privatsphäre und das Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts werden zunehmend eingeschränkt und missachtet.

In der Europäischen Union werden schon heute in vielen Ländern (und bald flächendeckend) die durch Telekommunikation entstehenden Verkehrsdaten mindestens sechs Monate gespeichert. Dies stellt Hunderte von Millionen Menschen unter den Generalverdacht, Telekommunikationseinrichtungen für kriminelle Zwecke zu nutzen.

Die US-amerikanischen Einwanderungsbehörden verlangen umfangreiche Datensammlungen über alle europäischen Fluggäste, bevor sie in den USA landen dürfen. Viele staatliche Einrichtungen in Deutschland, allen voran der Innenminister, tun es ihnen gleich und wünschen sich zweckverändernde Zugriffe z. B. auf Fluggastdaten, Autobahnmautdaten und private Videoaufzeichnungen. Sie gieren nach Überwachungskameras und heimlichen Online-Durchsuchungen, sie vermessen und katalogisieren uns mithilfe biometrischer Daten wie Fingerabdrücken, Gesichtsmerkmalen und DNS-Profil. Da erscheint es zur Erschließung der umfangreichen Datenbanken nur folgerichtig, dass uns eine Personenkennziffer verordnet wird, die uns von der Geburt bis über den Tod hinaus eindeutig identifiziert. Unter dem Vorwand, terroristische Gefahren abzuwehren, werden von staatlicher Seite immer neue Ideen zu Datensammlungen entwickelt und dabei die Einschränkung der Grundrechte systematisch und absichtsvoll betrieben. Ob solche Maßnahmen zu mehr Sicherheit führen, ist völlig ungewiss; dass sie die Freiheit beeinträchtigen, ist dagegen offensichtlich.

Die DVD, das FIfF und der FoeBuD fordern alle politisch Verantwortlichen auf, sich für die Erhaltung der Grundrechte einzusetzen, statt ständig zu versuchen, mithilfe angstschürender Schreckensszenarien den schleichenden Abbau wesentlicher demokratischer Errungenschaften zu rechtfertigen.

Hans-Jörg Kreowski

Bericht des FIfF-Vorstands

Es folgt eine schriftliche Zusammenfassung des Berichts, den ich als Vorsitzender auf der Mitgliederversammlung des FIfF am 13. Oktober 2007 im Namen des Vorstands mündlich vorgetragen habe. Berichtet wird über den Zeitraum von der 22. FIfF-Jahrestagung vom 3. bis 5. November 2006 in Bremen zum Thema „Alles hören, alles sehen, alles machen – dank Informatik" bis zur 23. Jahrestagung am 13. Oktober 2007 in Bielefeld zur „Datensammelwut" (und ein wenig darüber hinaus).

Die Bedeutung des FIfF

Da der Bericht auch die gravierenden Schwierigkeiten anspricht, in denen das FIfF steckt, sei vorab seine Bedeutung betont. Der Name FIfF ist Programm, weil es ein Forum bietet, auf dem sich alle Interessierten mit den vielfältigen Aspekten von Informatik und Gesellschaft auseinandersetzen können. Informatik ist ein aufregendes Fach sowohl als technische Disziplin als auch politisch und gesellschaftlich. Der Einsatz von Informations- und Kommunikationstechnik verändert seit Jahrzehnten massiv und nachhaltig die Arbeits- und Lebensbedingungen vieler Menschen, und das weder immer noch automatisch zum Guten. Hinzu kommt, dass gerade in letzter Zeit ein gewisser Teil der Politik Amok läuft und versucht, alle Barrieren des Datenschutzes niederzureißen. Gegenstimmen und Gegengewichte sind nötiger denn je. Das FIfF wird also im Konzert mit anderen Nichtregierungsorganisationen dringend gebraucht.

Das Übliche und mehr

Viele Mitglieder des FIfF sind im Berichtszeitraum mit verschiedenen Aktivitäten im Namen des FIfF und im FIfF-Kontext in Erscheinung getreten. Um einen Eindruck von der Vielfalt und Art der Beiträge zu geben und damit vielleicht auch zur Nachahmung oder phantasievollen Bereicherung anzuregen, werden sie als Journal aufgelistet. Für alle Einträge, die fehlen, weil sie mir entgangen sind, möchte ich mich entschuldigen. Gleichzeitig bitte ich um Hinweise auf alle Ereignisse und Aktivitäten, die im Journal vermisst werden, damit sie in der Webversion berücksichtigt werden können.

19. Dezember 2006: Weihnachtsvorlesung von Hans-Jörg Kreowski an der Universität Bremen zum Thema „Informatik in der Verantwortung – Verantwortung in der Informatik"

22. Dezember 2006: Brief des FIfF-Vorsitzenden im Namen der Mitgliederversammlung an den Bundespräsidenten und die Bundesregierung mit der Aufforderung, sich für die Leichenschändungen deutscher Soldaten in Afghanistan zu entschuldigen

22. Januar 2007: Gemeinsame Erklärung zur Vorratsdatenspeicherung, initiiert vom AK Vorratsdatenspeicherung, unterzeichnet von 27 Verbänden einschließlich FIfF

14./15. Februar 2007: Anmerkungen zum Denken und Fühlen informationstechnischer Systeme, Vortrag im Projekt Menschenbilder (MeBiT) von Wolfgang Hesse u. a., Europäische Akademie, Bad Neuenahr – Ahrweiler, Hans-Jörg Kreowski

10. März 2007, Bremen: *Vorträge von* Hans-Jörg Kreowski über „Was ist das FIfF?" und Ralf E. Streibl über „Krieg im Computerspiel", Jubiläumsveranstaltung „25 Jahre Neue Villa Ichon"

16. März 2007: Fachgespräch der Bundestagsfraktion der Grünen: „Modernisierung des Datenschutzes", Werner Hülsmann

16. - 18. März 2007, Dachau: FIfF-Klausur zur Organisationsentwicklung und Zukunftssicherung

23. März 2007: Zwei Artikel von Werner Hülsmann in der Broschüre des AStA der FH Münster „What the fuck is informationelle Selbstbestimmung": „Freiheit oder Sicherheit" (S. 54) und „Arbeitnehmerdatenschutz" (S. 60) sowie eine Kurzdarstellung des FIfF (S. 65), Download der Broschüre als PDF-Datei: *http://www.astafh.de/wp-content/uploads/2007/03/download.pdf*

18. April 2007, Venlo, Niederlande: Colloquium 'Applied Ethics – Participatory Design', Fontys Hogeschool, Dagmar Boedicker

27. - 29. April 2007, Berlin-Adlershof: Kontrolle durch Transparenz - Transparenz durch Kontrolle, Tagung des Fachbereichs Informatik und Gesellschaft der GI e. V., mit FIfF-Stand und FIfF-Beteiligung

8. Mai 2007: Unterzeichnung des Memorandum of Understanding (MoU) mit ICANN als zivilgesellschaftliche At-large-structure (ALS) in der European At-Large-Organization (EURALO). Anschließend Beteiligung an den Wahlen zum ALAC (At-large advisory committee) und zum EURALO-Vorstand

15. Mai 2007: Vortrag „Internet Governance" im Rahmen der Ringvorlesung „Informatik und Gesellschaft" der Fachschaft Informatik, Universität Karlsruhe, Stefan Hügel

16. Mai 2007: Arbeitsgruppe 'Informatik und Ethik', 35,0. Konferenz der Informatik-Fachschaften (KIF), Universität Karlsruhe, Stefan Hügel und Kai Nothdurft

16. Mai 2007: „Videoüberwachung durchschauen" – Ein Rundgang durch Berlin-Mitte mit Peter Bittner, veranstaltet durch den AK Videoüberwachung und Bürgerrechte des FIfF und den AK Überwachungstechnologien der GI

27. Mai 2007: ZDF-Beitrag zum Thema Videoüberwachung, u. a. mit Beiträgen von Peter Bittner. Redakteur: Ulrich Hansen (Redaktion Kultur und Wissen), Sendetermine: 27.05.07 9:00, ZDF, sonntags – TV fürs Leben; 29.05.07 13:30, 3sat, sonntags – TV fürs Leben (Wiederholung); Online-Artikel zum Beitrag von Ulrich Hansen:

http://www.heute.de/ZDFde/inhalt/30/0,1872,5541406,00.html (heute.de)

http://www.zdf.de/ZDFde/inhalt/30/0,1872,5541406,00.html (sonntags – TV fürs Leben); der Videostream des Beitrages ist in der ZDFmediathek unter dem Titel „Und was ist mit dem Datenschutz?“ zu finden unter: *http://www.zdf.de/ZDFmediathek/inhalt/21/0,4070,5541365-5,00.html*

30. Mai 2007: Pressemitteilung des FIfF: „Seminarlisten beschlagnahmt.... Erklärung von Joe Weizenbaum“ (im Zuge der bundesweiten Razzien am 9. Mai 2007 gegen Globalisierungskritiker waren auch Räume eines Wissenschaftlers durchsucht worden, und dabei hatten die Ermittler unter anderem Teilnehmerlisten aus Seminaren des Uni-Dozenten mitgenommen)

20. Juni 2007: Das FIfF gratuliert der DVD zum 30jährigen Bestehen, kurzer Beitrag für DANA Datenschutz Nachrichten 2/2007, Hans-Jörg Kreowski

10. Juli 2007: Presseerklärung zur Vorratsdatenspeicherung

16. Juli 2007: Presseerklärung des FIfF zur Verschärfung der Hackerparagraphen, Kai Nothdurft

15. September 2007: Ist Wissenschaftsförderung sozial?, zweistündiger Workshop auf dem 3. Bremer Sozialforum, Hans-Jörg Kreowski

22. September 2007, Berlin: Demonstration „Freiheit statt Angst“ mit über 15.000 Teilnehmerinnen und Teilnehmern, unterstützt vom FIfF

12. Oktober 2007, Bielefeld: Verleihung der BigBrotherAwards, unterstützt vom FIfF

13. Oktober 2007, Bielefeld: 23. FIfF-Jahrestagung zur „Datensammelwut“

14. Oktober 2007: Bielefelder Erklärung wider Überwachungs- und Datensammelwahn zusammen von DVD, FIfF und FoeBuD

23. Oktober 2007: FIfF opposes making TLS-authz an experimental standard

31. Oktober 2007, München: 29. GuHT-Forum „Überwachung – Schutz der Bürger oder Bedrohung ihrer Grundrechte?“, unterstützt vom FIfF

1. November 2007: Vortrag von Eva Hornecker über „Verantwortung im informatischen Berufsalltag – Warum es wichtiger ist die Arbeitskulturen informatischen Handelns zu reflektieren als über ethische Theorien und Whistleblowing zu reden ...“ im Fachschafts-Kolloquium über Gesellschaftliche Auswirkungen der Informatik, Fachbereich Informatik, Technische Universität Darmstadt

6. November 2007, Bremen: Demonstration unter dem Motto „Freiheit statt Angst – Für die Grundrechte!“, mitorganisiert von der FIfF-Regionalgruppe Bremen mit einem Redebeitrag von Hans-Jörg Kreowski

9./10. November 2007, München: „Datenschutz mit Augenmaß“, Klaus Köhler

Einige Ereignisse möchte ich noch zusätzlich kommentieren.

Dazu gehört die jährliche FIfF-Klausur im März, die in diesem Jahr wie schon im Vorjahr zwei Tage Zeit ließ, über die Weiterentwicklung des FIfF nachzudenken. Die Klausurtagung vom 28. bis 30. März 2008 in Bad Hersfeld soll die dritte Veranstaltung zur Organisationsentwicklung und Zukunftssicherung sein, wobei es diesmal nicht so sehr darum geht, Ideen zu entwickeln und Pläne zu schmieden, sondern mehr darum, was schon geschafft ist und was noch zu tun ist, um die Überlegungen aus 2006 und 2007 umzusetzen. Mitglieder, die Interesse haben, bei diesem Unterfangen mitzuwirken, können sich gern bei mir melden.

Von den diversen aufgeführten Aktivitäten scheint mir Peter Bittners Mai-Rundgang durch Berlin-Mitte zum Aufspüren von Videokameras bemerkenswert, weil es einmal nicht um einen Vortrag, einen Artikel oder eine Pressemitteilung geht. Wenn viele es ihm gleichtun, könnte allmählich ein flächendeckender Atlas der Videoüberwachung entstehen. Besonders erwähnenswert ist auch die Pressemitteilung vom 30. Mai 2007 „Seminarlisten beschlagnahmt ... Erklärung von Joseph Weizenbaum“. Denn sie war Anlass und Ausgangspunkt für die Herausgabe der Sonderausgabe der FIfF-Kommunikation „Wider den Zeitgeist“. Dieses Extraheft ist sicherlich ein Highlight der FIfF-Arbeit in diesem Jahr mit beachtlicher Außenwirkung. Alle Mitglieder mögen sich aufgefordert fühlen, das Heft breit zu verteilen.

FIfF und Geld

Das FIfF-Journal mit seinen kleinen und großen Ereignissen zeigt aus meiner Sicht durchaus, dass das FIfF präsent ist und auch Erfolge vorweisen kann. Da das nirgends explizit erscheint, sei hier darauf hingewiesen, dass bei vielen Aktivitäten des FIfF von Anja Riemer und Christian Lilienthal in der Geschäftsstelle wertvolle Arbeit im Hintergrund geleistet wird. Ohne sie wäre manches unmöglich. Aber das FIfF steckt auch in einigen Schwierigkeiten. Dazu gehören finanzielle Probleme.

Bis 2005 hat das FIfF Überschüsse angesammelt, die nach dem Rat von Finanzexperten systematisch abgebaut werden mussten, um die Gemeinnützigkeit nicht zu gefährden. Das ist 2006 geschehen mit der Herausgabe der Broschüren zur elektronischen Gesundheitskarte und zu RFID sowie der Neukonzeption der Webseiten. Was 2006 von allen Beteiligten übersehen wurde, war die Tatsache, dass die Differenz zwischen Einnahmen und Ausgaben sich nicht nur aus gezielten Maßnahmen zum Überschussabbau zusammensetzte, sondern auch rund 9.000 Euro zusätzliches Defizit enthielt. In diesem Jahr wird aller Voraussicht nach dieses Defizit ansteigen. Neben den sinkenden Einnahmen wegen der allmählich sinkenden Mitgliederzahl und steigenden Kosten aller Art ist die Differenz zwischen Einnahmen und Ausgaben vor allem dadurch begründet, dass das FIfF inzwischen Kosten für Layout und Redaktion der FIfF-Kommunikation im Umfang von 3.000 Euro pro Heft selbst bezahlen muss, die bis Mitte 2006 ganz und bis Anfang 2007 teilweise aus anderen Quellen von edlen Spendern abgedeckt wurden.

Die wichtigsten Zahlen für 2007 im Überblick:

Einnahmen (geschätzt)
33.000 Euro

Überschuss aus 2006
18.000 Euro

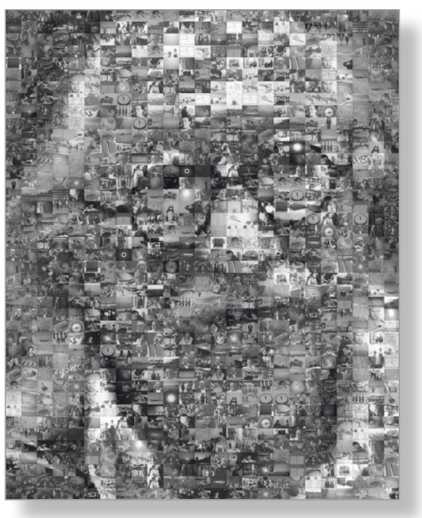
Ausgaben (geplant und geschätzt)
52.000 Euro

Das FIfF wird allerdings in diesem Jahr noch nicht ins Minus rutschen, weil durch Sofortmaßnahmen des Vorstands rund 3.000 Euro eingespart werden konnten. Aber die Zahlen offenbaren, dass dringender Handlungsbedarf besteht.

Die Optionen sind klar: Ausgaben senken und Einnahmen erhöhen. Bei den Ausgaben gibt es eigentlich nur zwei große Posten mit der Geschäftsstelle, die rund 13.000 Euro kostet, und der FIfF-Kommunikation, die mit rund 25.000 Euro zu Buche schlägt. Die Geschäftsstelle zu verkleinern, ist eigentlich nur schwer vorzustellen, ohne dass es erhebliche Einbußen bei der laufenden Arbeit gäbe. Kostensenkende Veränderungen bei der FIfF-Kommunikation müssen sehr sorgfältig bedacht werden. Die Zeitschrift ist das Aushängeschild des FIfF; daran zu rütteln, wäre kaum ratsam.

Vor allem aber die Einnahmeseite bietet Ansatzpunkte. Eine Spendensammlung ist bereits vom Vorstand angeschoben worden (siehe meinen Brief an das FIfF in der letzten FIfF-Kommunikation). Das erscheint mir eine nahe liegende Maßnahme, wenn die Mitgliedsbeiträge die Kosten nicht decken, obwohl nicht unbedingt angenehm ist, die Mitglieder über den regulären Beitrag hinaus um zusätzliche Spenden zu bitten. Entsprechend muss überlegt werden, ob die Mitgliedsbeiträge erhöht werden müssen. Ein Betrag von 100 Euro statt 60 Euro wäre in etwa kostendeckend, das klingt aber doch reichlich viel auf einmal. Vom Vorstand aus wird auf jeden Fall versucht, Förder- und Sponsorenmittel einzuwerben.

Über die finanzielle Entwicklung muss bis spätestens bei der nächsten Mitgliederversammlung Klarheit herrschen. Alle Mitglieder, die Vorschläge und Ideen haben, wie ein ausgeglichener Haushalt erreicht werden kann und sollte, mögen sich bitte an den Vorstand wenden. Auch Meinungsäußerungen zu den vorgeschlagenen Maßnahmen oder der Finanzmisere insgesamt sind natürlich willkommen.



DVD-Cover, Weizenbaum. Rebel at Work

FIfF und Engagement

Alle Mitglieder, die über die Mailingliste erreichbar sind, haben Anfang September den Brandbrief von Dagmar Boedicker erhalten, in dem sie sich vehement beklagt, dass zu wenige Mitglieder aktiv sind, deshalb zu wenig geschafft wird und die wenigen Aktiven sich aufreiben. Indizien dafür gibt es einige. Beispielsweise ist es seit Jahren äußerst schwierig, Freiwillige zu finden, die die Jahrestagungen organisieren. Da ist der Vorstand meist mehr involviert, als ihm lieb ist, und wofür er eigentlich auch nicht genug Kapazität hat. Die diesjährige Tagung hat bestens nach Bielefeld gepasst und insgesamt auch recht gut geklappt. Die Organisation aber war eher ein Notbehelf als beispielhaft.

Auf der anderen Seite ist aber vielleicht „Einsicht in die Notwendigkeit" gefragt, dass nämlich im Moment nicht mehr geht und wenig besser ist als nichts. Das hieße, die wenigen Aktiven machen, was sie können, ohne die Frustrationsgrenze zu überschreiten. Ich selbst gehe davon aus, dass die Lethargie über kurz oder lang überwunden wird. Denn die politischen Verhältnisse schreien geradezu nach einer Gegenbewegung.

Erfolgsmeldungen

Damit der Bericht nicht mit den aktuellen Problemen endet, habe ich mir zwei Erfolgsmeldungen aufgehoben.

Zwei FIfF-Mitglieder sind von der Gesellschaft für Informatik (GI) besonders geehrt worden. Veronika Oechtering und Andreas Spillner sind in diesem Jahr als GI-Fellows ausgezeichnet worden. Die GI würdigt damit Veronikas Engagement im Gender-Kontext und insbesondere ihre Organisation der Sommeruniversität *informatica feminale,* die in diesem Jahr zum zehnten Mal in Bremen stattfand. Die informatica feminale wird seit den Anfängen vom FIfF unterstützt. Andreas hat sich um das Thema Softwarequalität besonders verdient gemacht, aber auch sein gesellschaftliches Engagement wurde ausdrücklich gelobt, womit wohl u. a. gemeint sein muss, dass er die FIfF-Jahrestagung 2006 organisiert hat.

Der Film „Weizenbaum. Rebel at Work.", der von Peter Haas und Silvia Holzinger (Il Mare Film) produziert wurde, hatte am 17. November 2007 seine Premiere in Jena und wurde seitdem an über 20 Orten in Deutschland und Österreich vorgeführt (darunter in Bielefeld während der FIfF-Jahrestagung). Der 80-minütige Film zeichnet das Leben von Joseph Weizenbaum nach und zeigt die wichtigsten Stationen dieses Wissenschaftlers und Gesellschaftskritikers, der sicher das berühmteste FIfF-Mitglied ist. Wer mehr über den Film wissen und vielleicht auch eine Vorführung organisieren möchte, sei auf die Webseite *http://www.ilmarefilm.org* verwiesen.

Hans-Jörg Kreowski im Namen des alten Vorstands

Werner Hülsmann

Kampagne gegen Datensammelwut

Überregionale Arbeitsgruppe gegründet

Auf der diesjährigen Jahrestagung beschloss die Arbeitsgruppe Datensammelwut, *dass das FIfF eine Kampagne gegen die Datensammelwut initiieren sollte. Es gab viele Vorschläge für mögliche Arbeitsinhalte, die der neuen überregionalen Arbeitsgruppe als Basis dienen können.*

Nachdem unter den etwa zwanzig Teilnehmer/-innen Einigkeit bestand, dass es höchste Zeit für eine Kampagne des FIfF gegen die Datensammelwut ist, wurden Ziele formuliert. Die beiden wichtigsten:

- Aufmerksamkeit erregen
- Widerstand wecken

Weitere Ziele der Kampagne sollten sein:

- Breite Bevölkerungsschichten sensibilisieren
- Wirksamkeit der Maßnahmen hinterfragen, zum Beispiel, ob die angekündigten Überwachungsmaßnahmen erforderlich sind
- FIfF in die Öffentlichkeit bringen
- Verdeutlichen, dass der Widerstand gegen die Datensammelwut immer größer wird
- Gesellschaftliche Verantwortung aufzeigen
- Beratungskompetenz für Politik und Bürger/-innen aufbauen
- Alternativen aufzeigen
- Stimmung gestalten: Informationelle Selbstbestimmung ist cool

Forderungen

Anschließend wurden Forderungen erhoben, die von der Kampagne umgesetzt werden sollen:

- Informationspflichten verbessern: Verantwortliche Behörden bzw. Institutionen müssen Betroffene über die gespeicherten personenbezogenen Daten jährlich informieren.
- Das Informationsfreiheitsgesetz muss nachgebessert werden.
- Eine regelmäßige Überprüfung (Evaluation) der Wirksamkeit von Überwachungs- und Sicherheitsgesetzen muss verbindlich eingeführt werden. Entsprechende Gesetze sollen ein Ablaufdatum erhalten. Sie werden automatisch unwirksam, wenn keine Evaluation stattgefunden hat oder diese keine befürwortenden Ergebnisse erbracht hat.
- Kollateralschäden untersuchen, die die Überwachungs- und Sicherheitsgesetze bei Menschen, in der Gesellschaft und an der Demokratie bewirken (Gesetzesfolgenabschätzung analog zur Technikfolgenabschätzung).
- Das Bundesministerium für Bildung und Forschung soll entsprechende Studien fördern.

Maßnahmen

Nachdem Ziele und Forderungen formuliert waren, sammelten die Teilnehmer/-innen der Arbeitsgruppe Ideen für Aktionen und Maßnahmen:

- Katalog mit Fallbeispielen erstellen
- How To's (wie mensch sich vor Überwachung schützen kann) erstellen
- Multiplikatoren schulen
- Stadtführungen zur Videoüberwachung
- Vernetzung mit bestehenden Aktionen
- Bielefelder Erklärung zum öffentlichen Appell und/oder zur Online-Petition erweitern

Werner Hülsmann

Werner Hülsmann, Diplom-Informatiker mit Schwerpunkt Datenschutzrecht, Jahrgang 1961, Inhaber von *Datenschutzwissen.de* und selbstständiger Datenschutzberater, ist seit 2004 beim unabhängigen Datenschutzzentrum anerkannter Sachverständiger für IT-Produkte (rechtlich, technisch) und Kooperationspartner des virtuellen Datenschutzbüros. Er ist Vorstandsmitglied der Deutschen Vereinigung für Datenschutze (DVD) e.V, Bonn und des FIfF e.V., Bremen

- Wahlkreisabgeordnete anschreiben oder besuchen
- Drittmittelantragsteller/-innen aus der Forschung an Universitäten und Hochschulen unterstützen
- Kontakte zu anderen Fachdisziplinen herstellen, beispielsweise Psychologen und Soziologen
- Studien *vermarkten*
- Stiftungen und Sponsoren aus der Industrie *anzapfen*
- Audio- und Videopodcasts bereitstellen
- Schülerwettbewerb *Ich erforsche meine Stadt* zum Thema Überwachung initiieren
- Werbeplatz für Datenschutz-freundliche Firmen bereitstellen
- Beispiele für übertriebenen Sicherheitseifer sammeln und dokumentieren
- Das FIfF muss eine Experten-Organisation des Deutschen Bundestags werden!
- Lobbyarbeit

Handeln

Leider konnte in der Kürze der Zeit kein konkreter Handlungsrahmen entworfen werden. Die Arbeitsgruppe ging auseinander mit einem Arbeitspaket, das aus Zielen, Forderungen und Maßnahmen besteht und zum weiteren Handeln auffordert. Der Moderator der Arbeitsgruppe fand sich bereit, sich um die Koordination und Fortführung der Kampagne zu kümmern.

Aufruf

Interessierte Mitglieder und Nichtmitglieder, die in der überregionalen Arbeitsgruppe des FIfF zur Kampagne gegen die Datensammelwut mitwirken möchten, sind herzlich eingeladen, sich unter http://lists.fiff.de/mailman/listinfo/kampagne-gegen-datensammelwut in die Mailing-Liste der Arbeitsgruppe einzutragen. Für Rückfragen oder Angebote mitzuarbeiten (gerne auch bei der Koordination) steht das Vorstandsmitglied Werner Hülsmann (E-Mail: werner@fiff.de) zur Verfügung.

Dagmar Boedicker

AG FIfF-Kommunikation

auf der Jahrestagung 2007

Wer die Diskussion auf der FIfF-Mitgliederliste verfolgt hat (Anmeldung über http://lists.fiff.de/mailman/listinfo/mitglieder) weiß es schon: Die FIfF-Kommunikation wird im Lauf des nächsten Jahres in andere Hände übergehen. Damit die Übergabe möglichst reibungslos abläuft und die neuen Ideen gute Startbedingungen vorfinden, haben sich auf der Jahrestagung 16 Teilnehmer/-innen zu einer Arbeitsgruppe zusammengesetzt, Bilanz gezogen und Anregungen gesammelt. Sebastian Jekutsch, Redakteur der FIfF-Kommunikation, hat die AG moderiert.

Was die Leser an der FIfF-Kommunikation schätzen

Alle 16 Teilnehmer/-innen stimmten darin überein, dass für die Reputation der einzigen deutschsprachigen Zeitschrift ausschließlich zum Thema „Informatik und Gesellschaft" (IuG) eine Print-Ausgabe wertvoll und erhaltenswert ist. (Dieser Konsens ist wohl nicht repräsentativ, wie Stimmen auf der FIfF-Mitgliederliste gezeigt haben.) Die Anwesenden finden verschiedene Aspekte der gedruckten Ausgabe vorteilhaft, so die Möglichkeit, an jedem beliebigen Ort, auch unterwegs darin zu lesen. Sie schätzen die Zeitsouveränität beim Lesen, die Dauerhaftigkeit gegenüber einem flüchtigeren Online-Angebot, haptisches Vergnügen, einfachere Archivierung über lange Zeiträume, ... Allerdings vermissten manche die Möglichkeit, auf zurückliegende Ausgaben online zugreifen zu können.

Viele legen Wert darauf, dass die FIfF-Kommunikation periodisch erscheint. Auch die Bündelung in Schwerpunkten ist mehrheitlich gewünscht. Ich habe in der AG dargestellt, dass sie auch aus der Notwendigkeit entstand, die kleine Hauptredaktion zu entlasten.

Darf ich einige lobende Zitate aus den Stellungnahmen zitieren?

- Die FIfF-Kommunikation ist seriös,
- dient der Verankerung im Verein,
- kann als Vehikel für weitere Aktionen dienen,
- ist ein Archiv von IuG-Themen,
- profilbildend und als Werbemittel mit Außenwirkung geeignet,
- sie ist keine reine Nachrichtensammlung.

Was sie vermissen

Viele vermissen eine vollständige Online-Ausgabe; es kam der Vorschlag, sie den Abonnenten parallel zur gedruckten Ausgabe gegen einen kleinen Aufpreis anzubieten. Vergriffene Ausgaben werden gewünscht, sie sollten vollständig als PDFs verfügbar sein. Aus urheberrechtlichen Gründen dürfte sich das als unmöglich erweisen, die schon länger geplante Umstellung auf Creative-Commons-Lizenz drängt für die Zukunft.

Eine Vielzahl von Themen fehlt, am besten in einem Mix von wissenschaftlichen, Nachrichten- und anderen Texten. Die FIfF-Kommunikation soll mehr auf nicht-akademische Adressaten zugehen.

Bei den Schwerpunkten bleiben ganz eindeutig Wünsche offen: Sie müssten stärker fokussiert und nicht zu klein sein sowie Praxisberichte enthalten. Sebastian als der Zuständige für die Aufnahme in die Website wünscht sich einen Automatismus für das Einstellen von Beiträgen.

Die Autoren werden in Zukunft die Stichworte für die Verschlagwortung schon bei der Absprache ihrer Beiträge erhalten, und Abstracts sollen schon vor Erscheinen der FIfF-Kommunikation auf die Website.

Weitere Wünsche: die FIfF-Kommunikation auf *Ehrensenf* vorstellen, eine bessere interne Vernetzung durch das Heft und mehr Aktualität durch eine Online-Ausgabe/Blog/Vernetzung/News auf der FIfF-Website.

Vor einschneidenden Änderungen, vor allem Erweiterungen, sind Kosten und Nutzen abzuwägen. Der zukünftigen Redaktion und wohl auch dem Vorstand wird es nicht erspart bleiben, sich weitere Gedanken zu Wirtschaftlichkeit von und zur besseren Recherchierbarkeit für die FIfF-Kommunikation und die Website zu machen.

All das macht richtig viel Arbeit, einige Helferinnen und Helfer haben sich gefunden, wir wünschen ihnen viel Erfolg!

Umstritten ist

Es gab unterschiedliche Auffassungen schon unter der kleinen Schar der Anwesenden: Manche/r hätte die FIfF-Kommunikation gern dünner, manche/r gern dicker, einige nehmen sie, wie sie kommt. Manche möchten vier Ausgaben, anderen genügen auch weniger. Weniger Ausgaben bringen sicher Ersparnisse, interessanterweise am wenigsten bei den Portokosten, denn die steigen bei weniger Ausgaben. Bei geringerer Auflage hält sich die Ersparnis leider in Grenzen, Layout und Redaktion werden nicht weniger aufwändig und billiger.

Zum wissenschaftlichen Anspruch, den die FIfF-Kommunikation bisher eigentlich nicht erhoben hat, verweise ich auf die Diskussion auf der FIfF-Mitgliederliste.

Eine warnende Stimme wies darauf hin, dass der Wunsch, eine bessere interne Vernetzung und mehr Aktualität anzubieten, von *einer* Redaktion wohl nicht zu leisten wäre. Wir bräuchten wohl zwei, eine Online- und eine Print-Redaktion. Die Frage ist: Können wir zusätzliche Arbeit in eine Online-Ausgabe stecken?

Finanzierungsvorschläge und Ideen

Ob Abonnenten und Mitglieder wohl mehrheitlich bereit wären, auf die Print-Ausgabe zu verzichten? Das würde Porto sparen, die nicht verschickten Exemplare könnten wir für die Werbung nutzen.

Sollten wir Anzeigen akquirieren? Dagegen gab es eine Gegenstimme und einige Zweifel.

Koop-Angebote

Carsten Büttemeier wird einen Vorschlag zu einer interaktiven FIfF-Kommunikation formulieren und an die Hilfswilligen schicken. Das ist kein Geheimwissen – auch andere Interessierte können diesen Vorschlag natürlich erhalten.

Dietrich Meyer-Ebrecht wird einen Wiki-Zugang für alle Helferinnen und Helfer einrichten.

Leserbrief

FIfF-Kommunikation: Schlechtes Gewissen oder Ruhekissen

Hallo liebe Liste,

auch bei mir liegt die FIfF-Kommunikation als mahnende Erinnerung an die Möglichkeit einer besseren Welt regelmäßig auf dem Fenstersims im Badezimmer.

Ich weiß, wie viel Aufwand und Herzblut die Veröffentlichung jeder einzelnen FIfF-Kommunikation kostet. Ich weiß wie viel Mühe es bedeutet, die Beiträge zu einem Themenschwerpunkt zusammenzukratzen und zu redigieren. Ich habe eine hohe Achtung vor allen, die das auf sich nehmen. Dennoch oder gerade deswegen behaupte ich:

Die FIfF-Kommunikation ist mit ihren Inhalten, ihrer Form und dem jeweiligen Entstehungsprozess Teil des Problems und nicht der Lösung. Ich möchte deshalb die von mir in einer vorhergehenden Mail formulierte Leitlinie angepasst als Argumentationshilfe verwenden:

FIfF-Ko gewaltfrei radikalisieren, FIfF-Ko entprofessionalisieren, FIfF-Ko entwissenschaftlichen:

- Mit weniger Aufwand mehr erreichen
- FIfF-Ko präsenter machen.

1. FIfF-Ko radikalisieren: Die FIfF-Ko ist trotz ihrer hochpolitischen Inhalte keine politische Zeitschrift (mehr). Sie provoziert nicht, sie eckt nicht an. Eine Zeitschrift, die nicht Themen der politischen Debatte setzt, sondern ihnen allenfalls mit bis zu 20 Jahren Verzögerung nachrennt, ist nicht politisch. Nur durch mehr Radikalität besteht die Chance, die Wahrnehmung der FIfF-Ko außerhalb des FIfF positiv zu nutzen.

2. FIfF-Ko entprofessionalisieren: Wer als potentieller Autor die FIfF-Ko liest, bekommt einen Professionalitätsschock. Aufwand und Qualitätsansprüche an Artikel sind wirklich oder scheinbar hoch – zu hoch. Der redaktionelle Aufwand ist sicher zu hoch. Auch die Länge der Artikel schreckt Leser und Autoren ab - mir z. B. würde die eine oder andere einseitige(!) politische Sottise mehr gefallen.

3. FIfF-Ko entwissenschaftlichen: Die FIfF-Ko enthält viele Artikel echter oder scheinbarer wissenschaftlicher Qualität – ohne tatsächlich und auch im redaktionellen Prozess wissenschaftliche Qualität sicherzustellen. Ich kenne die Innereien von z. B. Berufungskomissionen: Wer glaubt, ein FIfF-Ko-Artikel gäbe mehr als ein paar Fleißpünktchen, täuscht sich. Sorry, wenn ich das so hart sage: Auch die wirtschaftliche Lage rechtfertigt nicht den Versuch, die FIfF-Ko als Karrierehilfsmittel zu instrumentalisieren. Wem's nebenher nutzt – schön, aber einen solchen Anspruch an die FIfF-Ko zu formulieren, ist nicht zulässig.

Um zum Badezimmer als Ausgangspunkt dieser Reise zurückzukehren. Wie ihr an der Abkürzung merkt, habe auch ich ein positiv affektives Verhältnis zur FIfF-Ko. Deswegen lese ich trotzdem regelmäßig nur das Inhaltsverzeichnis und Dagmars Editorial.

Liebe Grüße,

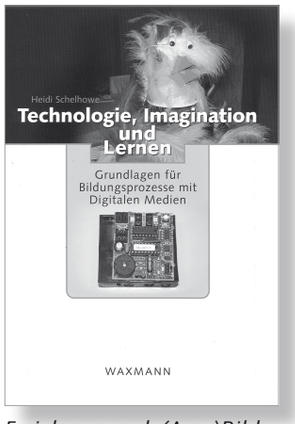
Jens (Woinowski)

Anmerkung der Redaktion:
Dies ist ein Beitrag von Jens zur Diskussion über die FIfF-Kommunikation auf der FIfF-Mitgliederliste, den wir als Leserbrief veröffentlichen.

Lesen -
Neues für den Bücherwurm

Dagmar Boedicker

Bildungsprozesse
Technologie, Imagination und Lernen



Dieses Buch „handelt von den Aufregungen und Turbulenzen, die Digitale Medien in die Welt des Lernens bringen. [...] ihr[em] Potenzial, unsere Gedanken und Imaginationen nicht nur zu speichern und zu vermitteln, sondern sie weiter zu entwickeln, kontrolliert durch Regeln, die sich verselbstständigen in Automaten, sich unserer direkten Kontrolle entziehen, ...“ Es richtet sich an Menschen, die sich mit der Erziehung und (Aus-)Bildung von Kindern und Jugendlichen beschäftigen oder beschäftigen werden, aber auch an Software-Entwickler und Informatiker beiderlei Geschlechts. Es stellt neue und interessante Fragen, die den Hype des Computereinsatzes in Bildungsprozessen überlebt haben, und befasst sich mit den veränderten Bedingungen des Lernens, mit Lernkulturen, neuen Inhalten und Gestaltungsanforderungen an die digitalen Materialien für eine neue Art des Lernens.

Bildung und Bildungspolitik

Wie die Autorin in der Einleitung feststellt, hat

> *„Bildung [...] mit der Entwicklung des Subjekts zu tun, mit Ausbildung von Gemeinschaftlichkeit, mit dem Verhältnis zur Welt. Digitale Medien sind Medien, mit denen Kinder und Jugendliche ihre Identität erproben und neu erfahren, ihre Communitys strukturieren und über die sie sich Welt definieren. Diese Welt aber hat sich, ebenso wie unsere Kommunikationen, durch die ‚intelligenten' oder ‚interaktiven' Automaten verändert. [...] Schulen und Hochschulen sowie Bildungspolitik haben mit verschiedenen Maßnahmen darauf reagiert: Viel Geld ist in Hardware und Software für die Bildungseinrichtungen und in das ‚E-Learning' geflossen. [..] Gleichzeitig werden Stimmen laut, die sagen, schulischer Un-*

terricht müsse wieder vom Computer befreit werden, die Kinder säßen in ihrer Freizeit schon zu viel vor dem Bildschirm, Schule solle sich wieder auf traditionelle Bildungsaufgaben besinnen." (S. 9)

In diesem Spannungsfeld entwickelt Schelhowe ihr Plädoyer für ein neues, zeitgemäßes Lernen und Lehren.

Zum Inhalt

Kapitel 1 behandelt die Reaktionen von Jugendlichen auf die Neuen Medien, ihre Reaktion auf und den Umgang mit dem Computer und damit, wie sie ihn sich aneignen.

Kapitel 2: Das digitale Medium – was ist neu daran, und wo sind seine versteckten Potenziale?

Kapitel 3: Wie reagieren die Bildungsinstitutionen bislang darauf?

Kapitel 4 bis 6: Experimente und Erkenntnisse der Gruppe *DiMeB (Digitale Medien in der Bildung, Universität Bremen)* zur Rolle der digitalen Medien in Bildungsprozessen.

Kapitel 7: ... keineswegs abschließende Einsichten, und ob sie sich verallgemeinern lassen. In diesem letzten Kapitel stellt die Autorin den Bezug zwischen dem Medium und der Pädagogik noch einmal zusammenfassend heraus und beschreibt ein anzustrebendes Zusammenwirken von technischer und pädagogischer Kultur.

ZIM@School und andere Projekte

Schelhowe zitiert verschiedene Studien und Projekte, die den Prozess untersuchen, den das Lernen von jungen Menschen durchläuft, seit zu Gedrucktem, Filmen und Ton auch der Computer und das Internet getreten sind. Sie beschreibt Veränderungen im Lernen, denen sinnvollerweise auch Veränderungen im Lehren folgen sollten.

„Computerprogramme üben auf Jugendliche ihren Reiz gerade dadurch aus, dass sie als eigenes Gegenüber erfahrbar werden, mit einer (im Prinzip) logischen, aber doch nicht vollständig durchschaubaren Struktur und einer komplexen Reaktion auf das eigene Verhalten." (S. 26)

„Die gängige Lehrpraxis an (deutschen) Schulen passt nicht zu der Art von Lernen, bei der sich Computerfertigkeiten ausbilden. Computerfertigkeiten werden durch von subjektivem Interesse ausgelöstem, Learning by Doing' entwickelt." (S. 29)

Weil Computer sich nicht ausschließlich logisch-rational durchdringen lassen, ist neben dem systematischen Vorgehen diese spielerische Herangehensweise mit Intuition und wachsender Erfahrung auch für die Ausbildung von Informatikern außerordentlich wichtig.

„Wenn man sich erstmal eingelassen hat, treibt die komplexe Technik selbst weiter, lässt Neugierde entstehen und bewirkt weiteres Lernen, alleine und im Kollektiv." (S. 29)

Schülerinnen und Schüler trennen nicht zwischen Spielen und Lernen, die Übergänge sind fließend.

„Schüler: Videospielen am Computer, das ist schon ein Teil der Freizeit geworden. Hausaufgaben mach ich auch am Computer, Referate, oder so. Das kann man sich eigentlich schon schlecht mehr wegdenken. Frage: Woran denkt ihr denn, wenn ihr an Computer denkt? Schüler: (Lachen) Chatten, spielen, sowas halt." (S. 25)

Vorteile der Neuen Medien

Jugendliche erleben sie als „gesellschaftlich wirksame und machtvolle Technologien, die Veränderungen der alten Welt hervorrufen." Sie erproben neue Lernformen und empfinden dabei die unterschiedlichen Wissensquellen als gleichwertig, sie genießen den Zugang zu ganz verschiedenen Inhalten und Formen. Ihre Vertrautheit mit dem Medium verleiht ihnen eine „Bewusstheit eigener, von Erwachsenen unabhängiger Macht".

Lernen findet nicht mehr nur in der Schule statt, Wissen ist vernetzt und nicht auf den eigenen Kulturkreis beschränkt. Die Grenzen zwischen Lernen, Arbeit und Spiel verschwimmen, ganz besonders für Jugendliche. Daraus ergibt sich aber auch eine neue Beziehung zwischen Bildung und Lebenswelt. Der Freiraum neben der Lebenswelt, in dem Handlungen wiederholt und Fehler gemacht werden dürfen, in dem das Handeln zeitweise zweckfrei sein darf und Menschen sich den „Luxus der Erkenntnis, der Entwicklung der eigenen Persönlichkeit gönnen" dürfen, dieser Raum für Entwicklung erscheint der Autorin heute besonders wichtig.

Über die Bildungsinstitutionen urteilt Heidi Schelhowe, dass „ihre schon in früherer Zeit häufig kritisierten Funktionen als Disziplinierungsanstalten für die Taylorisierte Arbeitswelt und als Informationslieferanten überholt sind." Vielmehr müssten sie die Funktionen erfüllen, die die Pädagogik schon immer betont hat: „die Orientierung auf Persönlichkeitsentwicklung, auf Sozialität, auf die Fähigkeit zur gesellschaftlichen Mitgestaltung." Das Medium muss als Inhalt und Raum wahrgenommen werden, *benutzt* und hinterfragt, nicht nur *genutzt* werden.

Schelhowe, Heidi: Technologie, Imagination und Lernen, Waxmann Verlag Münster/New York/Berlin/München 2007. ISBN 978-3-8309-1780-9, 192 Seiten brosch., 19,90 Euro

Sebastian Jekutsch

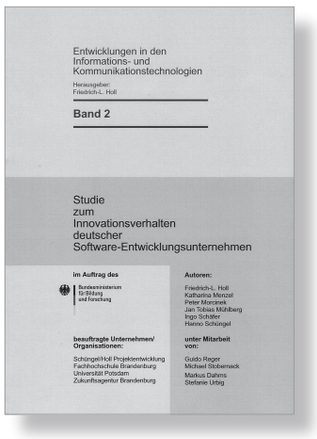
Studie zum Innovationsverhalten deutscher Software-Entwicklungsunternehmen

Angenommen, Sie seien Leiterin einer Software-Entwicklungsabteilung. Würden Sie auf die Frage „Sind Sie innovativ?" mit Nein antworten? Wahrscheinlich nicht. Ein Verdienst der hier vorgestellten Studien von Holl et. al. ist es festzustellen, dass

- sich in der Tat fast alle für innovativ halten,
- die Unternehmen an Innovativität allerdings geringe Maßstäbe ansetzen und
- sie diesen geringen Ansprüchen in der Praxis trotzdem kaum entsprechen, trotz aller Bekundungen.

Festgestellt haben die Autoren dies durch Befragungen, mittels Interviews und eines Online-Fragebogens. Der Trick der Forscher war es, anhand detaillierter Fragen Widersprüche zwischen Anspruch und Wirklichkeit aufzudecken. Etwa Folgendes:

- Einerseits sieht eine große Mehrheit der Befragten Software-Engineering als wichtig an, andererseits wendet ein Viertel von ihnen keinerlei entsprechende Techniken an.
- Einerseits kennen viele Unternehmen die Relevanz eines guten Marketings, andererseits sehen sie besonders hier eine ihrer zentralen Verbesserungsnotwendigkeiten.
- Einerseits werden vor allem kleine Unternehmen kritisiert, ihre Produkte änderten sich einzig auf Wunsch der Kunden, andererseits sind auch große Unternehmen kaum bereit, Ideen von außen aufzunehmen, z.B. durch Kooperation mit wissenschaftlichen Instituten.



Innovation wird von Führungspersonal oft lediglich als *Veränderungen am Produkt* verstanden, nicht als *Entwicklung einer neuen Idee zur Produktreife*. Die Unternehmen konzentrieren sich vor allem auf ihr Tagesgeschäft. Zur Innovation gehören aber auch Ideenförderung, Marketing, Beobachtung der Forschung, externe Kooperation und Risikobereitschaft, und vor allem in diesen Punkten haben nur wenige deutsche Softwareunternehmen Substanzielles vorzuweisen, dies durchaus auch große Firmen mit einem vermeintlichen Polster.

Ein interessanter Schwerpunkt der Studie sind Erkenntnisse zum Stand des Software-Engineering in der Praxis.

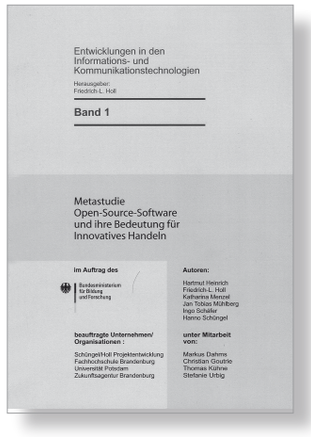
Die Studie ist gut lesbar, wenn auch oft trocken und länglich, der wissenschaftlichen Nachvollziehbarkeit geschuldet. Am interessantesten sind die Zusammenfassungen und Schlussfolgerungen am Ende des Buchs. Holl et.al. haben auch einige Vorschläge, wie sich die doch eher ernüchternde Situation verbessern könnte, Innovationsoffensive hin und her: Wen die Vorschläge interessieren, der sollte sich diese Studie besorgen.

Friedrich-L. Holl u.a.: Studie zum Innovationsverhalten deutscher Software-Entwicklungsunternehmen, 2006 Eigenverlag, Berlin, ISSN 1863-5016, 221 Seiten brosch. Online: http://www.innovationsanalysen.de/de/download/Innovationsverhalten_deutscher_SW-Entwicklungsunternehmen.pdf

Dagmar Boedicker

Metastudie

Open-Source-Software und ihre Bedeutung für Innovatives Handeln



Diese Metastudie hat mit gut 800 Literaturstellen eine Vielzahl von Veröffentlichungen und grundlegenden empirischen Untersuchungen analysiert, die sich mit Open-Source-Software (OSS) befassen. Es geht um die Frage, ob Open-Source-Software ein Motor für Innovationen ist, und ob sie in den kommenden Jahren wesentlich wichtiger werden könnte. – In einem weiteren Band haben die Wissenschaftler Ergebnisse ihrer Untersuchung zum Innovationspotenzial deutscher Software-Entwicklungsunternehmen veröffentlicht. In diese Untersuchung sind auch empirische Daten dazu eingeflossen, wie weit deutsche Software-Entwicklungsunternehmen bereit sind, Open-Source-Software einzusetzen und zu fördern (siehe die vorangehende Rezension von Sebastian Jekutsch). Es ist im Software-Bereich inzwischen fast unumstritten vorteilhaft, Open-Source zu nutzen, anders sieht es mit der Produktion aus. Sie erscheint weder den befragten Unternehmen als praktikable Geschäftsidee noch den Förderagenturen, die sich in ihren Projekten meist vorwiegend am Return on Investment orientieren. – Die OSS-Metastudie kommt zum Ergebnis, dass es sehr wohl Methoden und Prozesse im Umfeld der Open-Source-Software gibt, die auch für die kommerzielle Software-Entwicklung Innovativität, Wettbewerbs- und Zukunftsfähigkeit steigern könnten.

Was ist Innovation überhaupt?

Innovation mag ein Modebegriff sein, trotzdem ist sie natürlich mehr als das. Innovation ist überlebensnotwendig für Deutschland, ein Land, das nur mit sinnvollen, überlegenen Produkten seinen Mangel an Rohstoffen ausgleichen kann.

Die Autoren der Studie zitieren die folgende Definition und Klassifizierung des Innovationsbegriffs von Klincewicz (2004):

> *„So kann ein Produkt komplett neu sein, also ohne ein existierendes vergleichbares Produkt, es kann für das Unternehmen neu sein, auf einem neuen Markt [...] angeboten werden, oder – speziell im Bereich der Software-Industrie – für eine neue Plattform (ein neues Betriebssystem) angeboten werden. [...] Eine Innovation kann sich auch ausschließlich auf den Herstellungsprozess beziehen. Die Neuartigkeit muss also von den beteiligten Personen als solche wahrgenommen werden, nicht ausschließlich von den Kunden.“ (S. 88)*

Wie können OSS und proprietäre Software innovativer werden?

In sieben Kapiteln suchen Autorin und Autoren nach Antworten auf diese Frage.

Kapitel 1: Inwieweit befördert Open-Source-Entwicklung innovatives Handeln?

Kapitel 2: Wo und in welchem Maß wird Open-Source-Software vorrangig und wirtschaftlich sinnvoll eingesetzt?

Kapitel 3: Welche Methoden begünstigen den Einsatz von Open-Source-Software, und welche möglicherweise innovationssteigernden Effekte folgen daraus? Welche Auswirkungen hat das auf Verlässlichkeit, Wartbarkeit und Weiterentwicklung? Wie sicher ist Open-Source-Software?

Kapitel 4: Beeinflussen Projektstruktur, Organisation der verteilten Arbeit und Entscheidungsstrukturen die Arbeitseffizienz und Motivation der Entwickler?

Kapitel 5: Welche rechtlichen Rahmenbedingungen für Produktion und Vertrieb von Open-Source-Software sind in Deutschland und der EU wirksam?

Kapitel 6: Hier geht es um den Innovationsbegriff.

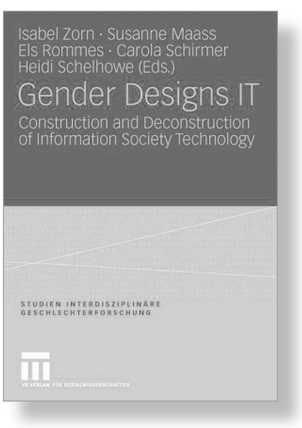
Kapitel 7: Fazit zu Vorteilen, Nachteilen, Chancen und Risiken von Open-Source-Software, ihrer Innovativität und der potenziellen Übertragung in die Praxis.

Holl, Friedich-L. (Hrsg.): Metastudie. Open-Source-Software und ihre Bedeutung für Innovatives Handeln, Eigenverlag /Berlin/ 2006. ISSN 1863-5016, 156 Seiten brosch.

Gerlinde Schreiber

Gender Designs IT

Construction and Deconstruction of Information Society Technology



Wie passen Gender *und* IT *zusammen? Informationstechnologie hat kein Geschlecht – so lautet die gängige Meinung. Doch beim Blick in unsere alltägliche Umgebung, in Filme und Werbung sehen wir: Technikkompetenz ist eine männliche Eigenschaft. Informationstechnik hat ein Geschlecht, und so lohnt der Blick aus Gender-Perspektive auf die IT. Genau dies unternehmen die Herausgeberinnen Isabel Zorn, Susanne Maass, Els Rommes, Carola Schirmer und Heidi Schelhowe im gerade erschienenen Buch „Gender Designs IT". Der Band baut auf Beiträgen zum Internationalen Symposium „GIST – Gender Perspectives Increasing Diversity for Information Society Technology" auf (Bremen, 2004) und stellt diese aktualisiert und strukturiert zusammen. Die Autorinnen bringen einen vielfältigen Hintergrund vornehmlich aus Informatik und Sozialwissenschaften mit.*

Die Herausgeberinnen strukturieren die Beiträge in die Rubriken

- Education and Empowerment
- Construction
- Deconstruction and Analysis.

Education and Empowerment stellt verschiedene Projekte zur gendergerechten Wissensvermittlung in der IT vor, inhaltliche Stichworte hierzu sind Game Design, Robotik, Webdesign und e-Learning.

Construction schildert den gegenwärtigen Zustand verschiedener Errungenschaften der IT (Call-Center, Netzwerke) und hinterfragt ihre Auswirkungen auf die gesellschaftliche Realität. Beispiel: Inwieweit wird die technische Ausgestaltung von Call-Center-Arbeitsplätzen den Ansprüchen an die Tätigkeit gerecht? Inwieweit sorgt diese technische Ausgestaltung selbst wiederum für den geringen Entscheidungsspielraum und das geringe Sozialprestige der Call-Center-Tätigkeit?

Analysis and Deconstruction untersucht aktuelle Entwicklungen in der IT (wie die Durchdringung des Alltags mit unsichtbarer Informationstechnologie), die Annahmen, die diesen Entwicklungen zu Grunde liegen und die Auswirkungen, die die Festschreibung dieser Annahmen durch die IT mit sich bringt.

Der Band führt unterschiedlichste Beiträge zum Thema zusammen: Projektbeispiele, Analysen, Beobachtungen. Den Herausgeberinnen gelingt eine kluge Strukturierung dieser Vielfalt, durch die die einzelnen sehr unterschiedlichen Beiträge zusammengehalten werden. Das Buch ist lesenswert für alle, die sich in der Fülle verschiedener Arbeiten, Ansätze und programmatischer Sichtweisen orientieren möchten.

Isabel Zorn, Susanne Maass, Els Rommes, Carola Schirmer, Heidi Schelhowe (Hrsg.): Gender Designs IT - Construction and Deconstruction of Information Society Technology, VS Verlag für Sozialwissenschaften, Februar 2007

Micha Lenk

Bericht von der 35,0. Konferenz der Informatik-Fachschaften

Die Hintergründe zum offenen Brief an die Bundestagsabgeordneten

Vom 16. - 20. Mai 2007 lud die Fachschaft Mathematik/Informatik der Uni Karlsruhe zur Konferenz der Informatik-Fachschaften ein. Knapp 100 Fachschafter aus ganz Deutschland und Österreich folgten der Einladung und trafen sich in den Räumen der Fakultät für Informatik. Die Teilnehmer trugen mit einem reichhaltigen Angebot an Arbeitskreisen zur Fachschaftsarbeit, Gesellschaft und Politik, kulturellen, spielerischen und technischen Themen dazu bei, dass sich politische Meinungen weiterentwickeln, Erfahrungen ausgetauscht oder auch ganz andere Horizonte erweitert werden konnten.

Den Organisatoren gelang es nicht nur, die Herausforderungen zu bewältigen, die eine Konferenz mit so vielen Teilnehmern mit sich bringt, sie konnten auch den vor kurzem fertig gestellten Film „Weizenbaum. Rebel at Work“ von Silvia Holzinger und Peter Haas nach Karlsruhe holen und im prominenten Zentrum für Kunst- und Medientechnologie (ZKM) Karlsruhe vorführen. Der Film über das Leben des Computer-Pioniers und -Kritikers Joseph Weizenbaum war für die traditionell kritisch-hinterfragenden Teilnehmer der Konferenz eine wunderbare Ergänzung.

Es blieb nicht bei der anschaulichen Betrachtung am Beispiel Weizenbaums. Ein Arbeitskreis *Sicherheit*, der sich bei einer außerordentlich zahlreichen Beteiligung fast über die gesamte Konferenz erstreckte, befasste sich mit Fragen wie

- Wie weit geht der Sicherheitswahn, und wie weit geht Ihr mit?
- Wann sollte ein Informatiker "Nein" sagen zu geplanten Vorhaben?
- Wie weit darf man sich gegen seine Vorgesetzten oder eine Obrigkeit auflehnen? Und wie weit halten geltende Datenschutzbestimmungen dafür den Rücken frei?

Auf dieser Basis wurde ein offener Brief an alle Bundestagsabgeordneten verfasst, der im Sonderheft der FIfF-Kommunikation 3/2007 abgedruckt und online unter *http://www.kif.fsinf.de/wiki/KIF350:Arbeitskreise/Sicherheit_-_offener_Brief_-_Formulierung* nachzulesen ist. Im Abschlussplenum wurde der offene Brief als Resolutionsentwurf, d.h. als Stellungnahme aller Konferenzteilnehmer, eingebracht.

Eine Eigenart der Konferenz der Informatik-Fachschaften ist, dass Entscheidungen in ihren Plenen grundsätzlich mit größtmöglicher Zustimmung getroffen werden. Deshalb wird bei Weitem nicht jede Resolution vom Plenum angenommen und verabschiedet – zu kontrovers sind oft die Meinungen. Ganz anders bei dieser Resolution: Von Anfang an herrschte Konsens, dass sie verabschiedet werden müsse, was gerade in Anbetracht der Teilnehmerzahl beachtlich ist. In einer rekordverdächtig langen Sitzung von 13 Stunden wurde an den Formulierungen gefeilt und der offene Brief schließlich als Resolution verabschiedet.

Dem offenen Brief haben sich zum Zeitpunkt der Drucklegung folgende Organisationen angeschlossen:

- Chaos Computer Club (CCC) Bremen
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e.V.)

Micha Lenk

Micha Lenk studiert Informatik an der Universität Karlsruhe (TH) und ist seit Sommer 2001 Mitglied der Fachschaft Mathematik/Informatik. Er hat unter anderem dazu beigetragen, die Ringvorlesung *Informatik und Gesellschaft* an der Universität Karlsruhe ins Leben zu rufen.

Pia Grund-Ludwig

Solving the E-Waste Problem

1,3 Billiarden Euro Umsatz wurden bereits 2004 weltweit mit Informations- und Kommunikationstechnik erzielt. Einer der Gründe: Handys, Computer, aber auch andere elektronische Güter haben immer kürzere Lebenszyklen. Das liegt zum Einen daran, dass die Hersteller durch mehr oder weniger nützliche und innovative Innovationen natürlich ihren Umsatz halten und steigern wollen. Aber auch die Verbraucher spielen das Spiel mit und tauschen vor allem Kleingeräte wie CD-Spieler, MP3-Player, aber auch Handys zügig gegen neue Modelle aus. Das produziert enorme Müllberge: 40 Millionen Tonnen Elektromüll fallen jährlich weltweit an, hat die United Nations (UN) University ausgerechnet. Würde man das in Lastwagen füllen und diese Lastwagen hintereinander stellen, dann ginge die Schlange ein halbes Mal um den Globus.

Die UN University hat nun im März eine Initiative gestartet, die dieses Problem angehen soll. Sie nennt sich StEP. Das steht für Solving the E-Waste Problem, also Lösung des Elektronikmüllproblems. StEP richtet sich an die Hersteller, aber auch an Forscher und Verbraucherschützer. Zu den Herstellern, die bislang mitmachen, zählen unter anderem Cisco, Dataserv, Dell, Ericsson, Hewlett Packard, Microsoft, Nokia und Philips. Aus Deutschland sind das Fraunhofer-Institut für Zuverlässigkeit und Mikrointegration, das Freiburger Öko-Institut sowie die Deutsche Gesellschaft für Technische Zusammenarbeit mit an Bord. Aus Amerika machen die Umweltschutzbehörde EPA sowie das MIT und die Universität of California in Berkeley mit.

„Ziel ist es, die immer wertvoller werdenden Ressourcen zu retten und zu verhindern, dass sie die Umwelt verschmutzen," so Rüdiger Kühr von der United Nations University in Bonn. Dort sitzt auch das Sekretariat von StEP. Es geht zunächst darum, Rohstoffe wie Gold, Palladium oder Silber sowie knappe Ressourcen wie Indium wiederzuverwenden. Indium wird in Flachbildschirmen und Handys verwendet und wird immer rarer. „In den vergangenen fünf Jahren hat sich sein Preis versechsfacht", so Rüdiger Kühr, der für die UN University das Projekt koordiniert. Indium werde, so Kühr, bislang nur in wenigen Fabriken in Belgien, Japan und den USA wiedergewonnen.

Für die Hersteller geht es darum, sich über Verfahren zur Verwertung von Elektronikmüll zu verständigen. „Das wichtigste Ziel für uns bei StEP ist es, gute Verfahren für Recycling, die Behandlung des Elektroschrotts und den Umgang mit unseren Ressourcen und Geräten zu entwickeln," sagt Elaine Weidman, die bei Ericsson für StEP verantwortlich ist.

Wichtig ist dabei nicht nur das Recyceln. Ein Ziel von StEP sei auch, dass Produkte nicht so schnell auf den Müll wandern, ergänzt Jean Cox-Kearns. Sie ist bei Dell für Recycling-Programme in Europa verantwortlich:

> *„Wir wollen sicherstellen, dass es Verfahren gibt, die garantieren, dass Produkte optimal genutzt werden. Das bedeutet, dass wiederverwendbare Produkte wiederverwendet werden. Wenn sie nicht wiederverwendbar sind, sollen sie recycelt werden. Dabei muss sichergestellt werden, dass Komponenten, die wiederverwendet werden können auch wiederverwendet werden."*

Das müsse auch beim Design der Produkte berücksichtigt werden.

Die EU-Richtlinie zum Elektronikschrott

In Europa wird das Recycling über die Elektronikschrottrichtlinie der Europäischen Union geregelt. Kühr ist mit deren Inhalt einig, fordert jedoch eine Weiterentwicklung. So gehe es darin bislang nur um die Verantwortung der Hersteller für das Recycling. Soziale Fragen, etwa bei der Herstellung der Produkte, würden zu wenig berücksichtigt. Auch ein Redesign, das eine längere Lebensdauer sichere, oder die Weiterverwendung gebrauchter Geräte spiele in der E-Schrott-Richtlinie eine untergeordnete Rolle. Kühr hat dazu konkrete Ideen. Er könne sich beispielsweise vorstellen, dass beim Update eines PC nicht nur aktuelle Software, sondern auch Informationen zum Recycling aufgespielt werden. Dann wüssten die Verbraucher, was sie mit ihren Geräten anfangen können und wie hoch beispielsweise der Wiederverkaufswert ist, argumentiert Kühr. Sechs Monate nach der offiziellen Gründung der Initiative verweist Kühr auf erste Erfolge: Mitglieder des Konsortiums haben eine Studie erarbeitet, die die Umsetzung der Elektroschrottrichtlinie der Eu-

Pia Grund-Ludwig

Pia Grund-Ludwig ist freie Journalistin. Sie arbeitet für Tages- und Fachzeitschriften sowie unterschiedliche Radiosender.

ropäischen Kommission bewertet. Es ist eine von drei Studien dazu. Eins der frappierendsten Ergebnisse sind die sehr geringen Sammelquoten. Die Richtlinie werde der Bevölkerung zu wenig publik gemacht, so Kührs Erklärung. Über die sozialen Dimensionen wie Abbau oder Entstehung von Arbeitsplätzen gebe es dagegen noch keine validen Ergebnisse. Ausführliche Ergebnisse sollen noch in diesem Jahr vorliegen. Diskussionen hätten begonnen, StEP zum wissenschaftlich-technischen Berater der Basler Konvention zu machen und so die dortigen politischen Diskussionen durch StEP-Empfehlungen zu befördern. Ziel der Basler Konvention ist es, Abfallexporte in Entwicklungsländer besser zu kontrollieren und weltweit ein umweltgerechteres Abfallmanagement zu realisieren.

Recycling in Entwicklungsländern

In den Entwicklungsländern sind nämlich ganz andere Probleme zu bewältigen. Dort sind die Bedingungen für Recycling häufig chaotisch. Vieles wird einfach in Hinterhöfen unter katastrophalen Arbeitsbedingungen und unter Missachtung des Umweltschutzes auseinandergeschraubt. Illegale Exporte von Schrott, der in Entwicklungsländern verwertet wird, sind immer noch an der Tagesordnung. Die Arbeitsbedingungen sind schlecht, die Belastung durch Gifte wie Dioxine oder Furane ist hoch. Dazu kommt die Verschmutzung von Erde und Wasser durch Inhaltsstoffe der Elektronikgüter wie bromhaltige Flammhemmer, PCB, oder Blei.

StEP will in China Projekte durchführen, die dies ändern. Jaco Huisman von der Technischen Universität Delft ist dafür verantwortlich. Bislang gebe es viel Recycling im Land, die bisherige informelle Verwertung in Hinterhöfen führe aber zur Rosinenpickerei. Nur die lukrativsten Metalle würden wiedergewonnen, der Rest einfach weggeworfen. „Wir wollen eine große Fabrik zur Verarbeitung von Elektronikschrott aufbauen und dadurch eine weiter gehende Verwertung und eine hochwertige Demontage in großem Umfang sicherstellen."

Elektroschrott
Verena Lehmbrock – Berlin, FIfF-Fotowettbewerb 2006

Wichtig ist Huisman die Nutzung westlichen Know-hows, aber auch die Zusammenarbeit mit Experten aus China: „Wir wollen die Erfahrungen der Chinesen nutzen. Das ist mittlerweile ein wichtiges Herstellerland, die Leute wissen, welche Materialien verwendet werden." Es sei wichtig, dass nicht von Europa aus dekretiert werde, was zu geschehen habe, sondern dass Lösungen von Menschen aus den Ländern selbst entwickelt werden. Natürlich gebe es auch Kontakte zu Umweltschutzorganisationen vor Ort. Und, so betont Huisman, man müsse sich auf die Gegebenheiten vor Ort einstellen und diese berücksichtigen, auch wenn manche dies für einen Rückschritt halten. Das gelte insbesondere für den Einsatz billiger Arbeitskräfte: Die gebe es nun einmal, das sei eine Tatsache, und die Aufgabe des Projekts sei herauszufinden, wie sich das sinnvoll in Strategien zur Demontage nutzen lasse. Aber, so verspricht Huisman, bessere Arbeitsbedingungen und höhere Löhne als bei den Hersteller von Elektronikprodukten gebe es in den Recycling-Firmen allemal. In Bezug auf die Arbeitsbedingungen arbeite man auf einem für China guten Niveau und wolle diese auf internationales Niveau heben.

Der Text basiert auf einem Artikel in Heise Online (*www.heiseonline.de*) und einem Beitrag für den Deutschlandfunk (*www.dradio.de*).

Greenpeace hat vor einem Jahr einen „Leitfaden für grünere Elektronik" vorgestellt und jetzt eine erste positive Bilanz gezogen. „Unternehmen konkurrieren jetzt darum, die ersten zu sein, die gefährliche Substanzen entfernen und ihre Produkte in verantwortlicher Weise zurücknehmen und wiederverwerten" heißt es in der Studie. Nokia schneidet im Greenpeace-Ranking am besten ab, gefolgt von Sony Ericsson auf Platz 2 und Dell und Lenovo gemeinsam auf Platz 3. Iza Kruszewska, die für die Kampagne verantwortlich ist, wertet es insbesondere positiv, dass sich die Kampagne zwar auf die Leitmarken konzentriere, Verbesserungen aber in der gesamten Breite der Branche zu sehen seien.

Seit Beginn der Kampagne gebe es deutlich mehr Produkte ohne PVC und bromhaltigen Flammschutz, so Greenpeace. Zu den Unternehmen, die sich neu engagieren, zählt sie Asus. Das Unternehmen habe substantielle Änderungen seiner Umweltrichtlinien vorgenommen. Auch in Indien habe man ein Ranking eingeführt, das zu Veränderungen bei den großen Elektronikanbietern Wipro und HCL geführt habe. Fortschritte gab es auch bei Sony und LG Electronics. Die hatten sich bei der letzten Studie noch Strafpunkte eingehandelt, weil sie in einem Verband waren, der sich gegen die Verantwortung der Hersteller für die Verwertung entsorgter Produkte eingesetzt hat. Mittlerweile habe Sony in den USA das beste Programm für Wiederverwertung und Rücknahme aufgelegt, so Greenpeace. HP hat Punkte eingebüßt. Das Unternehmen solle konkrete Zeitpunkte für die Entfernung gefährlicher Chemikalien aus seinen Produkten nennen, so die Forderung der Umweltschützer. Panasonic hat sich durch die Weigerung, eine Entsorgungspolitik aufzulegen, den letzten Platz eingehandelt.

Lorenz M. Hilty

Markt, Lügen und Video

Wie man einen Kurs in Forschungsmarketing ohne Sinnkrise übersteht

Wir sind angetreten, um zu lernen, wie wir unsere Forschungsergebnisse besser vermarkten können. Herr Dr. W., vorgestellt als erfahrener Marketingberater, erscheint adrett auf der Bühne. Marketing sei eine Geisteshaltung, bekommen wir zu hören. Marketing macht man immer, sogar unbewusst. Sogar wenn wir nur miteinander reden, machen wir Marketing.

Wozu Marketing gut ist, zeigt gleich sein erstes Beispiel: Das Videosystem VHS habe sich im Markt durchgesetzt, obwohl das Konkurrenzsystem – er nennt es »Beta 2000« – technisch überlegen gewesen sei. Wir staunen. Wie ist das Wunder möglich? VHS habe eben das bessere Marketing gehabt, sagt Herr W. Ein Raunen geht durchs Publikum. Da sieht man doch gleich, dass die Welt ohne Marketing arm dran wäre. So arm, dass man bessere Videorekorder gehabt hätte.

Moment mal, Herr W.! Überträgt man Ihr Beispiel auf die Wissenschaft, bedeutet das ja: Forschungsergebnisse schlechter Qualität lassen sich mit dem richtigen Marketing gegen besser fundierte Ergebnisse durchsetzen. Oder die seriösere Forschungsgruppe verliert bei der Einwerbung von Drittmitteln gegen die Konkurrenz, weil diese die schöneren Anträge schreibt. Ich glaube zwar, dass das so ist, habe es aber bisher nicht für eine förderungswürdige Seite des Wissenschaftsbetriebs gehalten. Offenbar fehlt mir dazu noch die richtige Geisteshaltung.

»Guter Punkt!« erwidert Herr W. auf meine skeptischen Einwände und sammelt weitere Fragen, rastlos durchs Publikum streifend.

Nun kommt er auf das Thema Qualität zu sprechen. »Qualität ist, was den Kunden zufrieden stellt«, verkündet er und hechtet wieder auf die Bühne.

Meine Gedanken schweifen ab. Ich erinnere mich an Professor R. von der Universität Genf, der mit seinen Studien immer wieder belegte, dass Passivrauchen für die Gesundheit unbedenklich sei. Bis bekannt wurde, dass er ein zweites Einkommen aus der Tabakindustrie bezog. Hut ab! Der Kerl hat gewusst, was Qualität ist. Der muss zufriedene Kunden gehabt haben.

Zufrieden konnte auch der Exxon-Konzern sein, der Forscher und Institute bis 2005 dafür bezahlte, Erkenntnisse über den Klimawandel in Frage zu stellen und professionell Verwirrung zu stiften. Harte 10.000 US-Dollar für jeden Wissenschaftler, der einen Artikel schrieb, der den Klimabericht der UNO in Zweifel zog. Jetzt wird mir alles klar: Das waren Qualitätsprämien! Insgesamt 16 Millionen Dollar. Für dieses Geld hätte man noch ein paar Touristen den Aletschgletscher zeigen können, bevor er ganz verschwindet. Aber es geht hier ja um Forschungsmarketing, nicht um Tourismusmarketing.

Während ich mir diese Gedanken mache, läuft unser Wanderprediger zur Hochform auf, wirbelt wieder im Publikum herum. »Guter Punkt!« entgegnet er immer wieder auf kritische Fragen der Kollegen. Ja, diese anfängliche Skepsis sei bei Akademikern aus dem Elfenbeinturm der Forschung immer zu spüren. Aber wir haben ja noch einen ganzen Tag vor uns, um gemeinsam daran zu arbeiten.

Wie naiv war ich doch, bevor ich diesen Workshop betrat. Ich betrachtete uns Wissenschaftler als »Zwerge auf den Schultern eines Riesen«, wie man seit Bernhard von Chartres sagt. Zwerge, die bemüht sind, einen bescheidenen Beitrag zum Wissensfortschritt zu leisten, damit unsere Kinder dereinst auf noch höhere Schultern steigen können. Ja, ich glaubte allen Ernstes, die *Scientific Community* hätte ihre eigenen Qualitätsmaßstäbe. Welche Verblendung. Ich war dem Aberglauben an Unvoreingenommenheit, Präzision und Integrität verfallen.

Jetzt erfahre ich: Ich bin gar kein Zwerg! Ich bin eine Marionette des Marktes! Da bin ich aber erleichtert. Wie gut, dass es Berater wie Herrn W. gibt, die einem dazu die richtige Geisteshaltung eintrichtern. Kunden, Kunden, Kunden. Studierende sind Kunden, Fördertöpfe sind Kunden, Evaluations-Teams sind Kunden, einfach alle sind Kunden. Die Welt ist voller Kunden-Könige, eine Universalmonarchie. Nur wir sind die Deppen, wir stehen knapp vor dem Eingang in die selbstverschuldete Unmündigkeit.

In gewisser Weise hat Herr W. vielleicht sogar Recht. Wenn wir uns darauf einigen könnten, dass die kommenden Generationen die wichtigsten Kunden der Wissenschaft sind, wären wir gar nicht so weit auseinander.

Es ist nur so schwierig, mit dem Referenten Argumente auszutauschen. Anscheinend kann er auf Fragen und Kommentare nur mit »Guter Punkt!« antworten und seine Slideshow weiterklicken, um animierte Leere zu zeigen. Das wirkt, als hätte ihn jemand dressiert. Schade, sonst hätte ich ihn noch gefragt, wie

Lorenz M. Hilty

Prof. Dr. Lorenz M. Hilty leitet die Abteilung »Technologie und Gesellschaft« der Eidgenössischen Materialprüfungs- und Forschungsanstalt Empa und lehrt an den Universitäten St.Gallen und Zürich.

man etwas an Kunden verkauft, die noch nicht geboren sind. Stattdessen verlasse ich den Saal. Den Ausspruch »Guter Punkt« könnte ich kein weiteres Mal ertragen.

In einem Workshop über Forschungsmarketing hätte ich etwas weniger Show und mehr Diskussion erwartet. Aber ich bin hier ja nur Kunde. Nur Kunde? Genau: Mit der Verinnerlichung des Marketing-Evangeliums scheint es beim Referenten noch ein wenig zu hapern. Trotz froher Kunde bin ich kein froher Kunde. Guter Punkt?

Interessiert es Sie, was die Videokassette im Innersten zusammenhält? Mich nicht. Dennoch sei der Form halber ergänzt, dass das Eingangsbeispiel von Herrn W. sachlich falsch war. Es gab nie ein Format namens »Beta 2000«. Die Konkurrenzformate von VHS waren Betamax und das technisch überlegene Video 2000. Dieses hat den Konkurrenzkampf hauptsächlich deshalb verloren, weil der Philips-Konzern, so seltsam das klingt, aus religiösen Motiven keine Lizenzen an die Pornofilm-Industrie verkaufen wollte. Und die Videotheken mit ihren Pornos haben das Rennen entschieden. Marketing ist eben doch nicht an allem schuld.

Christiane Floyd

Software-Engineering in Äthiopien

Am 11. September 2007 bin ich zum dritten Mal in Addis Abeba angekommen – gerade rechtzeitig zum Beginn des äthiopischen Millenniums, das aufgrund des geltenden Julianischen Kalenders in der Nacht zum 12.9.2007 mit rührender Begeisterung gefeiert wurde. Alles soll anders werden. Den Geist der letzten tausend Jahre, die durch Kriege und Konflikte gezeichnet waren, und das frühere Abessinien von einer hoch stehenden Kulturnation zu einem der ärmsten Länder der Welt machten, will man hinter sich lassen. Am Fernsehen wurde immer wieder eine schöne junge Frau gezeigt, gekleidet in den Landesfarben grün-gelb-rot, die feierlich in ihren ausgestreckten Händen eine weiße Taube hielt und sie langsam aufsteigen ließ. Frieden nach innen – zwischen den über 80 Ethnien und den Religionen (es gibt in etwa gleich viele Christen und Muslime) – und nach außen, insbesondere mit den schwierigen Nachbarn Eritrea, Somalia und Sudan, braucht das Land am meisten, wenn es sich entwickeln will.

Die Begeisterung wurde von der Bevölkerung getragen und von der Regierung gefördert. Man hoffte vor allem, dass viele aus der äthiopischen Diaspora nach Hause kommen würden. (Hunderttausende haben das Land infolge der politischen Verhältnisse und dem Mangel an Zukunftsperspektiven in den letzten Jahrzehnten verlassen.) Die Hoffnung hat sich nur teilweise erfüllt, auch wenn bereits am Flughafen der traditionelle Kaffee für die Neuankommenden ausgeschenkt wurde und etliche Minister persönlich zur Begrüßung Rosen verteilten.

Beim Abflug in Frankfurt hatten wir von Terrorwarnungen gehört. Passiert ist zum Glück nichts. Die Sicherheitsmaßnahmen waren aber unübersehbar. Die großen Straßen, auf denen sich die Politiker zu den offiziellen Feiern bewegten, waren gespickt mit Bundespolizisten, die schussbereite Gewehre trugen. Das Feuerwerk um Mitternacht fand unangekündigt ganz woanders statt als erwartet. Noch Tage später wurden wir beim Verlassen der Stadt zu einem Ausflug und bei der Rückkehr kontrolliert. – Für die Terrorgefahr wurde Eritrea verantwortlich gemacht. Die Gewehre hätten sich aber auch auf die eigene Bevölkerung richten können. Niemand hat vergessen, dass noch vor zwei Jahren, während der Proteste anlässlich der abgebrochenen Wahlen, aus diesen Gewehren geschossen wurde, und der Blutzoll war hoch. Was hat sich geändert seit damals?

Die Menschen sind skeptisch, würdigen aber manche positive Entwicklung. Vor ein paar Wochen wurden endlich die seit den Wahlen eingekerkerten Oppositionspolitiker frei gelassen. Zum Millennium wurde auch SMS wieder frei gegeben. Die Regierung hat mit einer Initiative begonnen, um die Bettler von den Straßen der Hauptstadt in ihre Dörfer zurückzubringen und dort wieder anzusiedeln. Der Schulbeginn wurde um eine Woche verschoben, um eine landesweite Konferenz zur Qualitätsverbesserung der Lehre abzuhalten. Das Gehalt der Lehrenden in den staatlichen Hochschulen wurde annähernd verdoppelt. Die Regierung trifft sich mit der Jugend, mit Vertretern der Regionen, um mehr Partizipation zu gewährleisten. Sogar dass Ministerpräsident Meles bei der Millenniumsfeier vor laufender Fernsehkamera seine Frau nach dem Tanz küsste, sei doch ein erfreuliches Zeichen bei dieser Regierung, die immer noch die

Christiane Floyd

Christiane Floyd ist Professorin für Softwaretechnik, 1978-91 an der Technischen Universität Berlin, seit 1991 leitet sie den Arbeitsbereich Softwaretechnik an der Universität Hamburg. Sie ist Hauptautorin des Ansatzes STEPS (Softwaretechnik für partizipative Systemgestaltung). 1984 war sie Gründungsvorsitzende des FIfF.

Narben des Bürgerkriegs 1991 trägt, aus dem sie hervorgegangen ist. Viele einzelne Maßnahmen – Symbolik? Ablenkung? Echte Verbesserung?

Ich bin nicht zum Feiern gekommen, sondern um ein Promotionsstudium im Bereich IT aufbauen zu helfen. Meine ersten beiden Besuche 2006 und 2007 und meine Aktivitäten in Europa haben dazu beigetragen, dass dieser Studiengang ins Leben gerufen wurde. Nun soll es losgehen. Ich bin vom DAAD zur Hochschulberaterin an der Universität Addis Abeba ernannt worden, das Programm wird vom Deutschen Ministerium für Entwicklungszusammenarbeit finanziert. Mit dem Bewilligungsschreiben erhielt ich einen zerschnittenen Papierstreifen, auf dem stand „Spende der Bundesrepublik Deutschland". In meiner Eigenschaft als Spende plane ich, im Verlauf der nächsten beiden Jahre viermal einen Monat in Äthiopien zu verbringen.

Informatik in Entwicklungsländern?

Mit dieser Frage wurde ich schon in den Achtziger Jahren an der TU Berlin konfrontiert. Damals war ich Vertrauensdozentin für Ausländische Studierende. Ich lernte Einzelschicksale kennen, die mir nahe gingen. Ich verstand, warum viele, die zum Studium nach Deutschland kamen, darauf schlecht vorbereitet waren, und welchen Existenzkampf sie zu bestehen hatten. Und es wurde mir die Lücke klar zwischen dem, was wir in der Informatik lehrten und forschten, und der Situation, in der sich die Entwicklungsländer befanden.

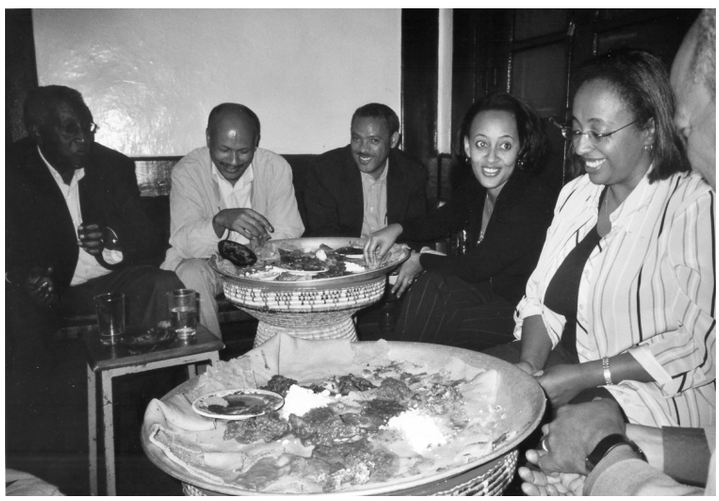
Die Informatik wurde nicht nur aufgrund der Interessen in den Industrieländern vorangetrieben, sie verkörpert den Kontext, in dem sie entstanden ist. Sie setzt nahtlos auf den Denk- und Verfahrensweisen auf, die seit der Aufklärung Geltung erfahren haben und in der Industrialisierung umgesetzt wurden. Die Formalisierung fast aller gesellschaftlicher Tätigkeitsbereiche, das ständige Bestreben, Vorgänge zu rationalisieren, die Nutzung abstrakter Modelle, um den Umgang mit der komplexen Wirklichkeit zu erleichtern – das alles sind Voraussetzungen dafür, dass Informatik „greift". Dieses Denken findet in anderen Kulturen erst allmählich Eingang. Auch bringt die Ausdifferenzierung des Faches eine Spezialisierung mit sich, die in Entwicklungsländern nicht relevant ist.

In der Zeit des Kalten Kriegs kam noch die politische Dimension dazu. Autoritäre Regierungen verschiedener Couleur betrachteten die teure Technik als Statussymbol und nutzten sie zur Verfestigung ihrer Macht. In Äthiopien etwa herrschte von 1974 bis 1991 das DERG-Regime (wörtlich „Komitee") unter Mengistu Haile Mariam, eine durch einen Militärputsch gegen Kaiser Haile Selassie an die Macht gekommene Regierung, die einen harten, leninistisch geprägten Kommunismus vertrat und für den „Roten Terror" in den Siebziger und Achtziger Jahren verantwortlich ist. In dem damals von Hungerkatastrophen gepeinigten Land wurde eine riesige Armee am Leben erhalten, die seit dem Bürgerkrieg und dem Regime-Wechsel 1991 zwar geschrumpft, aber nach wie vor überdimensioniert ist. In der Militärhochschule gibt es ein Forschungsinstitut für Robotik, das angeblich nach westlichen Maßstäben ausgestattet ist.

Wenn Informatik nur die Interessen einiger weniger voranbringen soll, wollte ich dazu keinen Beitrag leisten. Ich engagierte mich für partizipative Systementwicklung – wie war ein solcher Ansatz mit den Verhältnissen in einer durch Diktatur bestimmten Gesellschaft zu vereinen?

Seither haben sich die Informatik und die gesellschaftliche Bedeutung der von ihr hervor gebrachten Technologien ebenso tief greifend gewandelt wie der weltweite politische Kontext. Im Jahr 2000 hat die UNO die Nutzung der Informationstechnologien für Entwicklung unter ihre Millenniumsziele aufgenommen. Auch Äthiopien, wo sich die Verhältnisse seit 1991 allmählich stabilisiert haben, findet sich in der globalisierten Informationsgesellschaft wieder. Die Regierung hat Informationstechnologien als Chance erkannt. Sie sollen helfen, die Armut zu bekämpfen – *poverty that kills* in den Worten von Ministerpräsident Meles.

Äthiopien hat von der Weltbank eine größere Budget-Hilfe zu diesem Zweck erhalten. Eine ICT-Development Agency wurde geschaffen, die landesweit die Entwicklungsprojekte koordiniert und die Regierung berät. Zunächst wurde die Infrastruktur aufgebaut, nun ziehen Breitbandkabel durch das Land, und mit etwas Geduld und Glück kann man sogar in entlegenen Gegenden das Internet nutzen. Der Engpass ist jetzt das sog. Capacity Building, das Aufbauen von Kompetenz auf allen gesellschaftlichen Ebenen. Und siehe da, die Entwicklung soll partizipativ erfolgen – soweit das in einem extrem autoritär geprägten Land leistbar ist.



Gemeinsames Essen

Bei der Entwicklung der äthiopischen Zivilgesellschaft hat die Universität Addis Abeba (AAU) eine herausragende Rolle gespielt. Gegründet 1950 als Haile-Selassie-Universität in einem ehemaligen kaiserlichen Palais hat sie um 1960 erstmals eine Generation gebildeter junger Leute der Oberschicht hervorgebracht. Ihre Studentenbewegung Ende der Sechziger Jahre sollte der Reform des Landes dienen. Sie wurde gewaltsam unterdrückt, gab jedoch den ersten Anstoß zum Sturz des Feudalsystems. – Die Informatik an der AAU ist unter bescheidensten Umständen entstanden und hat Wurzeln in der Mathematik, den Ingenieurswissenschaften sowie der Informations- und Bibliothekswissenschaft. Erst wurden diverse BSc-, dann MSc-Studiengänge aufgebaut. Jetzt gibt es eine Fakultät für Informatik, in der die bisher separaten Teile zusammengefasst sind, und ein neues Gebäude, in dem auch das PhD-Programm angesiedelt wird.

Menschen zwischen Vergangenheit und Zukunft

Die Menschen, mit denen ich zu tun habe, gehören der immer noch kleinen gebildeten Schicht an. Sie sind mir gegenüber offen, herzlich und lächelnd. Sie betonen das Gute, das ihnen in den letzten Jahren widerfahren ist, die Chancen, die ihre Kinder hoffentlich haben werden, ihre Verbundenheit mit Verwandten, die in der Diaspora leben. Nur allmählich gewinne ich ein Gefühl dafür, was sie durchgemacht haben.

Kollegen in meiner Altersklasse gibt es nur wenige. Sie haben sich in den 70er Jahren für den Umsturz engagiert und sind dann zur Zielscheibe des roten Terrors geworden. Wer selbst überlebt hat, hat seine Brüder und Freunde sterben sehen. Zur Zeit des DERG, erzählt man mir, waren unerwartete Anrufe gefürchtet, vor allem frühmorgens. Jede Familie hatte Opfer zu beklagen – eins, zwei, manchmal drei. Am Vormittag gingen sie zu ihren Vorlesungen, am Abend wurden ihre Leichen erschossen auf der Straße gefunden. Wie sollte man es den Müttern sagen? Man hat sie nicht direkt angerufen, sondern ein nahe stehendes Familienmitglied. Ein Netzwerk zur Unterstützung wurde gebildet. Erst dann wurden sie verständigt. Nur so ließ sich diese Zeit überstehen.

Anders war die Erfahrung der ländlichen Bevölkerung. Für die ärmeren Schichten brachte das Ende der Feudalgesellschaft durchaus Erleichterung. Der Großgrundbesitz wurde enteignet, das Land parzelliert, Schulen wurden gebaut und die Gesundheitsversorgung verbessert. Dies wurde jedoch überlagert durch heftige ethnische Konflikte und Freiheitskämpfe, in denen das DERG-Regime brutal gegen die Bevölkerung vorging: Gefängnis, Folter, Hinrichtungen, Bombardierung ganzer Landesteile waren die Folge. Dazu kamen furchtbare Hungersnöte, die auch noch politisch instrumentalisiert wurden. Durch Tod und Flucht wurde die Bevölkerung doppelt dezimiert.

Den Zurückgebliebenen geht die Entwicklung zu langsam. Auch nach Jahrzehnten liegt die Angst noch im Blut. Sie scheuen sich, Verantwortung zu übernehmen und lassen lieber andere Entscheidungen treffen. Und doch gibt es Menschen, die sich eine eigenständige Vision für die Zukunft des Landes bewahrt haben, ein Bewusstsein dafür, dass es anders sein könnte und auch anders werden sollte, und dass sie selbst dazu einen Beitrag leisten können. Das trifft vor allem für die jüngeren zu, die unter vergleichsweise freieren Umständen aufgewachsen sind.

Zwar lebt die Hälfte der Bevölkerung in bitterer Armut, aber das Land ist in Aufbruchsstimmung. Die Regierung ist nicht demokratisch legitimiert, man versucht sich aber zu arrangieren; der Wirtschaft geht es etwas besser; das Verständnis für ziviles Engagement wächst; es gibt Menschen, die aufbauen wollen, und trotz zahlreicher lähmender Regelungen dazu auch den Freiraum finden.

Mein erster Kontakt war Rahel Bekele, die ich durch die Internationale Frauenuniversität 2000 kennen gelernt habe. Sie lehrt an der AAU, ist Mutter von mehreren Kindern, und doch ist es ihr gelungen, in Hamburg zu promovieren. Durch sie bin ich nach Äthiopien gekommen. Mit der Zeit habe ich mich auch mit anderen Äthiopiern angefreundet. Für Neue im Land wie mich ist die großzügig gewährte Gastfreundschaft der erste überwältigende Eindruck und dann die allmähliche Erschließung der uralten Hochkultur mit ihren vielen Facetten, von denen wir in Europa so wenig wissen. Die Menschen sehen es gern, dass ich mich für das Land und seine Geschichte interessiere. Sie wollen ihre Traditionen in die Zukunft mitnehmen.

Neues Informatikgebäude

Rahels Mann, Tesfaye Biru, ist jetzt mein wichtigster Gesprächspartner. Er hat die Informatik in Äthiopien zu großen Teilen aufgebaut, viele jüngere Leute orientieren sich an ihm. Er war auch Projektleiter beim Aufbau der Infrastruktur. Wir haben die industrielle Revolution und die Agrarrevolution versäumt, sagt er. Aber die Informationsrevolution werden wir nicht versäumen. Mit 44 Jahren holt er endlich seine Promotion nach. Ich betreue seine Dissertation über *Software Process Improvement* vor dem Hintergrund von zwanzig Jahren Erfahrung in Lehre und Projekten in Äthiopien. Seinen Ansatz nennt er *Reflective Steps*. Man muss den jungen Menschen eine Perspektive geben, sagt er. Der Promotionsstudiengang war seine Vision, nun ist er der Direktor.

Ein internationales Netzwerk

Zuerst war eine institutionalisierte Kooperation mit Hamburg gewünscht, doch scheiterte das an Kapazitätsproblemen. Dann habe ich im Juli 2006 mit Tesfaye Biru eine Initiative *International Network Joining Ethiopia in Research and Application of IT* gegründet, die sich zum Ziel setzt, Persönlichkeiten aus der internationalen Informatik zur Zusammenarbeit mit Äthiopien zu gewinnen. Zu den Gründungsmitgliedern gehören Prof. Peter

Hauptgebäude der Universität Addis Abeba

Löhr von der FU Berlin und Prof. Gustav Pomberger von der JKU Linz. Etliche Kollegen und Kolleginnen dieser beiden Universitäten sowie der Universität Hamburg haben sich bereiterklärt, im Rahmen des Möglichen mitzuwirken.

Wer einmal in Äthiopien war, weiß das Akronym INJERA-IT zu würdigen: Traditionell finden hier Mahlzeiten statt, bei denen alle von einem großen gemeinsamen Teller essen. Aus dem einheimischen Getreide *Teff* (das gemahlen und fermentiert wird) werden Fladen gebacken, auf denen die Fleischgerichte bzw. die Gemüsespezialitäten serviert werden. Man reißt Stück für Stück vom Fladen ab und holt sich damit eine mundgerechte Menge von Fleisch oder Gemüse. Die Basis dieser Mahlzeit heißt Injera, verallgemeinernd steht das Wort auch für gemeinschaftliche Aufgabe. Wir haben uns die Aufgabe gestellt, den weiteren Aufbau der Informatik in Äthiopien zu fördern.

Zusammenarbeit kann bedeuten, nach Addis Abeba zu gehen, um Kurse zu halten, die auch kompakt durchgeführt werden können. Oder Forschungsmöglichkeiten für junge Leute an europäischen Universitäten zu bieten und dabei mit den Betreuern in Addis Abeba zu kooperieren. Die Bereitschaft der Kollegen und Kolleginnen war wesentlich, um den Promotionsstudiengang zu konzipieren und zu lancieren, der ohne ausländische Beteiligung nicht möglich wäre.

Injera-Mahlzeit

Ein Promotionsstudiengang im Bereich IT

Im Unterschied zu bisher, wo einzelne Hochbegabte ins Ausland promovieren gingen und in vielen Fällen nicht mehr zurückkehrten, sollen sich in Zukunft hoffnungsvolle Studierende vor Ort weiter qualifizieren können. Das Promovieren im *Sandwich-Modell* in Zusammenarbeit mit einer ausländischen Universität wird jetzt auch vom DAAD gefördert.

An der AAU wird dem entstehenden Studienprogramm eine hohe Bedeutung zugemessen. Zuerst sollen die jungen Lehrenden an der Universität profitieren. In Europa würden sie unter Betreuung an ihrer Promotion arbeiten – hier sind sie auf sich gestellt, tragen große Verantwortung und haben kaum ältere Vorbilder.

Der Studiengang besteht aus einem Jahr Vorlesungen und Seminaren, gefolgt von drei Jahren Forschung und Niederschrift der Dissertation. Die Kandidaten und Kandidatinnen werden von ihren Arbeitsplätzen beurlaubt, bekommen ein Stipendium und haben nur eine Lehrverpflichtung, die in etwa der von wissenschaftlichen Mitarbeitern entspricht.

Sechs Gebiete wurden als vordringlich ausgewählt: Wireless Communication Systems, IP-Networks, Natural Language Processing, Information Retrieval, Information Systems und Software-Engineering. Ich bin Beraterin für das gesamte Programm, vor allem aber für den Software-Engineering-Zweig, wo ich am Aufbau von Lehre und Forschung mitwirke.

Ein vorläufiges Exposé muss für die Aufnahme ins Promotionsstudium vorgelegt werden. Das eigentliche Abenteuer besteht darin, dass niemand hier Erfahrung mit Forschung und der Betreuung von Dissertationen hat.

Die Lehrenden in diesem Programm sind zwar selbst promoviert, aber Forschung haben sie bisher nicht aufbauen können. Der Grund ist einfach: Sie werden an der Uni so bescheiden bezahlt, dass sie ihre Familien durch Nebenjobs ernähren müssen. Auch die Gehaltserhöhung reicht nicht aus. Um den Freiraum für Forschung und Promotionsbetreuung herzustellen, müssen also substantielle finanzielle Anreize geschaffen werden. Offenbar gibt es jetzt Geld. Eine Herausforderung besteht darin, Projektförderung in die Wege zu leiten, damit Forschung wachsen kann. Das allein wird jedoch nicht genügen.

Vor allem gilt es, ein Forum herzustellen, in dem Forschungsfragen erörtert, Forschungsprojekte ausgearbeitet, Forschungsanträge diskutiert, Exposés von Kandidaten und Kandidatinnen geprüft, bewertet und zugeordnet werden. Im kommenden Semester soll es also erstmals ein Forschungsseminar geben, in

dem die Beteiligten auf Junior- und Seniorebene miteinander ins Gespräch kommen. Darauf aufbauend will man mit den ausländischen Partnern Kontakt aufnehmen.

Software-Engineering – aber wie?

Software-Engineering ist hier dringend nötig. Die gute alte Software-Krise hat mit einiger Zeitverzögerung Äthiopien erreicht und voll zugeschlagen. Da kommt einiges zusammen: keine angemessene Ausbildung, wenig Verständnis für Entwurfs- und Programmiermethodik, kaum Bewusstsein für die Erfordernisse von Mensch-Maschine-Interaktion und die Notwendigkeit, im Zuge der Entwicklung und Einführung von Software die Geschäftsprozesse zu reformieren. Oder überhaupt erst aufzubauen. Und das in allen Organisationen. Nun soll an der Universität in Zusammenarbeit mit der Wirtschaft ein Kompetenzzentrum entstehen, das relevante Forschung für das Land betreibt.

Aus Sicht von Tesfaye Biru sind die Besonderheiten in seinem Land mangelnde Qualifikation, Knappheit der Ressourcen und die Notwendigkeit, Software-Entwicklung, Software-Nutzung sowie Organisationsentwicklung gemeinsam zu betrachten. Software-Engineering in Äthiopien wird sich nicht an den Anforderungen von Militär, Großindustrie oder weltweit operierenden Softwarefirmen orientieren, sondern an mittelständischen Softwarefirmen im Land, an Anwendungen in Organisationen und vor allem bei der Regierung. E-Learning, E-Government und E-Health sind neben kommerziellen Anwendungen die großen Themen. Und vielleicht in Zukunft die Zusammenarbeit mit Industrieländern in Offshoring-Projekten.

Mit Dr. Rahel Bekele (links) und Ethiopia Tadesse

Man kann sich keine Verschwendung leisten: weder umfassende Modellierung, noch Wegwerf-Prototypen. Inkrementelles Vorgehen ja – aber jeder Zyklus muss Nutzen bringen. Partizipation ja – aber es gibt keine qualifizierten Benutzer. Es geht nicht um Business Process Re-Engineering, sondern um Business Process Design.

Vision und Wirklichkeit

Der neue Promotionsstudiengang passt gut in die derzeitige Aufbruchsstimmung. Es ist eine kühne Vision, deren Verwirklichung noch einige Wunder erfordert. Die ersten Schritte sind hoffnungsvoll. Ob er den Drang junger Leute, außer Landes zu gehen, aufhalten kann, bleibt dahin gestellt. Ob die Prioritäten richtig gesetzt sind, kann ich nicht beurteilen. Dass die Informatik einen echten Beitrag zur Armutsbekämpfung leisten kann, wage ich kaum zu hoffen. Ich hoffe aber, dass den jungen Promovierten eine Multiplikatorenrolle zukommen wird, die auch andere gesellschaftliche Aufgaben voranbringt. Und so setze ich mich gern dafür ein – es ist mein Beitrag zur Entwicklung des Landes, und ich freue mich, dass ich ihn leisten kann.

Kurz vor meiner Abfahrt wünschen mir die Menschen immer noch mit glänzenden Augen „Happy Ethiopian Millenium". Ja, das wünsche ich ihnen auch!

Fotos von Christiane Floyd

Hans-Georg Wischkowski

Weder Sicherheit noch Recht

Online-Durchsuchung, mehr Polizei-Befugnisse und starker Staat sind die gängigen Antworten in der Terrorismusbekämpfung. Wer allerdings die aktuelle politische Debatte zur inneren Sicherheit in Deutschland mit den realen Bedingungen von Aufklärung und Strafverfolgung vergleicht, wird beides kaum zur Deckung bringen können.

In Sachen Terrorismus ist das Bundesinnenministerium unmissverständlich: „Der internationale Terrorismus hat sich mit den Anschlägen des 11. September 2001 zu einer weltweiten Bedrohung entwickelt. (...) Die Bundesregierung hat die Sicherheitsstrukturen unseres Landes mit einer Reihe umfangreicher gesetzlicher und administrativer Maßnahmen gezielt ausgebaut und der neuen Bedrohungslage angepasst."

Der Schutz der Bevölkerung hat höchste Priorität: Um die „Bevölkerung zu schützen, vorzusorgen und die Verwundbarkeit unseres Landes zu reduzieren, werden die Sicherheitsvorkehrungen regelmäßig untersucht. (...) Insbesondere durch eine Überprüfung der Infrastruktursysteme sind, beispielsweise im Luftverkehr, deutliche Sicherheitsgewinne erzielt worden."[1] Natürlich wurden die „Kompetenzen des Bundeskriminalamtes und des Bundesamtes für Verfassungsschutz zur Informationsgewinnung und zum Informationsaustausch erweitert"[2].

„Um den Terrorismus auch in seinen instabilen Herkunftsregionen wirksam zurückdrängen, trägt die Bundesregierung zu den Einsätzen der internationalen Gemeinschaft bei. Deutschland beteiligt sich (...) im Rahmen der Anti-Terror-Koalition bei der

Bekämpfung des Terrornetzwerks in Afghanistan. Das Bundesinnenministerium nimmt mit der Hilfe beim Aufbau der Polizei in Afghanistan aktiv an diesem Prozess teil." [3] so das BMI weiter.

Eingedenk der von niemandem bestrittenen verstärkten terroristischen Bedrohung ist es sicher eine hervorragende Sache, die afghanische Polizei auszubilden und in Deutschland regelmäßig die Sicherheitsvorkehrungen beispielsweise im Luftverkehr zu untersuchen. Mehr Sicherheit durch mehr polizeiliche Arbeit im Inland wäre auch nicht schlecht - nur: wer soll die leisten?

In der Zeit zwischen 2001 und 2006 haben Bund und Länder bei ihren Polizeien 7.000 Stellen abgebaut[4]. Der Sinn dieser zumindest etwas unorthodoxen Maßnahme erschließt sich auch dann nicht, wenn man liest, dass im August 2007 deutsche Polizeibehörden mit Hilfe der Freunde aus den USA eine Gruppe daran hindern konnten, Terroranschläge mit Autobomben auszuführen. Laut Gewerkschaft der Polizei war nämlich der Arbeitsaufwand für die Aufklärung – von der Überwachung der Verdächtigen zur Übersetzung der Abhörergebnisse, über die Ermittlungen bis zum Austausch des Chemikalienvorrats – so hoch, dass ein weiterer Fall nicht hätte bearbeitet werden können.

Weil die deutsche Polizei zu Hause so dringend benötigt wird, hatte das BMI – so der Spiegel – nach Afghanistan auch anfangs erst fünf, dann 40 Ausbilder entsandt und die Aufgabe dann ganz an eine europäische Formation abgeschoben[5].

Dank *veränderter Schwerpunktsetzung* wurde für die Beobachtung der organisierten Kriminalität und Verfolgung ihrer Straftaten in den letzten Jahren so viel Personal abgezogen, dass dieser Bereich der Kriminalität kaum noch wirkungsvoll bekämpft wird. Als Weckruf hat auch der brutale Mafiamord unter italienischen Ehrenmännern in Duisburg nicht ausgereicht.

Wenn wir den gewerkschaftlich organisierten Praktikern glauben, dass die Personaldecke der Polizei schon sehr dünn geworden ist, dann ist es um so interessanter, sich genauer anzusehen, welche Folgen die Ausweitung der Befugnisse des BKA und des Bundesamtes für Verfassungsschutz zur Informationsgewinnung haben werden. Auch hier wird die Gefahr als beachtlich dargestellt. Bundesinnenminister Schäuble erklärt, das Internet sei für Islamisten Raum für die Vorbereitung und Verabredung von Taten:

> *„Terroristische Aktivitäten verlagern sich immer mehr in die virtuelle Welt des world wide web. Das Internet bietet den Terroristen ein gigantisches Forum: Es ist Kommunikationsplattform, Werbeträger, Fernuniversität, Trainingscamp und think tank in einem."*

Schäuble benannte zwei konkrete Maßnahmen:

> *„Deshalb brauchen wir im nachrichtendienstlichen Bereich die Möglichkeit der so genannten Online-Durchsuchung. [...] Im Januar dieses Jahres haben Bundesamt für Verfassungsschutz und Bundeskriminalamt die Arbeit im neu errichteten Gemeinsamen Internetzentrum aufgenommen. In enger Kooperation mit anderen Sicherheitsbehörden – wie Bundesnachrichtendienst, Militärischer Abschirmdienst, der Generalbundesanwältin, aber auch unseren Partnern im Ausland – werden hier islamistische Websites beobachtet und ausgewertet."* Denn: *„häufig nehmen Radikalisierungsprozesse nicht in bestimmten Vereinen oder Moscheen ihren Ausgang, sondern im Internet."*[6]

Online-Durchsuchung, *Internetzentrum* beim *Gemeinsamen Terrorismusabwehrzentrum* (GTAZ), das Internet als Aktionsschwerpunkt der Polizei – allein dies erfordert qualifiziertes Personal. Die Auswertung *islamistischer Websites* und ganz besonders die Online-Durchsuchung sind – so der BKA-Präsident Ziercke im Stern – so aufwändig, dass nicht mehr als 10 Online-Durchsuchungen pro Jahr möglich seien. Wer sich einmal überlegt, welchen Aufwand die Durchsuchung der Daten auf einem PC verursacht – die ggf. in mehreren Sprachen vorliegen –, kann nachvollziehen, dass sie die Kapazitäten von IT-Fachleuten bei der Polizei, Übersetzern und Fahndern mit den nötigen Kenntnissen bei der Terrorfahndung schnell an die Grenzen des Möglichen bringen wird.

In der Realität sind bei den Polizeibehörden des Bundes und der 16 Länder insgesamt etwa 350 Beamte mit der Überwachung des offenen Internets beschäftigt[7]. Überwiegendes Einsatzgebiet sind Delikte im Bereich der Kinderpornografie. Laut BMI sind derzeit im GTAZ 190 Personen in der Terrorbekämpfung beschäftigt[8], darunter Experten aus dem BKA, dem Bundesamt für Verfassungsschutz, dem Bundesnachrichtendienst, den Kriminal- und Verfassungsschutzämtern der Länder, der Bundespolizei, dem Zollkriminalamt, dem Militärischen Abschirmdienst, dem Bundesamt für Migration und Flüchtlinge und dem Generalbundesanwalt[9]. Wenn alle Länder mitmachen, heißt das: 40 Behörden - davon 19 Polizeibehörden – entsenden rein rechnerisch im Schnitt 5 Beamte. Das GTAZ bindet also ca. 100 der 350 bekannten und mit der Internetfahndung betrauten Polizisten der Republik. Es ist unbekannt, wie viele dieser Beamten des Englischen oder gar des Arabischen mächtig sind, um gegen Islamisten vorgehen zu können.

Überdies haben die Bundesbehörden auch nur begrenzt IT-Fachleute in Reserve. Damit Deutschland als vorletztes Land in Europa - vor Albanien - einen Digitalfunk für Polizei und Rettungsdienste erhält, wurden IT-Fachleute aus verschiedenen Bundeseinrichtungen für Entwicklungsaufgaben des neuen Bundesamtes für den Digitalfunk abgeordnet. Als Ersatz sucht das BMI derzeit anderswo nach weiteren IT-Fachleuten[10].

Ist diese Differenz zwischen Schein und Sein neu? Keineswegs. Die Erneuerung des aus den 70er Jahren stammenden IT-Systems INPOL[11] schlug in den letzten Jahren zunächst fehl. In den 16 Ländern plus dem Bund haben sich bei der Polizei diverse parallele Systeme etabliert, deren Zusammenwirken immer nur begrenzt funktionierte. Dasselbe gilt für die Erneuerung diverser anderer Systeme[12] bzw. die Entwicklung neuer IT-Systeme etwa für die Steuerverwaltung[13].

Soweit Gespräche mit IT-Fachleuten aus Sicherheitsbehörden einen Schluss zulassen, haben dort die Kenntnisse in Sachen IT und vor allem zum Internet in den letzten fünf Jahren zugenommen. Wenn heute das Zollkriminalamt als Variante des *Bundestrojaners* Keylogger einsetzt, um verschlüsselte Internet-Telefonie zu überwachen[14], zeigt das – lässt man einmal die fehlende Rechtsgrundlage und die Missachtung des Bundesgerichtshofes

beiseite – immerhin einen Kompetenzfortschritt gegenüber der mittlerweile nicht länger geäußerten Forderung aus den 90er Jahren, nur staatlich kontrollierte Kryptiersysteme zuzulassen.

Bei aller Begrenztheit der Einblicke in die IT-Fähigkeiten der Polizeibehörden entsteht dennoch der Eindruck, dass es dort nur sehr wenige Fachleute mit Kompetenzen in Sachen IT gibt. Von den geringen Personalkapazitäten steht zudem nur ein kleiner Teil für die Erfordernisse der Verfolgung terroristischer Aktivitäten zur Verfügung. Verbreitet ist immer noch der Umstand, dass Fahnder auf begrenzte interne und externe Kapazitäten bzw. Gutachter zur Analyse von Datenflüssen zurückgreifen müssen, um aus Dateien, aus offenem Internet-Verkehr oder aus überwachter Telekommunikation mehr oder weniger sachverständige Erkenntnisse zu ziehen.

Wenn also Deutschland bisher kein Attentat größeren Umfangs verzeichnen musste, so dürfte dieser Erfolg eher auf *klassische* Polizeiarbeit und Hilfe von befreundeten Diensten zurückzuführen sein, denn auf Polizeiarbeit, die – im Informatik-Sinn – IT-Systeme gezielt als Werkzeug oder Quelle einsetzt.

Während die Politik über Online-Durchsuchung, Internet-Überwachung und andere Formen der Hightech-Kriminalitätsbekämpfung redet und die Abschaffung von Grundrechten fordert, sind die Polizeibehörden in aller Regel überfordert, wenn es um den Einsatz von Computern und Internet geht. Weder gesetzgeberische Maßnahmen noch der Einsatz von 44 Mio. € in 2008 zur Fortführung des Programms zur Stärkung der Inneren Sicherheit (PSIS)[15] werden an diesem grundsätzlichen Kapazitäts- und Qualifikationsproblem der Sicherheitsbehörden irgend etwas ändern – im Gegenteil: Weitere Befugnisse werden die knappen Personalressourcen weiter überdehnen.

Zugespitzt formuliert: Der Bundesinnenminister setzt sich mit seinen Vorstößen zur Online-Durchsuchung und anderen Vorschlägen ungerührt dem Vorwurf aus, die Verfassung aushebeln zu wollen, um der Polizei neue Befugnisse zu verschaffen, die diese kaum nutzen kann. Die Polizei verfügt nicht einmal über die Ressourcen, um auf herkömmliche Weise Aufklärung zu treiben.

Der kurze Weg zu mehr polizeilichen Experten ist verbaut, weil die Fahndung nach Terroristen im Internet einerseits technische Expertise erfordert und andererseits vergleichsweise seltene Sprachkenntnisse, die zur Bewertung noch dazu spezifisches kulturelles und soziales Hintergrundwissen benötigen. Diese Kompetenzen aufzubauen dauert Jahre.

Bei der Online-Durchsuchung kommt hinzu, dass der Beweiswert von Erkenntnissen daraus vor Gericht minimal ist, da dieses Einsatzmittel darauf beruht, den angegriffenen Computer und die Daten darauf zu manipulieren. Die Online-Durchsuchung ist daher nur zur Verdachtsgenerierung und zur Informationsgewinnung geeignet.

Als ebenso wohlfeile wie falsche Erklärung bieten sich politische Verschwörungs- und andere Theorien an, bei denen versucht wird, Nichtstun mit geheimen Motiven zu erklären. Nichts zu tun und statt dessen rein verbal politische Themen anzureißen und zu besetzen, ist für die Politikwissenschaft das klassische Muster der *symbolischen Politik*. Dabei werden politische Symbole diskutiert, aber nicht in politisches Handeln umgesetzt, oder öfter: Handeln wird durch Worte ersetzt.

Verschwörungstheorie und politischer Zynismus kulminieren in der zur Erklärung untauglichen Unterstellung, konservative Politiker der inneren Sicherheit folgten der perfiden Logik, eine schlecht ausgestattete Polizei könne ihre Arbeit nicht angemessen verrichten und damit die Sicherheitslage nicht entschärfen. Sie förderten durch die andauernde Bedrohungslage den Ruf nach einem starken Staat und von Grundrechten *befreiten* Bürgern. Keiner dieser Denkansätze funktioniert jedoch in der politischen Praxis, wenn es um potenzielle oder womöglich erfolgte Terroranschläge geht, deren Hintergründe samt aller dabei begangenen politischen Fehler zumeist recht genau aufgeklärt werden. Unser politisches System ist beileibe nicht so verlottert, dass die zuständigen Minister und die Behördenleiter eine nachträgliche Untersuchung ihrer Fehler ungestraft – ohne Rücktritt – überstehen.

Camouflage und potemkinsche Dörfer

Ein tauglicheres Bild für die Differenz zwischen schwacher Leistung und geräuschvoll vorgeschobener Kulisse von Grundrechtsabbau zur Online-Durchsuchung ist das potemkinsche Dorf: Solange auf der politischen Bühne der heftige Disput um die Einschränkung unserer Grundrechte geführt wird, fragt niemand nach den realen Grenzen der polizeilichen Handlungsfähigkeit. Denn immer noch sind die alten Formen der Ermittlungstätigkeit entscheidend für polizeiliche Erfolge.

Die Logik dieser Schachzüge ist perfider: Die Verfassung wird geschleift, um zu verbergen, dass in den vergangenen Jahren gar nicht oder nicht an den richtigen Stellen in Kompetenz investiert wurde, um heute gegen Terroristen mit herkömmlichem polizeilichen Handeln erfolgreich zu sein. Ermitteln, Befragen, Auswerten – das Denken bei der Ermittlungsarbeit – ist Sache von Menschen, nicht von Computern. Wer heute schon nicht genug Beamte hat, um die offenen Quellen im Internet auszuwerten, wird ganz sicher nicht genug haben, um per Online-Überwachung die Festplatten all jener zu durchsuchen und auszuwerten, die zu recht oder zu unrecht für verdächtig gehalten werden. Und wie schon mit ihren bestehenden Befugnissen wird die Polizei – auch wenn die Grundrechte denn dezimiert sind – nicht in der Lage sein, ihre neuen Aufgaben zu erfüllen.

Seit über 10 Jahren sind die Ermittlungsbehörden kaum voran gekommen bei der Bekämpfung von Kriminalität mit Hilfe der IT. Seit den terroristischen Anschläge 2001 sind die Polizeibehörden weiter geschrumpft, das notwendige Expertenwissen für die Strafverfolgung wird auch in absehbarer Zeit nicht zu Verfügung stehen. Bei diesen Voraussetzungen kann keine Verfassungsdebatte schrill genug sein, um von solchen kolossalen Versäumnissen abzulenken. Und so entlarvt sich letztlich die konservative Versprechung eines *Rechts auf Sicherheit* als Verwahrlosung von Recht *und* Sicherheit, gibt es in ihr doch weder Sicherheit noch Recht.

Hans-Georg Wischkowski ist Informatiker und arbeitet als Berater und freier Publizist.

Quellen

1 *BMI: Bekämpfung des Terrorismus; http://www.bmi.bund.de/cln_028/nn_165104/Internet/Content/Themen/Terrorismus/DatenundFakten/Bekaempfung__des__Terrorismus__Id__93040__de.html*
2 *ebd.*
3 *ebd.*
4 *So der GdP-Vorsitzende Konrad Freiberg auf dem Gewerkschaftskongress am 10. 11. 2006 in Berlin*
5 *Der Discount-Krieg, in: Der Spiegel, Nr. 41,, 2007, S. 32-38, S. 36ff*
6 *Veröffentlichung des Verfassungsschutzberichts 2006. Rede von Bundesminister Dr. Wolfgang Schäuble anlässlich der Vorstellung des Verfassungsschutzberichts 2006 am 15. Mai 2007 in Berlin. Siehe: http://www.bmi.bund.de/nn_662956/Internet/Content/Nachrichten/Reden/2007/05/BM__VBS.html*
7 *Virtuelle Front; in: Der Spiegel, Nr. 30, 2007, S. 26 – 27, S. 27*
8 *http://www.bmi.bund.de/cln_028/nn_165104/Internet/Content/Themen/Terrorismus/DatenundFakten/Gemeinsames__Terrorismusabwehrzentrum__de.html*
9 *ebd.*
10 *Vgl. u.a. das Stellenangebot des BKA für ein Team „zur Untersuchung von Straftaten im Zusammenhang mit Computernetzwerken" in der c't, Nr. 20, 2007 S. 267*
11 *Nach einem abgebrochenen ersten Projekt zu INPOL-neu nahm der Bund 2003 eine weiterentwickelte Software der Länder Hessen und Hamburg in Betrieb. Vgl.: „Schily: Umstellung auf neues Polizei-Computersystem abgeschlossen"; www.heise.de/newsticker/meldung/39512*
12 *Jüngstes Beispiel ist das „Streitkräftegemeinsame Führungsinformationssystem" der Bundeswehr, vgl.: Technisch k.o.; in: Der Spiegel, Nr. 5, 2007, S. 44*
13 *Die zur Entwicklung einer bei Bund und Ländern gemeinsam genutzten Software zur Abwicklung der Steuererhebung gegründete Firma fiscus wurde 2006 aufgelöst, vgl.: „Länder mit Vereinfachung von Finanzverwaltung gescheitert", http://www.heise.de/newsticker/meldung/67762*
14 *„Trojaner weiter im Einsatz"; in: Der Spiegel 41, 2007, S. 17*
15 *Monatsbericht des BMF, Juli 2007, S. 44; http://www.bundesfinanzministerium.de/lang_de/nn_17844/nsc_true/DE/Aktuelles/Monatsbericht__des__BMF/2007/07/070718agmb022,templateId=raw,property=publicationFile.pdf*

Thilo Weichert

Überwachung und Datenschutz –

Politik contra Bundesverfassungsgericht

Eine Umfrage anlässlich des Tags der Deutschen Einheit 2006 ergab, dass das Bundesverfassungsgericht mit 91% Zustimmung die höchste Wertschätzung im Lande genießt. Kurz dahinter rangiert mit 80% die Polizei. Weit abgeschlagen landeten der Bundestag und die politischen Parteien.[1] *Würden wir dieses Ergebnis – im demokratischen Vertrauen auf die politische Mündigkeit des Volks – auf die Wahrung der Bürgerrechte bei der Bekämpfung des Terrorismus übertragen, so müssten uns keine gesteigerten Befürchtungen plagen, erweist sich doch das Verfassungsgericht als Garant der Bürgerrechte, während die Gefahr von Regierung und Politik ausgeht, die sich geringen Zuspruchs erfreuen. Dass es in demokratisch regierten Staaten nicht immer so freiheitlich zugeht, wissen wir aus den USA, in denen selbst minimale Akzeptanz einen Präsidenten und dessen Regierung bisher nicht daran hinderten, bei der Terrorismusabwehr die bürgerlichen Freiheiten mit Füßen zu treten – und dies weitgehend unbeschadet von gerichtlichen Korrekturen.*

Demokratische Staaten weisen nun einmal komplizierte Strukturen auf, bei denen es aus guten Gründen nicht immer auf die Mehrheiten ankommt. *Gewaltenteilung und Gewaltenkontrolle* wirken als Korrektive, die politischen Freiraum mit Beschränkung kombinieren. Dabei wirken die Korrektive nicht präventiv und erziehend, sondern oft erst nach Jahren und sanktionierend. In Bürgerrechtskreisen wird dies immer wieder beklagt, erweist sich doch die Politik oft als von wenig rechtsstaatlichem Bewusstsein beseelt. Beispiele sind dafür die staatliche Terrorismusbekämpfung und der Schutz des Grundrechts auf informationelle Selbstbestimmung. Sie können einen geradezu zur Verzweiflung bringen, wenn man nicht eine Gelassenheit aufbringt, die auf die Selbstheilungskräfte unserer Demokratie vertraut.

Ein *Blick in die Geschichte* und über den Tellerrand des 11. September 2001 hinaus lehrt uns, dass wir heute in liberaleren Zeiten leben als zuvor. Dabei müssen wir nicht unbedingt zurück in das Kaiserreich, die Weimarer Republik oder den kalten Krieg gehen, gar nicht zu reden von der Zeit des Nationalsozialismus oder der realsozialistischen DDR-Diktatur. Noch in den 70er und 80er Jahren erlebten wir heute kaum vorstellbare politische Repression. Ein differenzierter Blick zeigt aber, dass wir heute bürgerrechtlich in einer mittelmäßigen Demokratie leben und das Mittelmaß der Feind des Guten ist. Von einer katastrophalen Situation kann zwar nicht gesprochen werden; Entwarnung ist aber ebenso wenig angesagt.

Dies kann eindringlich am *Umgang mit dem Recht auf informationelle Selbstbestimmung* erläutert werden. Dabei handelt es sich nicht um ein ehrwürdiges klassisches Freiheitsrecht, das auf eine lange Tradition zurückblicken kann, so wie dies etwa beim Recht auf Pressefreiheit oder auf Versammlungsfreiheit der Fall ist. Doch handelt es sich um ein Grundrecht, dem in unserer modernen Informationsgesellschaft eine zentrale Rolle zukommt: Unsere Informationsgesellschaft zeichnet sich gegenüber der vorangegangenen Industriegesellschaft dadurch aus, dass fast jede Freiheitsbetätigung informationell vermittelt wird. Redefreiheit verwirklicht sich weniger auf Marktplätzen und in Versammlungssälen als im Internet. Gleichheit und Gerechtigkeit sind nicht mehr gelebte Solidarität sozial homogener Gruppen, sondern die Kombination von Diskriminierungsverboten und Kontrollmechanismen in den Dateien der Kranken-

versicherungen, der Rentenanstalt oder der Bundesagentur für Arbeit. Freizügigkeit ist angesichts des globalen Verkehrs auch eine Frage der Verkehrsüberwachung, z.B. mit Hilfe von elektronischen Mautsystemen und *Passenger Name Records.* Bedrohung für politische Verfolgte geht von elektronischen Akten bei und internationalem Datenaustausch zwischen Polizeien und Geheimdiensten aus. Selbst die Religionsfreiheit manifestiert sich nicht nur im Kirch- oder Moscheebesuch, sondern auch in der Speicherung der Religionszugehörigkeit in polizeilichen Dateien und Dossiers.

Die Entwicklung des Rechts auf informationelle Selbstbestimmung

Dieser Wahrheit öffnete sich früh unser deutsches Bundesverfassungsgericht (BVerfG). Zwar ist das moderne Konzept des Datenschutzes, der *Privacy*, über 100 Jahre alt und geht wesentlich auf die US-Supreme-Court-Richter Warren und Brandeis zurück. Doch war es das Bundesverfassungsgericht, das knapp 80 Jahre später im Volkszählungsurteil[2] aus dieser Einsicht ein stimmiges Grundrechtskonzept entwickelte und seitdem konsequent anwendete und weiterentwickelte. Es erwies sich damit weltweit als Pionier, dem selbst anerkannte internationale Gerichte wie der Europäische Menschenrechtsgerichtshof in Straßburg oder der Europäische Gerichtshof in Luxemburg erst mit großer Verzögerung folgten. Diese beiden europäischen Gerichte sind auch auf dem Weg, das allgemeine Persönlichkeitsrecht und den Schutz der Privatsphäre zu einem Recht auf informationelle Selbstbestimmung weiterzuentwickeln, obwohl sie teilweise von völlig anderen Rechtstraditionen beeinflusst werden.[3]

Das BVerfG näherte sich dem nun entbrannten vermeintlichen Konflikt zwischen Terrorismusbekämpfung und Datenschutz mit zunächst eher unverdächtigen Entscheidungen. Das Verbot der Datenverarbeitung auf Vorrat und die Grundsatzentscheidung zum Recht auf informationelle Selbstbestimmung ergingen im sicherheitspolitisch unverdächtigen Bereich der Statistik.[4] Auch die Weiterentwicklung des Grundrechts erfolgte nicht im spezifischen Sicherheitsrecht. Dies ist wohl auch dem Umstand zuzuschreiben, dass die 90er Jahre, also die Zeit nach der Volkszählungsentscheidung 1983 und vor dem 11. September 2001, sicherheitspolitisch eher als eine liberale Zeit eingestuft werden können. Es gab zwar neue Eingriffsmöglichkeiten für Sicherheitsbehörden, sie blieben aber in einem vertretbaren Rahmen. Die Entscheidungen zum Datenschutz im Sicherheitsbereich stammen aus der jüngsten Zeit. Sie ergingen übrigens nicht nur vom BVerfG, sondern auch von Landesverfassungsgerichten.

Grundlagen der Verfassungsentscheidungen sind zwei unterschiedliche Konstellationen. Zum einen geht es um die – quasi letztinstanzliche – Entscheidung über einzelne Ermittlungsakte von Sicherheitsbehörden. Diese Rechtsprechung steht weniger im Fokus politischer Wahrnehmung, wenngleich hierbei teilweise dogmatische Grundlagen erarbeitet werden, die direkte Auswirkungen auf die Gesetzgebung haben. Bei der zweiten Kategorie von Entscheidungen geht es um die politisch hochbrisante Überprüfung der Verfassungskonformität von Sicherheitsgesetzen. Aus der Zeit vor dem 11. September 2001 will ich nur drei Entscheidungen erwähnen, die Leitcharakter für die Zeit danach hatten: 1995 entschied das BVerfG zur strategischen Fernmeldeüberwachung, einer klassischen sicherheitsbehördlichen, geheimen Jedermann-Kontrolle, und definierte dabei enge materielle und prozedurale Grenzen.[5] Dass sich auch die Verfassungsgerichte der Länder einer vereinfachenden Sicherheitslogik entziehen, das bewiesen der Verfassungsgerichtshof von Sachsen, der 1996 zentrale Regelungen des Polizeirechts, insbesondere den Einsatz verdeckter Ermittlungsmethoden, als verfassungswidrig aufhob[6], und der von Mecklenburg-Vorpommern, der 1999 die Schleierfahndung verwarf.[7]

Die verfassungspolitischen Leitentscheidungen des BVerfG zum Verhältnis Sicherheit und Datenschutz ergingen nach 2001. Dies sind die beiden Entscheidungen zum Lauschangriff und zur präventiven Telekommunikationsüberwachung nach dem Außenwirtschaftsgesetz vom 3. März 2004[8], die Zurückweisung der präventiven Telefonüberwachung im Niedersächsischen Sicherheits- und Ordnungsgesetz vom 27. Juli 2005[9] und die Rasterfahndungsentscheidung vom April 2006[10]. Auch Landesverfassungsgerichte trugen zur kritischen Sicht einer neuen Sicherheitspolitik bei. So wurden in Sachsen 2003 und 2005 das Polizeigesetz und das Verfassungsschutzgesetz für teilweise verfassungswidrig erklärt wegen der mangelnden Benachrichtigung Betroffener bzw. zu weit gehenden Ermittlungsbefugnissen im Gefahrenvorfeld.[11] Bemerkenswert ist zudem eine Entscheidung des Bayerischen Verfassungsgerichtshofs, eines Gerichts, das Sicherheitsargumenten immer zugänglicher war als andere, das 2003 zwar die Schleierfahndung gehalten hat, hierfür aber enge Grenzen definierte.[12]

Aus bürgerrechtlicher Sicht muss aber Wasser in den bisher kredenzten Wein gegossen werden: Die Verfassungsgerichte haben manch angreifbares Gesetz gehalten und manche dogmatische Vorgabe gemacht, die Anlass zum Widerspruch ist. So begrenzte das BVerfG den Schutz des Telekommunikationsvorgangs (in Verkennung der realen Einflussmöglichkeiten der Betroffenen auf die technischen Abläufe) auf den reinen Telekommunikationsvorgang. Der Eingriffscharakter rein technischer Überwachung wurde relativiert.[13] Das Zeugnisverweigerungsrecht von Journalisten erstreckt sich nicht auf die telekommunikative Informationsbeschaffung.[14] Zwar gab es einige kategorischen Festlegungen durch die Verfassungsgerichte, etwa in

Thilo Weichert

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

Bezug auf den Kernbereichsschutz, doch wurden der Effektivität der Strafrechtspflege sowie dem Gefahrenabwehrinteresse, also generell dem Aspekt der „inneren Sicherheit“ immer eine hohe Wertigkeit zugewiesen und die Entscheidungen erst nach einer Verhältnismäßigkeitsprüfung getroffen.

Politische Reaktionen

Die Reaktion der Politik auf die Verfassungsgerichtsentscheidungen hat sich in jüngster Zeit geändert: Das klassische Muster war, dass auch kritische Entscheidungen aus Respekt vor der Würde der Gerichte begrüßt wurden. Argumente für Sicherheit und Effektivität der Strafrechtspflege wurden gewürdigt und erlangte Rechtssicherheit begrüßt.

Dieses Reaktionsmuster scheint seit den Entscheidungen zu Lauschangriff und Rasterfahndung nicht mehr durchgängig zu gelten. So befand der brandenburgische Innenminister Jörg Schönbohm: „Das Gericht muss umdenken. Auch in Karlsruhe muss man zur Kenntnis nehmen, dass wir eine neue Gefährdungslage haben, die sich von der betulichen Kriminalitätslage des Kalten Kriegs grundlegend unterscheidet“. Deutlicher der rechtspolitische Sprecher der CDU/CSU-Bundestagsfraktion Jürgen Gehb: „Ich habe den Eindruck, dass einige Richter seit Jahren ihren Elfenbeinturm nicht mehr verlassen haben.“ Innenminister Wolfgang Schäuble äußerte gegenüber Verfassungsrichtern anlässlich eines gemeinsamen Abendessens, diese hätten den Sicherheitsbehörden mit dem großen Lauschangriff ein sehr wirkungsvolles Instrument aus der Hand geschlagen.[15]

Die dabei zum Ausdruck kommende historische Sicht ist einfach falsch. In den 60er Jahren lauerten Kommunisten angeblich noch überall, nicht nur, um einzelne Straftaten zu begehen, sondern um unsere rechtsstaatliche Ordnung insgesamt zu stürzen. Und in den 70er Jahren war der Terrorismus der RAF real wie medial nicht weniger präsent als heute Al-Quaida und der islamistische Terror. Wie dem auch sei: Die Politiker wie auch viele Medien vermitteln den Eindruck, als habe das Bundesverfassungsgericht jedes Mal, wenn es zwischen dem Datenschutz des Einzelnen und den Sicherheitsinteressen der Allgemeinheit entschieden habe, sich im Zweifel für Ersteren entschieden.[16] Dieser Eindruck trügt. Es ist vielmehr so, dass die Gerichte praktisch sämtliche Maßnahmen im Rahmen einer Verhältnismäßigkeitsprüfung grundsätzlich zugelassen, und dann materiell- und prozessrechtlich, technisch oder organisatorisch eingeschränkt haben. Von einer Gefahr, dass der Staat wehrlos würde[17], kann keine Rede sein.

Rollen

Verfassungsrichter sind – so will es unsere Rechtsordnung – weitestgehend unabhängig, anscheinend zum Leidwesen manches Politikers. Sie sind weniger öffentlichen Stimmungen zugänglich als rationalen Argumenten. Sie sollen die objektiven Vorgaben unseres Grundgesetzes auf die aktuellen Realitäten anwenden, nicht aus subjektiver Betroffenheit medialem Alarmismus oder Regierungsmeinungen folgen. Das BVerfG verfolgt – neben der Funktion, Einzelfallgerechtigkeit herzustellen – vor allem die Aufgabe, langfristig den Bestand der Wertstrukturen unserer Gesellschaft zu wahren. Anders als die Politik, die auf durch markige Formulierungen erlangte, kurzfristige Aufmerksamkeit der Öffentlichkeit abzielt, ist beim BVerfG eine umfassende Abwägung das Mittel der Wahl, die sich in Dogmatik und bisherige Rechtsprechung einpasst oder diese weiterentwickelt.

Politiker unterliegen einer völlig anderen Denklogik. Sie müssen Entscheidungsfähigkeit signalisieren. Sie müssen den Sicherheitsbehörden wie auch der Bevölkerung das Gefühl vermitteln, dass sie alles Erdenkliche für die Sicherheit der Menschen tun. Dennoch setzt die Verfassung der symbolhaften entscheidungsstarken Aktion Grenzen. Dies musste erst jüngst der SPD-Bürgermeisterkandidat in Hamburg erkennen, als er einen Internetpranger für Sexualstraftäter forderte.[18] Der Einsatz gegen Kriminalität allgemein und gegen den Terrorismus speziell bleibt ebenso wie der Einsatz für Leben und Freiheit, für Wohlstand, Gerechtigkeit usw. konkretisierter Einsatz für die in unserer Verfassung garantierten Werte. Dies ist – hierüber müssen wir froh sein – nicht nur die Wahrnehmung einiger idealistischen Bürgerrechtsfanatiker, sondern allgemeiner Standard im Bewusstsein der Bevölkerung. Verfassungspatriotismus setzt die Identifikation der Menschen mit einem äußerst abstrakten Wertegefüge voraus. Diese Identifikation findet heute in einem großem Maße statt, wobei die Menschen ihren relativen wirtschaftlichen Wohlstand mit der Verteidigung dieses Wertegefüges verbinden.

Für einen bürgerlichen Politiker ist es fatal, wenn ihm glaubhaft nachgesagt wird, seine Politik verstoße sehenden Auges gegen die Verfassung. Der *Verfassungsfeind*, der seit Bestehen der Bundesrepublik als Ausgrenzungsmerkmal etablierter Politik diente, hängt heute wie ein Damoklesschwert über manchem Law-and-Order-Politiker. Die fließenden Grenzen zum real existierenden Rechtsextremismus müssen definitorisch und durch verbale Bekenntnisse klar gezogen werden. Die abstrakte Berufung auf die Verfassung gehört heute ebenso zum Pflichtprogramm wie die Vermittlung konkreter Ordnungskompetenz. Dabei wird zunächst die eigene Verfassungsinterpretation als Erklärungsmuster präsentiert. Diese lässt sich aber nicht mehr glaubwürdig vermitteln, wenn sie erkennbar in Widerspruch zu den Aussagen des Verfassungsgerichts steht, dem die Verfassung die Definitionsmacht des *Verfassungsgemäßen* zugesteht. Das musste beispielsweise der schleswig-holsteinische Innenminister Stegener erfahren, der meine Kritik an seinen Polizeirechtsvorschläge damit abtat, Thilo sei „allein zu Haus“ und dann bei der hierzu durchgeführten Parlamentsanhörung erfahren musste, dass sämtliche Gutachter – benannt von der CDU bis hin zum Südschleswigscher Wählerverband, vom ADAC über Richter- und Anwaltsverbände bis hin zur Polizeigewerkschaft – die Verfassungswidrigkeit seiner Pläne bestätigten. Eher verzweifelt beteuerte er weiter, sich in guter *Wohngemeinschaft* mit den Verfassungsrichtern zu befinden.[19]

Ist die Verfassung als Legitimation staatlichen Handelns in Deutschland heute unumstritten, so bedeutet das nicht, dass ihr Auftrag durchgängig ernst genommen würde. Wird der Politik allzu offensichtlich, dass sie sich mit ihren Vorschlägen außerhalb der eigenen Verfassung befindet, so bleibt ihr nur noch die Forderung nach der Änderung der Verfassung, was aber im Grundrechtsbereich auf hohe mediale Aufmerksamkeit und öffentlichen Widerstand stößt.[20] Politiker wie Bundesinnenminister Schäuble dürften zumindest ahnen, dass sie sich mit ihren Überwachungsforderungen außerhalb der Rechtsordnung stellen, wenn sie Äußerungen wie die folgende von sich geben: „Meine

Überzeugung ist, dass nationale Rechtsordnungen wie internationales Recht zu dieser neuen Form der Bedrohung im Grunde nicht mehr richtig passen".[21]

Die Politik bedient sich hierbei der Sprache der *Alltagsvernunft*. Ein gängiges Argumentationsmuster besteht darin, dass nach Betonung der Sicherheitsgefahren und der Bedeutung der Verfassung, auch des Rechts auf informationelle Selbstbestimmung, die eigene politische Forderung als die *mit Augenmaß* dargestellt wird, die dem gesunden Menschenverstand und dem Volksempfinden entspräche. Meinungsumfragen sind zur Verfassungsinterpretation wenig geeignet, schon gar, wenn spontane Empfindungen erfragt werden, über die es in der öffentlichen Diskussion bisher keine ausführliche Debatte gegeben hat. Tatsächlich findet derzeit noch eine sehr eingeschränkte, aber zunehmende Debatte über Datenschutz und Bürgerrechte in den öffentlichen Medien statt. Ihre Initiatoren und Beteiligten, etwa Datenschützer oder Bürgerrechtsorganisationen, werden immer noch allzu leicht als Außenseiter oder gar als idealistische, nützliche Helfer der Terroristen dargestellt.

Eine andere Rolle kommt in dieser Auseinandersetzung den Sicherheitsbehörden zu. Sie genießen hohe allgemeine Wertschätzung, die mit jeder gesetzlichen Befugnisausweitung nach Terroranschlägen oder sonstigen öffentlichkeitswirksamen Verbrechen bekräftigt zu werden scheint. Doch sind sich diese Stellen oft auch der damit verbundenen Probleme bewusst: Die Einräumung neuer technischer Überwachungsbefugnisse ist mit der Erwartung verbunden, dass sie auch genutzt werden, ob tauglich oder nicht. Mit diesen Befugnissen gehen oft überzogene Erwartungen einher, die von der Polizei nicht erfüllt werden können. Sie verschlingen u.U. – personell wie finanziell – Ressourcen, die an anderer Stelle sinnvoller eingesetzt werden könnten. Uferlose Befugnisnormen verunsichern die Polizeibeamten ebenso wie die betroffenen Bürgerinnen und Bürger. Komplizierte und unklare Normen fördern die Fehlanwendung und rechtliche Angreifbarkeit konkreter Maßnahmen. Hinzu kommt eine wichtige Veränderung des sicherheitsbehördlichen Selbstverständnisses. Vielen bei der Polizei passt das überkommene Image als Kontrolleur und Überwacher nicht mehr. In der praktischen Arbeit reduziert es nämlich die soziale Kontrolle durch die Bevölkerung und ihre Kooperationsbereitschaft und löst Abwehrhaltungen aus. Es kommt daher nicht von ungefähr, dass die Polizeivertreter bei der Anhörung zur Novelle des schleswig-holsteinischen Polizeirechts weitgehend in das gleiche kritische Horn stießen wie Datenschützer und Juristen.[22]

Die Bedeutung der Technik

Während die klassischen Freiheitsrechte eine relativ hohe rechtliche Beständigkeit aufweisen, trifft dies für die informationellen Freiheiten nicht zu. Das muss nicht Ausdruck einer permanenten Einengung des Grundrechts auf informationelle Selbstbestimmung sein, so wie es von manchen Bürgerrechtlerinnen und Bürgerrechtlern wahrgenommen wird. Vielmehr ist es zunächst einmal eine natürliche Folge des technischen Fortschritts: Solange es den genetischen Fingerabdruck zur Täteridentifizierung nicht gab, musste er auch gesetzlich nicht geregelt werden. Solange Funkzellenabfragen zur Personenlokalisierung keinen Erkenntniswert versprachen, gab es keinen rechtlichen Bedarf an einem solchen Ermittlungsinstrument. Weitere Beispiele sind Videoüberwachung, IMSI-Catcher oder die Kfz-Kennzeichenerkennung. Manche dieser Maßnahmen sind – kontrolliert angewendet – sicherheitsbehördlich sinnvoll und können bürgerrechtsverträglich geregelt und eingegrenzt werden. Vorsichtige Befugnisregelungen können, wenn Erfahrungen mit einem neuen technischen Werkzeug vorliegen, u.U. später weniger restriktiv gefasst werden. Ein Beispiel hierfür ist die Nutzung von DNA-Markern zur Täteridentifizierung bei der Strafverfolgung.[23] Es wäre politisch nicht verantwortlich, den Sicherheitsbehörden Befugnisse vorzuenthalten, die einen effektiven Beitrag zur Verbesserung der Sicherheitslage versprechen, ohne unverhältnismäßig in Bürgerrechte einzugreifen.

Zweifellos traf nie das traditionell und bis heute kolportierte Bild der Polizei zu, sie müsse auf dem Fahrrad Verbrecher fangen, die im Porsche unterwegs seien. Die Technikentwicklung verändert sowohl die Erscheinungsformen der Kriminalität wie auch deren Bekämpfung. Dass technische Möglichkeiten in der Praxis nicht in Anspruch genommen wurden, lag oft genug nicht an fehlenden Befugnisnormen, sondern am mangelnden technischen Know-how der Sicherheitsbehörden oder auch daran, dass sich die Behörden von deren Nutzung keine entscheidenden Erkenntnisgewinne versprachen. Unbestreitbar bleibt, dass im Interesse bestimmter Eingriffsnormen neue Ermittlungsmöglichkeiten u.U. einer ausdrücklichen gesetzlichen Regelung zugeführt werden müssen.

Dabei darf man nicht aus dem Auge verlieren, dass neue Informationstechnologie weit mehr kann als der polizeilichen Praxis zugestanden werden darf. Technisch wäre die dauernde Rundumüberwachung aller Menschen kein Hexenwerk mehr, dank Video, Biometrie, RFID, Telekommunikationsüberwachung, GPS, Internetauswertung, Chips, Datenbankabfragen ... In Deutschland besteht – anders als etwa in angelsächsischen Staaten – ein großer gesellschaftlicher Konsens, dass eine solche Rundumüberwachung unerwünscht und aus Gründen des Freiheitsschutzes eine Tragödie wäre.[24] Die Grenzen auszuloten, ist angesichts der technischen Details oft nicht einfach und eine dauernde politische und gesellschaftliche Herausforderung.

Die Politik ist dabei gerne bereit, mehr zuzulassen, als später vom BVerfG noch als akzeptabel angesehen wird. Dies hat mehrere Gründe: Die Bürgerrechtspolitik wird von Innen- und Justizministern gemacht, die zugleich oberste Polizei- und Strafverfolgungschefs sind, was zwangsläufig zu einer gewissen professionell bedingten Einseitigkeit führt. Die derzeitige Generation der Innen- und Rechtspolitiker ist zwar technikgeneigt, aber zugleich von wenig Technikverständnis beseelt. Die Begeisterung ist leicht zu wecken, eine praktische oder gar kritische Durchdringung der geförderten Technik ist meist nicht feststellbar.

Technologie ist das *Schmiermittel* unserer Gesellschaft, unserer Wirtschaft, unseres Wohlstands. Weshalb sollte es nicht auch als Schmierstoff der Sicherheit genutzt werden? Auch wenn die drei Antworten hierzu auf der Hand liegt, gehören sie nicht zum Repertoire vieler Politiker:

1. Technik ermöglicht es, in die intimsten Kernbereiche einzudringen, etwa ins Schlafzimmer, in die familiäre Kommunikation.

2. Technik ermöglicht die geheime Ausforschung, ohne Spuren zu hinterlassen.

3. Die Überwachungstechnik macht nicht am Verdächtigen oder an der Gefahrenperson halt, sondern ermöglicht die Erfassung von jedermann und jederfrau.

Die mit diesen drei Fakten verbundenen Risiken wurden von vielen deutschen Politikern bisher nicht erkannt. Wenig erkenntnisfördernd ist der Umstand, dass sich deutsche Regierungspolitiker mit denen anderer Staaten umgeben, die der selben Logik unterworfen sind wie sie selbst, und die Allmachtsphantasien erliegen, ohne von einem unabhängigen Verfassungsgericht immer wieder zur Ordnung gerufen zu werden.

Lernen könnten und sollten die deutschen von italienischen Politikern, denen derzeit gerade wieder bewusst gemacht wird, dass ihr intimstes, technisch aufgezeichnetes Liebesgeflüster an die Öffentlichkeit gezerrt werden kann.[25] Deutsche Politiker erleben sich nicht als potenzielles Opfer der Überwachung, sondern als Entscheider hierüber. Geheime Ermittlungen sind zumeist weit entfernt von der eigenen sinnlichen Betroffenheit. Die Privatsphäre vieler Politiker wird weniger durch sicherheitsbehördliche Informationstechnik bedroht als durch eine wohlwollende, aber dennoch gnadenlose Presse, die auch vor dem privaten Swimming Pool in Mallorca nicht Halt macht. Persönliche Betroffenheit kann sensibilisierend wirken, etwa, wenn der jetzige Ministerpräsident von Baden-Württemberg, Günter Öttinger, in den 80er Jahren als Besucher einer telefonüberwachten Pizzeria plötzlich mit Protokollen eigener Gespräche konfrontiert wird. Anders dagegen scheint die Überwachung von Angela Merkels Wohnung durch die Kameras des Sicherheitsdiensts des Pergamonmuseums in Berlin keine nachhaltige Bewusstwerdung zur Folge gehabt zu haben. Wahrscheinlich war sie dafür zu selten zu Hause.[26]

Der Blick eines Verfassungsrichters ist insofern weniger getrübt: Deren Privatleben ist bisher medial tabu. Eigene technische Kompetenz ist bei ihnen derzeit wohl ähnlich gering ausgeprägt wie bei Politikern. Sie setzen sich aber mit der gesellschaftlichen Realität elektronischer Überwachung im Gerichtsalltag eher auseinander als die Politik und erleben nicht nur das Ermittlungspotenzial moderner Technik, sondern auch die möglichen gravierenden Konsequenzen für die betroffenen Menschen. Am wichtigsten aber ist, dass die Erkenntnisquellen der Richter überlegen sind: sie können Experten laden, ausführlich über deren Expertise beraten und eine wohldurchdachte Entscheidung fällen. Welcher Minister kann sich heutzutage in der Sicherheitspolitik einen solchen Luxus leisten?

Tatsächlich wurde bisher noch keine Entscheidung des Bundesverfassungsgerichts von der Politik kritisiert, weil sie technisch unausgegoren wäre. Die unausgegorenen politischen Erklärungen und Entscheidungen, die zu informationeller Fremdbestimmung führen, würden dagegen dicke Bücher füllen und finden sich in fast jeder Tageszeitung. Die Patrouille auf der virtuellen Datenautobahn, von der ein Ex-Bundeskanzler noch in den 90ern fabulierte, unterscheidet sich eben von der auf der realen Autobahn.[27] Es ist Fakt, dass technisch versierte Kriminelle sich herkömmlicher elektronischer Überwachung entziehen können, nicht aber arglose Bürgerinnen und Bürger. Bei biometrischer Mustererkennung gibt es unvermeidbar noch hohe Fehlerquoten, die keine chirurgisch präzise Prävention oder Strafverfolgung zulassen. Die Politik hat noch nicht ausreichend verstanden, dass *intelligente Sicherheit* bzw. Strafverfolgung mit Informationstechnik einer Sicherheitsforschung bedarf, bei der (auch technisch) der Schutz informationeller Selbstbestimmung ein integraler Bestandteil sein muss. Ein beredtes Beispiel hierfür ist die Entscheidung der EU, die Speicherung von Telekommunikationsverbindungsdaten für mindestens ein halbes Jahr zwingend vorzuschreiben. Der damit verfolgte politische Wille passt weder in die technische Realität noch zum rechtsstaatlichen und freiheitlichen Auftrag unserer Verfassung. Ich prognostiziere noch eine lange, für die Politik leidvolle, aber hoffentlich erkenntnisfördernde Debatte zu diesem Thema für die nächsten Jahre.[28]

Ein Effekt von Überwachung auf die Sicherheit wird von Sicherheitspolitikern regelmäßig ausgeblendet – die aggressionsfördernde Wirkung diskriminierender Kontrollen und Überwachung. Auch hierüber gibt es – trotz aller Sicherheitsforschung – bisher kaum wissenschaftliche Erhebungen.[29] Die Geschichten der Attentäter von London sowie der Jugendlichen, die im August 2006 mit Kofferbomben in Deutschland Anschlagsversuche vornahmen, geben ernstzunehmende Hinweise. Die im Jahr 2002 bundesweit durchgeführte Rasterfahndung sollte daraufhin genau untersucht werden. Sie brachte – so das Eingeständnis der Polizei – keine sicherheitsrelevanten Erkenntnisse oder Ermittlungsansätze. Umso mehr verwiesen Polizisten wie Politiker auf die angeblich positive Wirkung des damit ausgelösten Ermittlungsdrucks auf die *Schläfer*. Dabei wird ignoriert, dass dieser Ermittlungsdruck weniger auf Schläfer ausgeübt wurde, deren Existenz bisher nicht erwiesen ist, als auf Angehörige einer großen gesellschaftlichen Gruppe, die als besonders terrorismusanfällig gilt: jung männlich, gebildet, islamischen Glaubens. Diese jungen Menschen wurden durch die Rasterfahndung nicht von bösem Tun abgehalten, sondern eher in die Arme von Hasspredigern getrieben, für die die Rasterung als Beleg ihrer menschenfeindlichen Thesen diente. Diese psychologische Dimension von Überwachung ist dem BVerfG bewusst und wird von Entscheidungen immer wieder angesprochen, nicht dagegen von unseren Law-and-Order-Politikern. Sie müssen sich daher die Frage gefallen lassen, ob nicht sie selbst und die von ihnen durchgeführten Maßnahmen ein Sicherheitsrisiko darstellen.

Allzu große Nachsicht für Politiker und deren Rolle ist nicht angesagt. Die Diffamierung des Eintretens für Grundrechte ist Ausdruck politischer, rechtlicher und moralischer Verrohung, gleichgültig, ob sich diese Diffamierung gegen einzelne Bürgerrechtler richtet oder gegen die Autorität des Verfassungsgerichts. Wer diese Rhetorik wählt, muss zurechtgewiesen werden. Er kann und soll dorthin gestellt werden, wo er steht, sei es als Verfassungsignorant oder gar als Verfassungsfeind.

Doch sollte niemand die Grundfesten unserer demokratischen Ordnung am Wanken sehen, wenn unsere Politiker das Verfassungsgericht dann wegen seiner Rechtsprechung kritisieren, wenn eindeutig verfassungswidrige politische Initiativen auf den Weg gebracht werden. Die Politik hat nur einen äußerst begrenzten Einfluss auf die Rechtsprechung des BVerfG – der Gewaltenteilung sei Dank. Zur Wahrnehmung der Freiheitsrechte gehört auch, das BVerfG kritisieren zu dürfen. Dies gilt übrigens nicht nur für die Politik, sondern auch für die Bürgerrechtler. Es gibt kritikwürdige Entscheidungen des BVerfG – auch in Sachen Datenschutz. Aber das ist eine andere Geschichte.

Quellen

1 *Frankfurter Rundschau 2.10.2006.*
2 *BVerfGE 65, 1 = Neue Juristische Wochenschau (NJW) 1984, 419.*
3 *Siemen, Datenschutz als europäisches Grundrecht, 2006.*
4 *Neben dem Volkszählungsurteil (Fn.2) schon 1969 im Microzensusurteil BVerfG NJW1969, 1707.*
5 *BVerfG NJW 1996, 114.*
6 *SächsVerfGH DuD 1996, 429, 493, 558.*
7 *Mecklenburg-Vorpommern LVerfG LKV (Landes- und Kommunalverwaltung) 2000, 149 = NJW 2000, 2016.*
8 *BVerfG NJW 2004, 999 und NJW 2004, 2213.*
9 *BVerfG NJW 2005, 2603.*
10 *BVerfG NJW 2006, 1939.*
11 *SächsVerfGH U.v. 10.7.2003 Vf43-II-00; NJW 2005 3559 = Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2005, 1310.*
12 *Bayerischer Verfassungsgerichtshof (BayVerfGH) NVwZ 2003, 1375.*
13 *BVerfG NJW 2007, 351 (IMSI-Catcher).*
14 *BVerfG 2003, 1787 (Schneider).*
15 *Fleischhauer/Hipp/Schmidt, Der Spiegel 35/2006, 25.*
16 *So ausdrücklich Fleischhauer/Hipp/Schmidt, Der Spiegel 35/2006, 25; dagegen Baum/Hirsch/Leutheusser-Schnarrenberger, Der Spiegel 37/2006, 14.*
17 *Vgl. Haas in abweichender Meinung BVerfG NJW 2006, 1949.*
18 *DatenschutzNachrichten (DANA) 4/2006, 169; Hamburgs SPD-Chef Petersen musste v.a. wegen dieser Forderung zurücktreten.*
19 *Pressemitteilung Innenministerium Schleswig-Holstein (SH) 12. 1.2006; Giebeler Landeszeitung SH 29.06.2006.*
20 *Eine solche Verfassungsänderung erfolgte zwecks Einführung des „großen Lauschangriffs" im Jahr 1998; eine solche erwägt Bundesinnenminister Schäuble angesichts der aktuellen Entscheidungen des BVerfG zur Ermöglichung der Online-Durchsuchungen, DANA 2/2007, 82.*
21 *Netzeitung 4.7.2007, Schäuble stellt Weltordnung in Frage.*
22 *https://www.datenschutzzentrum.de/polizei/polizeirecht.htm.*
23 *Die Regelungen der §§ 81e ff Strafprozessordnung (StPO) wurden 1997 eingeführt und seitdem sukzessive erweitert, wobei das Maß jetzt voll sein dürfte, vgl. Lütkes/Bäumler ZRP(Zeitschrift für Rechtspolitik) 2004, 87.*
24 *BVerfG NJW 2005, 1941 (GPS-Ortung).*
25 *DANA 2/2006, 89, 4/2006, 180, 183, 1/2007, 76.*
26 *DANA 2/2006, 86.*
27 *Ein erschreckendes Beispiel für Technikunverständnis und die Annahme der Schicksalhaftigkeit von Überwachungstechnologie zeigte jüngst Generalbundesanwältin Harms, DANA 2/2007, 82.*
28 *Vgl. die Dauerberichterstattung in der DANA, z.B. Schwerpunktheft 2/2006; Pressemitteilungen in DANA 1/2007, 48 ff.; 2/2007, 95.*
29 *Siehe hierzu den Essay von Weichert, „Überwachung bringt nichts und macht aggressiv", Ossietzky 3/2006, 875; www.datenschutzzentrum.de/polizei/weichert-ueberwachung2.htm und FIfF-Kommunikation Sonderausgabe 2007.*

Klaus-Peter Löhr

Der Staat hackt mit

Mehr Sicherheit durch Bundestrojaner?

„Die meisten Menschen sind über Terrorismus und Kriminalität beunruhigt, nicht über polizeiliche Schutzmaßnahmen. Sie wollen, dass der Staat ihre Sicherheit garantiert. Dazu muss er auch neue Technologien nutzen. Wir können nicht stehen bleiben, wenn das Verbrechen und der Terrorismus immer neue Kommunikationsmöglichkeiten zur Verfügung haben."

... so Innenminister Dr. Schäuble im Interview mit der *taz* vom 8.2.07. Zum Bündel der einschlägigen Initiativen des Innenministeriums (BMI) und des ihm unterstellten Bundeskriminalamts (BKA) gehört die sogenannte *verdeckte Online-Durchsuchung* der Rechner von Personen, die der Vorbereitung oder Durchführung von Straftaten verdächtigt werden, zu Zwecken der Prävention oder Strafverfolgung. Verdeckte Online-Durchsuchung bedeutet, dass Polizei oder Strafverfolgungsbehörden sich über das Internet unbemerkt Zugang zum Rechner eines Verdächtigen verschaffen und dort Software installieren, mit der gespeicherte Daten ausgelesen werden können. Auch eine längerfristige Überwachung des Verhaltens des Benutzers ist auf diese Weise möglich.

Technische Grundlage: IT-Unsicherheit

Das unbefugte und unbeobachtete Eindringen in fremde Rechner über das Netz wird überhaupt erst dadurch möglich, dass die meisten Systeme nur unzureichend gegen solche Angriffe geschützt sind, bedingt durch Software-Mängel oder durch Nachlässigkeit der Benutzer. Der Einbruch in einen Rechner über das Netz ist insofern mit dem Einbruch in eine Wohnung zu vergleichen, die entweder ein schlechtes Schloss hat oder nicht richtig abgeschlossen ist.

Besonders problematisch ist, dass gerade populäre, weit verbreitete Systeme eine Vielzahl von Schwachstellen aufweisen, die von gewieften Hackern für erfolgreiche Angriffe ausgenutzt werden können. Da solche Angriffe schwerwiegende Folgen haben können – von Datenspionage bis hin zur Sabotage – sind sie natürlich strafbar. Erst kürzlich wurde mit der Erweiterung des § 202 Strafgesetzbuch (StGB) sogar die Entwicklung entsprechender Werkzeuge unter Strafe gestellt. (Siehe dazu die Presseerklärung des FIfF vom 16.7.2007.)

Zu beobachten ist andererseits, dass sich die Software-Entwickler zunehmend der Verantwortung für die Qualität ihrer Produkte bewusst werden. In der Informatik hat das Thema *IT-Sicherheit* endlich den gebührenden Stellenwert erhalten. Die Zukunftsvision sind sichere Systeme, die das gesetzliche Verbot der *Überwindung der Zugangssicherung* (§ 202a(1) StGB) entbehrlich machen würden – weil nämlich ihre Zugangssicherung unüberwindbar ist. Man kann darüber streiten, wie realistisch eine solche Vision ist; unstrittig ist, dass schon heute viel getan werden kann, um die Sicherheit unserer Systeme deutlich zu er-

höhen. Damit würden womöglich auch die Initiativen für eine verdeckte Online-Durchsuchung ins Leere laufen; wir kommen später darauf zurück.

Was genau ist der *Bundestrojaner*?

Die vielen Schwachstellen in heutigen IT-Systemen sind von sehr unterschiedlicher Art, und dementsprechend gibt es eine Vielzahl unterschiedlicher Einbruchstechniken. Gemeinsam ist ihnen, dass der Angreifer versucht, *Schadsoftware* mit verdeckter Funktionalität auf dem Rechner zu installieren, die mehr oder weniger gravierende Auswirkungen haben kann (und im Übrigen auch als Basis für weitere Angriffe im Netz dienen kann). Eine grobe Klassifikation orientiert sich daran, ob ein spezifisches Benutzerverhalten die Voraussetzung für einen erfolgreichen Angriff darstellt, oder ob der Angreifer auch bei völliger Inaktivität des Benutzers Erfolg haben kann.

Letzteres ist bei einem nicht bereits mit Schadsoftware infizierten Rechner schwierig bis unmöglich (abhängig von der Sorgfalt, mit der der Eigentümer die vorgesehenen Schutzmechanismen einsetzt – wie etwa eine Firewall). Daher sind Angriffe beliebt, die auf die Unachtsamkeit des Benutzers im täglichen Umgang mit dem Rechner setzen. Jede Aktion des Benutzers, die einen Datenfluss aus dem Netz in den eigenen Rechner zur Folge hat, ist ein potenzielles Einfallstor für Schadsoftware.

Dieser Sachverhalt ist offensichtlich, wenn ich etwa ein attraktiv erscheinendes Programm aus dem World-Wide-Web herunterlade. Denn eigentlich müsste ich mir vorher die folgenden Fragen stellen – und beantworten: Worauf gründe ich mein Vertrauen, dass dieses Programm genau das tut (nicht mehr und nicht weniger), was mir versprochen wurde? Wenn es von Microsoft oder von XYZ kommt, vertraue ich Microsoft bzw. XYZ? Wenn ich es über eine Webseite beziehe, auf der Microsoft steht, worauf gründe ich mein Vertrauen, dass wirklich Microsoft für diese Seite verantwortlich ist?

Die meisten Menschen stellen sich diese Fragen nicht, mit dem Effekt, dass ihnen leicht etwas untergeschoben werden kann, was sie gar nicht haben wollten. Wenn sie das bei der Benutzung des Programms merken, ist es vielleicht schon zu spät, und das Programm kann bereits beträchtlichen Schaden angerichtet haben.

Tückischer sind Programme, die durchaus die versprochene Leistung erbringen, daneben aber noch eine verborgene, schädliche Funktionalität aufweisen, die lange unentdeckt bleiben kann. Ein solches Programm wird als Trojanisches Pferd – im Jargon Trojaner – bezeichnet.

Für die verdeckte Online-Durchsuchung sind Trojanische Pferde das ideale Vehikel: mit passender Funktionalität versehen und einmal eingeschleust, können sie alle möglichen Aktivitäten entwickeln, vom Durchsuchen der Festplatte über das Protokollieren von Tastatureingaben (keylogging) bis hin zur Kontaktaufnahme mit anderen Rechnern. Und selbstverständlich können sie in Kontakt mit ihrem Herkunftsort bleiben, gefundene Daten dorthin übermitteln und ferngesteuert ihr Verhalten verändern. Das geht so weit, dass über sie auch die am Rechner womöglich vorhandenen Mikrofone und Kameras gesteuert werden können (!).

Diese weitreichenden Möglichkeiten erklären, warum der Begriff *Bundestrojaner* mittlerweile zum Synonym für jegliche Schadsoftware für die verdeckte Online-Durchsuchung geworden ist. Zur Präzisierung muss gesagt werden, dass es *den* Bundestrojaner – im Sinne eines *universell* einsetzbaren Werkzeugs – nicht gibt. Für jeden Einzelfall – z.B. einen bestimmten Terrorverdächtigen – muss ein den spezifischen Umständen entsprechender Angriff konzipiert und mit erheblichem Aufwand ein maßgeschneidertes Trojanisches Pferd entwickelt werden. Das liegt an der Vielzahl der existierenden Systeme, ihren verschiedenen Varianten und Versionen, dem unvollständigen Wissen über die Installation bei dem Verdächtigen und nicht zuletzt an den Schwierigkeiten, dem Verdächtigen das Trojanische Pferd tatsächlich unterzuschieben – zumal wenn dieser Vorsicht walten lässt.

Nach einem Bericht der ARD vom 27.4.2007 wurden verdeckte Online-Durchsuchungen vom Bundesnachrichtendienst bereits in mehreren Fällen durchgeführt, und zwar auf der Grundlage einer vom früheren Innenminister Otto Schily erlassenen Dienstvorschrift.

Die Rechtslage

Eine vom Generalbundesanwalt beantragte verdeckte Online-Durchsuchung im Rahmen eines Ermittlungsverfahrens wurde vom Ermittlungsrichter des Bundesgerichtshofs (BGH) am 21.2.06 genehmigt, dann aber (vermutlich wegen technischer Schwierigkeiten) de facto nicht durchgeführt. Die Genehmigung erfolgte mit Bezugnahme auf §§ 105, 106 (Wohnungsdurchsuchung) der Strafprozessordnung (StPO). Ein zweiter Antrag des Generalbundesanwalts (u.a. wegen des Verdachts der Gründung einer terroristischen Vereinigung) wurde von einem anderen Ermittlungsrichter des BGH abgelehnt. Begründet wurde die Ablehnung damit, dass eine verdeckte Online-Durchsuchung einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung darstelle und durch die StPO nicht gedeckt sei, da die typischen Kriterien für eine Wohnungsdurchsuchung nicht erfüllt seien. Die gegen diese Entscheidung eingelegte Beschwerde des Generalbundesanwalts wurde vom 3. Strafsenat des BGH am 31.1.07 verworfen. Somit bleibt der Bundestrojaner bis zur Schaffung einer gesetzlichen Grundlage illegal.

Der Innenminister hat mittlerweile wiederholt deutlich gemacht, dass er den Bundestrojaner für unverzichtbar hält und daher in Abstimmung mit dem Justizministerium eine entsprechende Gesetzesinitiative auf den Weg bringen will. Vielfach wird bezweifelt, ob ein solches Gesetz vor dem Bundesverfassungsgericht Bestand hätte. Der Innenminister scheint entschlossen, wenn erforderlich auch eine Änderung des Grundgesetzes (Art. 13) anzustreben.

In diesem Zusammenhang ist auf die Situation in Nordrhein-Westfalen hinzuweisen. Der Landtag hat am 20.12.06 mit den Stimmen der Regierungskoalition (CDU und FDP) ein Gesetz verabschiedet, das einen Landestrojaner erlaubt: Der Verfassungsschutz des Landes Nordrhein-Westfalen darf unter bestimmten Bedingungen verdeckte Online-Durchsuchungen durchführen. Gegen dieses Gesetz sind zwei Verfassungsbeschwerden beim Bundesverfassungsgericht anhängig; eine Entscheidung wird für Anfang 2008 erwartet.

Sollte der Bundestrojaner legalisiert werden ...

... sind dann die an ihn geknüpften Hoffnungen von Polizei, Strafverfolgern und Verfassungsschützern überhaupt realistisch? Weiter oben wurde bereits darauf hingewiesen, dass das gezielte Installieren eines Trojanischen Pferdes keine einfache Sache ist. Kriminelle Organisationen verfügen heute über genügend informatische Kompetenz, um die Gefährdung ihrer Systeme durch Schadsoftware gut einschätzen zu können und sich entsprechend vorsichtig zu verhalten. Man kann davon ausgehen, dass ihre Systeme einen höheren Sicherheitsstandard aufweisen als die des Normalbürgers. Ein halbwegs intelligenter Terrorist wird vorsichtig genug sein, kein unbekanntes Programm aus dem Netz herunterzuladen. Wie können BKA-Ermittler trotzdem erfolgreich sein?

Am Beispiel der Viren, die einen Rechner befallen können, kann man sehen, dass man sich Schadsoftware auch ohne das bewusste Herunterladen von Programmen einfangen kann. Viele Benutzer wissen heute, dass man eine Anlage – z.B. ein Textdokument – zu einer E-Mail zweifelhafter Herkunft besser nicht öffnen sollte. Das Tückische bei dieser Art des Angriffs ist, dass man in einem Textdokument kein Programm vermutet. Dennoch kann ausführbarer Code in ihm verborgen sein, der durch das Öffnen des Dokuments aktiviert wird. Dieser Code realisiert typischerweise Makrobefehle zur Texteditierung und ist somit eine nützliche Sache. Er kann aber eben auch schädliche Funktionalität beinhalten. Traditionell ist das die Infektion des Rechners mit einem Virus, der sich über das Netz (z.B. wiederum über E-Mail) weiter verbreitet. Das BKA könnte diese Technik einsetzen, um Schadsoftware im Rechner eines Verdächtigen zu installieren; technisch läge in diesem Fall kein Virus vor (weil keine Weiterverbreitung), sondern eine Art Trojanisches Pferd. Allerdings ist es schwer vorstellbar, dass der intelligente Terrorist auf diesen wohlbekannten Trick hereinfällt – womöglich noch unter Ignorierung einer Warnung, die er vom Viren-Scanner beim Versuch erhält, die E-Mail-Anlage zu öffnen.

Für das Unterschieben von Schadsoftware gibt es aber noch raffiniertere Methoden. Auch beim Umherwandern im Web, also beim Betrachten von Webseiten mit Endungen .html oder .htm (die ja schließlich keine Programme sind) kann man sich Schadsoftware einfangen. Auch in Webseiten kann Programmcode eingebettet sein, sogar in noch viel flexiblerer Weise als man das von Textdokumenten her kennt. Diese Technik dient auch hier einem guten Zweck, ermöglicht sie doch interaktive Webseiten, die man nicht nur passiv betrachten kann. Den auch hier möglichen Missbrauch versucht man dadurch zu verhindern, dass der Browser, unter dessen Kontrolle der Code läuft, diesem Code ein nur sehr eingeschränktes Agieren erlaubt und somit schädliche Aktionen verhindert. Soweit die Theorie. Leider gibt es aber, wie in jeder komplexen Software, auch bei Browsern Schwachstellen, die einem raffinierten Angreifer ein Umgehen der Schutzfunktionen erlauben. Somit kann eine harmlos aussehende Webseite Code im Gepäck führen, der eine schädliche Wirkung entfaltet, ohne dass der Benutzer es merkt. Auch Webseiten können also wie Trojanische Pferde wirken.

Der schädliche Code muss nicht einmal direkt in der präparierten Seite enthalten sein (bzw. vom Server der Seite nachgeladen werden). Eine spezielle Direktive in einer Seite (das *<iframe> tag*) ermöglicht das Einbetten einer beliebigen anderen Seite – aus beliebiger Quelle – in einen Teilbereich der angezeigten Seite. Damit kann eine Seite so präpariert werden, dass beim Laden zusätzlich eine ganz andere Seite geladen wird, *und zwar unbemerkt,* denn für die Größe des Teilbereichs kann der Wert 0 eingestellt werden. Der Browser wendet sich dann nach dem Laden der ersten Seite an den Server des Angreifers, und von dort wird die Schadsoftware geladen, ohne dass der Benutzer es merkt.

Diese Technik kann dahingehend verfeinert werden, dass der Server des Angreifers, wenn er vom Browser des Opfers kontaktiert wird, Details über dessen Betriebssystem und den Browser abfragen kann. Mit diesem Wissen kann er, wenn er einen Fundus von Schadsoftware-Varianten für verschiedene Systeme vorhält, daraus die für das Opfer passende Variante wählen. Diese Idee wurde jüngst von einem russischen Hacker-Team umgesetzt und unter dem Namen *Mpack* auf den (kommerziellen!) Markt gebracht.

Treffen Sie irgendwelche Vorsichtsmaßnahmen, bevor Sie eine Webseite in Ihren Rechner holen? Sehen Sie sich die URL eines Links in der Fußzeile an, bevor Sie auf das Link klicken? Wenn ja, wie entscheiden Sie, ob sich dahinter eine vertrauenswürdige Webseite verbirgt? Vielleicht war die Seite ursprünglich vertrauenswürdig, ist aber inzwischen durch einen Hacker mit einer Schadfunktion versehen worden. Wenn die Seite über das https-Protokoll angesprochen wird, wiegen Sie sich dann in Sicherheit und klicken? Sie könnten anschließend – wenn Sie sehr sorgfältig sind – das Zertifikat des Webservers prüfen; der Schaden wäre dann aber schon eingetreten. Und auch ein einwandfreies Zertifikat garantiert nicht die Abwesenheit einer verborgenen unerwünschten Funktionalität.

All dies kommt dem verdeckten BKA-Ermittler entgegen (besonders so etwas wie *Mpack*). Wenn wir davon ausgehen, dass der vom Ermittler ins Visier genommene Terrorverdächtige beim Herumwandern im Web keine extreme Vorsicht walten lässt, muss der Ermittler nur noch dafür sorgen, dass der Verdächtige eine von ihm geeignet präparierte Webseite besucht.

Klaus-Peter Löhr

Prof. Dr.-Ing. Klaus-Peter Löhr ist Professor für Informatik a.D. an der Freien Universität Berlin, Fachbereich Mathematik und Informatik. Seine Fachgebiete sind Systemsoftware, Softwaretechnik und IT-Sicherheit. Er ist Mitglied des Präsidiumsarbeitskreises *Datenschutz und IT-Sicherheit* der Gesellschaft für Informatik.

Das ist allerdings leichter gesagt als getan und erfordert einiges *social engineering*. Die Kooperation mit den Betreibern beliebter Webserver – oder jedenfalls solcher, deren Seiten der Verdächtige vermutlich häufiger besucht – ist hilfreich; dort könnten dann eine präparierte Seite sowie dorthin verweisende *attraktive* Links auf anderen Seiten untergebracht werden. Spielt der Betreiber nicht mit, könnte der Ermittler versuchen, die Seiten heimlich entsprechend zu manipulieren (falls das vom Gesetz gedeckt wäre ...).

Das Ganze scheitert natürlich, wenn der Verdächtige das Herumwandern im Web vermeidet oder dafür einen anderen Rechner verwendet als den, auf dem seine sensiblen Daten liegen. Die professionell organisierte Kriminalität wird ohnehin ihre Systeme so organisieren, wie man das von sicherheitsbewussten Unternehmen kennt – mit mehrstufigen Firewalls zwischen Internet und Intranet, *entmilitarisierten Zonen*, sorgfältig nach Funktionalität getrennten Rechnern etc. Zu den weiteren Techniken, mit denen man den Ermittlern das Leben schwer machen kann, gehört natürlich auch die Verschlüsselung der Datenbestände. Die Durchsuchungssoftware muss dann über eine *Keylogging*-Funktionalität verfügen, die den Benutzer bei der Eingabe einer Passphrase für einen Schlüssel erwischt.

Der oben skizzierte Angriff auf einen Rechner ist nicht der einzig mögliche. Es können hier weder alle denkbaren Angriffe noch alle denkbaren Abwehrmechanismen gegen die verdeckte Online-Durchsuchung und auch nicht alle denkbaren Verfeinerungen und Erweiterungen des Bundestrojaners diskutiert werden. Die Liste der Möglichkeiten ist unbegrenzt – wie ja auch im täglichen Geschäft der Kampf zwischen dem IT-Sicherheitsexperten und dem Hacker dem Wettlauf zwischen Hase und Igel gleicht. Festzuhalten ist, dass die verdeckte Online-Durchsuchung einerseits technisch machbar ist (jedenfalls solange unsere Systeme Qualitätsmängel haben), andererseits aber trotz aller Automatisierungsmöglichkeiten ein schwieriges Unterfangen bleibt. Es ist wenig wahrscheinlich, dass der Bundestrojaner – so er denn kommt – bei ausgebufften Kriminellen erfolgreich einsetzbar sein wird.

Außer den beschriebenen gibt es noch zwei (vielleicht auch mehr) andere Ansätze für eine verdeckte Online-Durchsuchung. Erstens: der Staat könnte in die Infrastruktur des Internet eingreifen; ein Erfolg wäre angesichts der supranationalen Struktur des Internet allerdings zweifelhaft. Zweitens: der Rechner eines Verdächtigen könnte in dessen Wohnung direkt manipuliert werden (vergleichbar dem Verwanzen einer Wohnung). – Auch für derartige Ansätze existiert gegenwärtig keine Rechtsgrundlage.

Quo vadis, IT-Sicherheit?

Dass die Datenschutzbeauftragten, die Opposition im Bundestag, das FIfF, die Humanistische Union, der Chaos Computer Club etc. eine Legalisierung der verdeckten Online-Durchsuchung ablehnen, überrascht nicht; handelt es sich doch um einen weiteren Eingriff in Grundrechte (Unverletzlichkeit der Wohnung, informationelle Selbstbestimmung), einen Eingriff, dessen Verhältnismäßigkeit angesichts der nur mäßigen Erfolgsaussichten im Kampf gegen Schwerstkriminalität zweifelhaft erscheint. Die Position der Gegner wird bisweilen pointiert zusammengefasst durch den Satz „Die Regierung unterstützt die Terroristen bei der Abschaffung des liberalen Rechtsstaats". Auch die Medien zeigen sich weitgehend skeptisch bis ablehnend gegenüber den Plänen des Innenministers.

Bemerkenswert ist, dass auch informatische Fachverbände – die auf politische Neutralität achten – die Pläne dezidiert ablehnen. So hat sich die Gesellschaft für Informatik e.V. am 12.7.07 gegen eine Änderung des Art. 13 GG mit dem Ziel der Legalisierung des Bundestrojaners ausgesprochen. Nach einer Pressemeldung des IT-Unternehmensverbands Bitkom vom 23.4.07 lehnt auch die deutsche IT-Wirtschaft den Bundestrojaner ab. Die Fachverbände fürchten einerseits eine Schwächung von Bürgerrechten und Datenschutz (auch Schutz von Firmendaten) und andererseits bei IT-Sicherheitsprodukten Nachteile im internationalen Wettbewerb, die sich ergeben könnten, wenn es politischen Druck gegen zu viel IT-Sicherheit – weil nachteilig für die Ermittler – gibt.

Hier zeigt sich schlaglichtartig das Bizarre an der Diskussion um den Bundestrojaner. Wir alle wissen: IT-Systeme sind unsicher, erst recht im Netz. Dieser Mangel ist nicht naturgegeben, sondern menschengemacht. Die einschlägigen Unternehmen bekennen sich zu ihrer Verantwortung und versprechen Besserung. Wissenschaft und Technik arbeiten an sicheren Systemen. Etliche Unternehmen unterstützen die Initiative *Deutschland sicher im Netz e.V.,* die verkündet: „Der Verein wird die Zielgruppen, Hersteller und Betreiber ... informieren und sensibilisieren, aufklären und beraten sowie neue Schutzmaßnahmen identifizieren und etablieren, um die Sicherheit und das Vertrauen in das Internet und die Informationstechnologie zu stärken." Diese Initiative wird von der Regierung unterstützt. Der Innenminister, der für die Umsetzung des 2005 beschlossenen *Nationalen Plans zum Schutz der Informationsinfrastrukturen* zuständig ist, verkündete am 19.6.07: „Der Verein ‚Deutschland sicher im Netz e.V.' bündelt wichtige gesellschaftliche Akteure zum Thema IT- und Internet-Sicherheit und wird zukünftig ein bedeutsamer Partner für die Politik und alle gesellschaftlichen Gruppen sein. Deshalb werde ich die Arbeit des Vereins als Schirmherr gerne unterstützen".

Möchte der Minister nun nach Kräften die *IT-Sicherheit* befördern oder will er den Bundestrojaner, d.h. *IT-Unsicherheit*? Beides zu wollen, birgt die Gefahr der Schizophrenie. Zumindest stünde der Minister, wenn er seine Schirmherrschaft für *Deutschland sicher im Netz* ernst nimmt, in einem Zielkonflikt. Man tut ihm wohl nicht unrecht mit der Feststellung, dass er verdeckte Online-Durchsuchungen für wichtiger hält als die IT-Sicherheit. Das wirft im übrigen auch ein ungünstiges Licht auf das ihm unterstellte *Bundesamt für Sicherheit in der Informationstechnik* (BSI), das eigentlich bestrebt sein müsste, die Sicherheitslücken zu bekämpfen, die der Bundestrojaner ausnutzen soll.

Man könnte allerdings auch sagen, dass Herr Schäuble mit seinem Kampf um Troja, ob legalisiert oder nicht, den Kampf für mehr IT-Sicherheit jetzt schon erfreulich befördert hat. Die Informatik wird ihr Engagement gegen Schadsoftware verstärken, unabhängig davon, ob sie von Kriminellen oder vom BMI stammt. Ironischerweise ist in diesem Sinn die eingangs gestellte Frage „Mehr Sicherheit durch Bundestrojaner?" durchaus positiv zu beantworten.

Hilfreich für weitere Recherchen (Stand: 15.10.2007):

Wikipedia gibt einen knappen Überblick über die Materie, mit etlichen guten Verweisen: http://de.wikipedia.org/wiki/Bundestrojaner

Es gibt eine eigene Website zum Bundestrojaner: unter *http://www.bundestrojaner.de/* findet man aktuelle Nachrichten, ein Archiv, Stellungnahmen, Abwehrmaßnahmen und weiteres.

Sehr empfehlenswert – weil reich an Informationen, präzise und gut lesbar – ist der Aufsatz von Ulf Buermeyer, Die „Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, in HRRS: *http://www.hrr-strafrecht.de/hrr/archiv/07-04/index.php?sz=8*

Zum selben Thema siehe Hartmut Pohl, Zur Technik der heimlichen Online-Durchsuchung, in DuD – Datenschutz und Datensicherheit 31 (2007) 9, *http://www.dud.de/index.php;sid=b9be118ba4ddd5346739103ffa7e89cd/site=dud/do=show/id=471/alloc=122*

Dem juristisch interessierten Leser sei das Studium der BGH-Entscheidung vom 31.1.07 empfohlen: *http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=2007&Sort=3&Seite=9&nr=38779&pos=277&anz=514*

Der technisch interessierte Leser möchte sich vielleicht genauer über Mpack informieren:

http://www.symantec.com/enterprise/security_response/weblog/2007/05/mpack_packed_full_of_badness.html

http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/05/11/MPack.pdf?sitepanda=particulares

Vincent Brannigan

Email Privacy in the USA

Warshak v. United States

The 6th Circuit Court of appeals[1] has recently extended constitutional privacy rights to users of Email, determining that a statute that permitted secret access to such emails in the hands of the service provider did not meet constitutional standards, since it did not require a warrant. The Court issued a broad order against the government conducting such email searches. The case is Warshak v. United States.[2]

Privacy in the United States is an extremely complex legal problem particularly when it involves advancing technology. Privacy rights in the USA derive from the 4th Amendment to the US Constitution:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

Clearly all searches must be legally reasonable and some searches require constitutional warrants.

A warrant is an order issued by a judge based on a sworn affidavit and has to meet constitutional standards of probable cause and particularity. Properly issued warrants can be used for almost any kind of record or object.

A subpoena is a routine court "summons" to a person to hand over evidence. Subpoenas in cases such as Warshak are routinely directed to "third party custodians" such as banks, telephone companies and Medical record holders. The key difference is that subpoenas can be "quashed" i.e. withdrawn by the issuing court if they are found after a hearing to be improperly issued. As the Warshak court wrote:

> *"[o]ne primary reason for this distinction is that, unlike 'the immediacy and intrusiveness of a search and seizure conducted pursuant to a warrant[,]' the reasonableness of an administrative subpoena's command can be contested in federal court before being enforced."*

The order under the Stored Communications Act specifically prohibited the Internet Service Provider from notifying its client of the subpoena. Warshak sued when he was finally notified of the subpoena. The key issue in all constitutional privacy cases is whether a low level judicial approval such as a subpoena (especially without notice) is sufficient for a search and seizure or does a high level warrant requirement apply? How do the traditional legal concepts apply to new technology such as email?

The leading Supreme Court case on technical privacy issues is Kyllo[3]. Kyllo involved a thermal imaging camera which was used to measure the heat radiating from a house. The question was whether a warrant was needed. The Court expressed its current view of the law:

> *"a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable. …. We have subsequently applied this principle to hold that a Fourth Amendment search does not occur–even when the explicitly protected location of a house is concerned–unless 'the individual manifested a subjective expectation of privacy in the object of the challenged search,' and 'society [is] willing to recognize that expectation as reasonable.'"*

The Court concluded that viewing the home with a thermal imager was a search requiring a warrant:

> *"Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."*

The 6th Circuit applied the same analysis to email in Warshak. It had to find both a subjective expectation of privacy … and that … "society [is] willing to recognize that expectation as reasonable.

The court drew analogies, to telephone calls and the mail. In both cases long precedents define and protect the contents of mail and the telephone call:

> *"Two amici curiae convincingly analogize the privacy interest that e-mail users hold in the content of their e-mails to the privacy interest in the content of telephone calls, … because the caller 'is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world,' and therefore cannot be said to have forfeited his privacy right in the conversation"*

However in both telephone calls and mail the courts distinguish the protected contents of the transmission from the unprotected address and routing information.

> *"although the conduct of the telephone user in Smith 'may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.' … the use of pen register, installed at the phone company's facility to record the numbers dialed by the telephone user, did not amount to a search. This distinction was due to the fact that 'a pen register differs significantly from the listening device employed in Katz, for pen registers do not acquire the contents of communications.'" (Warshak)*

The court carefully looked at the technology to find the difference between content and routing information. The court found that the government's right to the routing information gave it no right to the contents

> *"the government … cannot, on the other hand, bootstrap an intermediary's limited access to one part of the communication (e.g. the phone number) to allow it access to another part (the content of the conversation)"*

The court determined that a search was unreasonable without a warrant and in a key footnote the court further limited the access provided by a warrant

> *"If the e-mails are seized pursuant to a warrant, the Fourth Amendment's particularity requirement would necessitate that the scope of the search somehow be designed to target e-mails that could reasonably be believed to have some connection to the alleged crime being investigated"*

The court declared the relevant portions of the Stored Communications Act unconstitutional and sent the case back to the lower court.

Unless Warshak is overturned by the Supreme Court it represents a declaration of substantial privacy interests in internet communications. Given the aggressive attempts to erode privacy protection after 9/11 it is a welcome reminder of the fundamental importance of privacy.

Citations

1 *Circuit Courts of Appeal are one step below the Supreme Court*
2 *Currently available at http://www.eff.org/legal/cases/warshak_v_usa/6th_circuit_decision_upholding_injunction.pdf*
3 *Kyllo v. United States, 533 U.S. 27 (2001)*

Sven Lüders

Weit entfernt von der Normalität

Der Gesetzentwurf der Bundesregierung zur Reform der Telefonüberwachung und anderer verdeckter Ermittlungsmaßnahmen

Seit Jahren steigt die Zahl abgehörter Telefonate in Deutschland kontinuierlich an. Allein im letzten Jahr wurden über 41.000 Anordnungen zur Telefonüberwachung erlassen. Dabei werden jedes Mal hunderte bis tausende Gespräche abgehört. Neben den Anschlussinhabern, gegen die sich die Überwachung richtet, sind auch ihre Gesprächspartner betroffen. Nur die wenigsten erfahren davon und können sich dagegen wehren, also nachträglich die Zulässigkeit dieses Eingriffs in ihre Privatsphäre durch ein Gericht prüfen lassen.

Dabei stellen die bekannten Zahlen zur Überwachung der Telefon- und Internetnutzer nur die Spitze des Eisbergs heimlicher Ermittlungsmethoden dar, mit denen Polizei und Staatsanwaltschaften Straftaten aufklären können. Über die heimliche Beschlagnahmung von Postsendungen, den Einsatz verdeckter Ermittler, das längerfristige Observieren und dergleichen Methoden ist kaum bekannt, wie oft, wie lange und wie erfolgreich sie angewandt werden. Bei jedem heimlichen Ermitteln stellt sich die Frage, ob dies für die Aufklärung der jeweiligen Straftaten wirklich angemessen und notwendig war.[1]

Insofern mag man sich über den Gesetzentwurf der Bundesjustizministerin freuen, mit dem sie die Telefonüberwachung reformieren und die verdeckten Ermittlungsmaßnahmen harmonisieren will (BT-Drs. 16/5846). Die Telefone würden künftig nur noch zur Verfolgung schwerer Straftaten überwacht, die

Betroffenen einen besseren nachträglichen Rechtsschutz erhalten und ihr Kernbereich privater Lebensgestaltung umfassender geschützt. Insgesamt werde der Grundrechtsschutz für die von heimlichen Überwachungsmaßnahmen Betroffenen ausgebaut, so Frau Zypries bei der Vorstellung des Gesetzentwurfs.

Der Teufel steckt bekanntlich im Detail. Ein genauerer Blick auf das jetzt im Bundestag verhandelte Gesetz zeigt, dass mit den geplanten Änderungen die Fehlentwicklungen kaum aufzuhalten sind und der verfassungsgemäße Normalzustand eines überwachungsfreien Lebens und Kommunizierens mit diesem Gesetz nicht wiederhergestellt wird. Mehrfach hatte das Bundesverfassungsgericht den Schutz eines Kernbereichs privater Lebensgestaltung angemahnt, in den staatliche Überwachung unter keinen Umständen eingreifen dürfe. Nach dem Gesetzentwurf ist ein Aufzeichnungsverbot für abzuhörende Telefonate nur dann vorgesehen, wenn abzusehen ist, dass es bei den Gesprächen „allein" um kernbereichsrelevante Themen gehe. Das wird faktisch nie passieren – es gibt kaum ein Gespräch mit Vertrauenspersonen, in dem nicht auch banale Dinge wie das Wetter angesprochen werden. Außerdem wäre der Schutz dieses Privatbereichs nicht nur bei der Überwachung von Telefonaten geboten. Auch beim heimlichen Lesen von Briefen (Postbeschlagnahme), beim Einsatz von V-Leuten oder der Video-Observation stoßen die Ermittler immer wieder auf private Dinge, die sie eigentlich nichts angehen. Einen umfassenden Schutz des Kernbereichs privater Lebensgestaltung sucht man in der Gesamtreform der verdeckten Ermittlungsmaßnahmen jedoch vergebens.

Es ist nicht zu erwarten, dass mit der Neuregelung die Zahl der Telefonüberwachungen oder anderer verdeckter Ermittlungen abnehmen wird. Der Widerwillen des Gesetzgebers, heimliche Ermittlungsmaßnahmen wirksam zu beschränken, zeigt sich bereits am Katalog der Straftaten, für deren Aufklärung Telefonüberwachungen eingesetzt werden darf. Es wurden nur einige unbedeutende, weil faktisch kaum begangene Anlasstaten gestrichen (etwa die Anstiftung zum Ungehorsam nach dem Wehrstrafgesetzbuch). Gleichzeitig fanden aber zahlreiche neue Anlasstaten aus dem Bereich der Wirtschaftskriminalität Eingang in diesen Katalog. Daher ist auch für die Zukunft mit einer weiteren Steigerung der jährlichen Zahlen der Telefonüberwachungen zu rechnen.

Auch ein weiteres Problem des bisherigen Verfahrens der Telefonüberwachung geht der Gesetzentwurf nur halbherzig an: Mehrere wissenschaftliche Untersuchungen[2] über die tatsächliche Anwendung des Richtervorbehaltes haben gezeigt, dass damit keine effektive Kontrolle über die Notwendigkeit und Wirksamkeit des Mitlauschens am Telefon verbunden ist. Viele Telefonüberwachungen wurden von den Richtern fraglos genehmigt, selbst wenn materielle oder formale Fehler in den Anträgen der Staatsanwaltschaften offensichtlich waren. Die Ursachen dafür sind bekannt: Zu wenige, zu unerfahrene Richter müssen zu viele Anträge entscheiden und erfahren kaum etwas darüber, welche Relevanz die so gewonnenen Daten für die Aufklärung der Straftaten letztlich hatten.

Zur Stärkung der richterlichen Kontrolle sieht der Gesetzentwurf nun vor, dass es sich bei der Anordnung einer Telefonüberwachung um eine auch im Einzelfall schwerwiegende Straftat handeln soll (§ 100a Abs. 1 Nr. 2 des Entwurfs zur Strafprozessordnung). Dieser Einzelfallprüfung kommt aber eine eher symbolische Bedeutung zu, wie Christopher Gusy in der parlamentarischen Anhörung über den Entwurf ausführte: „Ob die Tat entweder organisiert, gewerbs- oder bandenmäßig fortgesetzt u.ä. oder aber umgekehrt im Zustand eingeschränkter Schuldfähigkeit, mit nur geringem Schaden oder im Konflikt oder Affekt begangen worden ist, lässt sich im Verdachtsstadium regelmäßig schwerlich erkennen. Im Gegenteil: Die Aufklärungsmaßnahmen sollen ja gerade dazu dienen, auch solche Umstände aufzuklären. Daher kann die Schranke des § 100a Abs. 1 Nr. 2 StPO-E regelmäßig eher eine solche sein, welche zur späteren Einstellung der Ermittlungen führen kann, wenn sich keine schweren Umstände herausstellen. Hingegen kann sie als anfängliche Ermittlungsbremse kaum Wirkungen zeigen."[3] Eine wirksame Begrenzung der heimlichen Überwachung von Verdächtigen wäre wohl nur zu erreichen, wenn eine positive Anordnung den Richtern mehr Arbeit verschafft als die Ablehnung eines Überwachungsantrages. Das wäre dann der Fall, wenn sie auch über die Ergebnisse der Telefonüberwachung informiert würden und die entsprechende Auswertung und die statistischen Angaben zu leisten hätten.

Die Aufklärung von Straftaten ist zweifelsfrei eine wichtige Angelegenheit. Der Gesetzentwurf erhebt die „umfassende Wahrheitsermittlung" jedoch zur obersten Maxime, an der allein sich das Handeln der Strafverfolger zu orientieren habe. In vielen Fragen der Verfahrenssicherung orientiert sich der Gesetzentwurf an jenen Mindeststandards, welche das Verfassungsgericht in den letzten Jahren aufgestellt hat. Mehr Freiheiten sind nach der Logik des Gesetzgebers aber nicht geboten, kommen weitreichende Ermittlungsbefugnisse doch auch jenen Beschuldigten zugute, die irrtümlich verdächtigt wurden. Wer nichts zu verbergen hat, wird wohl nichts gegen seine Überwachung einzuwenden haben ... Ein freiheitliches Verständnis der Strafverfolgung sähe anders aus: Es würde die Arbeit der Polizisten und Staatsanwälte an den Grundsätzen des offenen, erkennbaren Handelns

Sven Lüders

Sven Lüders, Jahrgang 1973, ist in Ostdeutschland aufgewachsen. Er war von 1989 bis 1994 im Neuen Forum aktiv, studierte von 1993 bis 2000 Soziologie an der Freien Universität Berlin und ist seit 2004 als Geschäftsführer der Humanistischen Union tätig.

ausrichten, für das verdeckte Ermittlungen die ultima ratio sind. Das Bundesjustizministerium beweist mit seinem Gesetzentwurf – der in einzelnen Punkten sicherlich begrüßenswerte Verfahrenssicherungen enthält – dass wir davon weit entfernt sind. Bereits die verschiedenen Subsidiaritätsklauseln der verschiedenen verdeckten Ermittlungsmethoden zeigen, dass die Ermittler nahezu beliebig darauf zurückgreifen können. Dass der Aufenthaltsort eines Verdächtigen mit einem IMSI-Catcher (Ortung des Handys innerhalb des Mobilfunknetzes) einfacher zu ermitteln ist, als mit einer konventionellen Befragung von Bekannten und Verwandten, wird jeder Ermittler glaubhaft begründen.

Hinter dieser fehlenden Einordnung der verdeckten Ermittlungen steckt ein konzeptionelles Problem, welches auch die vorliegende Reform nicht lösen wird. Das Risiko, unberechtigterweise zum Objekt einer heimlichen Ausforschung zu werden, liegt einseitig bei den Überwachten. Für die Ermittler ist es im Zweifelsfall gewinnbringend, wenn sie alle Möglichkeiten des heimlichen Ausspionierens ausschöpfen. Die Gerichte mögen nachträglich über die Zulässigkeit der Maßnahmen entscheiden wie sie wollen, die so gewonnenen Ansatzpunkte für ihre weitere Ermittlungsarbeit nimmt ihnen niemand wieder weg. Die Lösung für diese falsche Risikoverteilung ist einfach und schon länger bekannt: Sie besteht in einem umfassenden Verwertungsverbot für alle illegal erlangten Informationen. Nur so ließe sich auch für die Ermittler ein Anreiz schaffen, von vornherein die Privatsphäre ihrer Beobachtungsobjekte zu achten.

Quellen

1 *Die Humanistische Union hat zu dem Gesetzentwurf eine ausführliche Stellungnahme abgegeben, die ihr stellvertretender Bundesvorsitzender Dr. Fredrik Roggan am 19. September 2007 bei der Sachverständigenanhörung des Deutschen Bundestages vorgestellt hat. Weitere Informationen dazu unter http://www.humanistische-union.de/themen/innere_sicherheit/verdeckte_ermittlungen/*

2 *Albrecht, Hans-Jörg, Dorsch, Claudia & Krüpe, Christiane (2003), Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen. Abschlussbericht des Max-Planck-Instituts für ausländisches und internationales Strafrecht (Freiburg)*
Backes, Otto & Gusy, Christhoph (2003), Wer kontrolliert die Telefonüberwachung? Eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung, Bielefelder Rechtsstudien Bd. 17, Peter Lang (Frankfurt/M.)

3 *Christoph Gusy, Stellungnahme zum Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BT-Drs. 16/5846) in der Sachverständigenanhörung des Rechtsausschusses des 16. Deutschen Bundestages am 19.9. 2007, Online: http://www.bundestag.de/ausschuesse/a06/anhoerungen/23_TKUE_allg__Teil/04_Stellungnahmen/index.html*

Die „Wanze" im Text ist von Antje Wegwerth

Petra Pau

Egon Schäuble

„Egon Olsen" ist ein Typ in einer Dänischen Kriminal-Komödie. Er hatte immer einen großen Plan, er führte ihn verblüffend genial aus und er landete zum Schluss dennoch immer im Knast. Bundesinnenminister Schäuble (CDU) hat auch einen großen Plan. Aber er heißt nicht Egon und er ist auch nicht komisch.

Wolfgang Schäuble spricht gern von einer *neuen Sicherheitsarchitektur*, die unverzichtbar sei. Wie diese konkret aussehen soll und was sie von der bisherigen unterscheiden wird, darüber redet er seltener. Stattdessen bemüht er einsichtige Floskeln. Zum Beispiel: „Freiheit und Sicherheit bedingen einander!" Oder: „Wir müssen terroristische Anschläge unterbinden, bevor sie geplant werden." Oder: „Wir brauchen Waffengleichheit mit dem internationalen Terrorismus!" Alles klingt sehr verantwortungsvoll und ist zugleich der größte Angriff auf das Grundgesetz seit Gründung der Bundesrepublik Deutschland.

Das sachlich und historisch begründete Trennungsgebot von Polizei und Bundeswehr wird in Frage gestellt. Polizei und Geheimdienste werden immer weiter zusammengeführt. Und der Datenschutz wird permanent als Sicherheitsrisiko an den Pranger gestellt und de facto abgeschafft. Die für jeden Rechtsstaat unverzichtbare Unschuldsvermutung wird aufgeweicht. Und selbst das absolute Folterverbot wird namens vermeintlicher Sicherheit in Frage gestellt. Das alles waren tragende Säulen der bisherigen Sicherheitsarchitektur. Sie werden attackiert und deshalb ist meine Warnung wohl nicht aus der Luft gegriffen: Es wird ein Wechsel angebahnt, weg vom demokratischen Rechtsstaat, hin zum präventiven Sicherheitsstaat.

Petra Pau

Petra Pau, Jahrgang 1963, Berlinerin, Mitglied des Bundestages seit 1998, derzeit Vize-Präsidentin des Bundestages, stellvertretende Vorsitzende der Fraktion DIE LINKE und Leiterin des Arbeitskreises „BürgerInnenrechte und Demokratie" sowie der Querschnittsarbeitsgruppe „Rechtsextremismus, Rassismus und Antisemitismus" der Fraktion.

Springen wir kurz zurück ins Jahr 1983. Damals wollte der Staat sein Volk zählen. Das war skeptisch. Viele Bürgerinnen und Bürger begehrten auf und bekamen letztlich vom Bundesverfassungsgericht Recht. Der Richterspruch ging als *Volkszählungsurteil* in die Geschichte ein. Er begründete das informationelle Selbstbestimmungsrecht und er stärkte den Datenschutz.

Die Begründung war sehr weitsichtig. Sie besagt nämlich sinngemäß: Bürgerinnen und Bürger, die nicht mehr wissen oder wissen können, was andere über sie wissen, sind nicht mehr souverän. Wer nicht mehr souverän ist, kann auch kein Souverän sein. Eine Demokratie ohne Souveräne aber gibt es nicht.

So weit *Karlsruhe* damals. Das ist die Dimension, um die es geht. Und wie ist die Wirklichkeit heute? Kann überhaupt noch jemand wissen, welche Daten andere über sie oder ihn angehäuft haben? Die technischen Möglichkeiten, Daten zu sammeln, wachsen. Ebenso die Begehrlichkeiten, dies zu tun. Und bei den meisten Bürgerinnen und Bürgern ist viel Naivität oder Gleichgültigkeit im Spiel. Was also müsste eine verantwortliche Politik umtreiben?

Der Datenschutz müsste gestärkt und den Bedingungen des 21. Jahrhunderts angepasst werden. Die Politik, die Medien und viele andere mehr müssten im besten Sinne eine neue Epoche der Aufklärung einleiten.

Praktisch aber passiert das Gegenteil. Bundesinnenminister Schäuble will partout Computer heimlich und online auslesen können. Damit ihn dabei niemand stören kann, wurde jüngst sogar ein Gesetz erlassen, dass die private Herstellung, Verbreitung und Nutzung von Sicherheits-Software unter Strafe stellt. Es enthält einen Verweis auf den Paragrafen 129 Strafgesetzbuch. Der wiederum definiert, was eine kriminelle Vereinigung ist. Künftig soll dieser Paragraf um weitere Absätze erweitert werden. Demnach könnten auch einzelne Personen eine kriminelle Vereinigung bilden. Warum nicht auch Tüftler vom Chaos Computer Club, die sich für die Sicherheit von privaten Computern oder von Firmennetzen engagieren?

Am 12. Juni 2007 gab es in Berlin eine Konferenz europäischer Datenschützer. Sie kam in den Hauptnachrichten nicht vor. Am selben Tag einigten sich die Innenminister der EU-Staaten, dass jede Landespolizei künftig Zugriff auf die DNA- und Fingerabdruck-Dateien der anderen haben soll. Das wurde medial als Erfolg gewürdigt. Die einen wollten Daten schützen. Die anderen haben sie ins Nirwana entlassen. Wirklich ins Ungewisse? Gewiss. Die deutsche Anti-Terror-Datei zum Beispiel ist so konstruiert, dass möglichst viele Daten über Personen gebündelt werden. O-Ton Schäuble: „Das ist sinnvoll, für die Polizei!“ Dabei verschweigt er wieder das Wesentliche. Die gemeinsame Anti-Terror-Datei wirkt wie ein großer Staubsauger. Er sammelt alles ein und liefert letztlich alles bei den Geheimdiensten ab. Nur sie haben den ungehinderten Zugriff. Auch das gehört zur *neuen Sicherheitsarchitektur*. Geheimdienste aber sind das Gegenteil von Transparenz. Ohne Transparenz wiederum gibt es keine Demokratie. Auch deshalb finde ich: Es ist höchste Zeit für eine neue, agile Bürgerrechtsbewegung. So, wie sie am 22. September auf der Berliner Demonstration der 18.000 gegen Datenvorratsspeicherung bereits spürbar wurde

Silke Stokar

G8-Gipfel – Schäubles Planspiele werden Realität

Bundeskanzlerin Merkel bezeichnete die Aufgabentrennung von äußerer und innerer Sicherheit als „von gestern“, und für Bundesinnenminister Schäuble gibt es keine klare Trennlinie mehr zwischen Krieg und Frieden. Er fordert den erweiterten Einsatz der Bundeswehr im Inneren, und gleichzeitig bereitet er die Bundespolizei auf Auslandseinsätze vor, bei denen es nicht mehr um den zivilen Polizeiaufbau gehen soll, sondern um militärische Befugnisse für die Bundespolizei im Ausland.

Wie schnell aus Planspielen ernste Realität wird, konnten wir beim G8-Gipfel erleben. Die *Feindaufklärung* im Vorfeld fand durch die Einleitung eines Ermittlungsverfahrens wegen Unterstützung einer terroristischen Vereinigung (§129 a) gegen die üblichen linken Zentren statt, die Bundesländer meldeten mögliche *Gefährder* an das BKA, im benachbarten Ausland wurden Erkenntnisse abgefragt. Wie schon bei der Fußball-WM mussten alle Journalisten ein Akkreditierungsverfahren mit umfangreicher Sicherheitsüberprüfung durchlaufen. Bemerkenswert und bislang einmalig in Deutschland war die *Nahaufklärung*. Ein ganzes Dorf (Heiligendamm) wurde sicherheitsüberprüft. Massiv eingeschränkt wurde die Bewegungsfreiheit der Bewohnerinnen und Bewohner. Nur durch Sicherheitsschleusen und mit besonderen Ausweisen konnten die Einwohner ihren Wohnort erreichen. Es bleibt die bange Frage: Wann und zu welchem Anlass wird das nächste Wohngebiet abgeriegelt und werden alle Bewohnerinnen und Bewohner unter eine totale Kontrolle gestellt?

Alle Informationen liefen bei der *Besonderen Aufbau Organisation (BAO) KAVALA* zusammen. Bis heute entzieht sich die BAO KAVALA der parlamentarischen Aufklärung und Kontrolle. Fragen im Bundestag werden entweder mit dem Hinweis zurückgewiesen, zuständig und verantwortlich sei das Land Mecklenburg-Vorpommern, oder Einzelheiten der Aufgabenwahrnehmung durch das BKA, den BND oder die GSG9 unterlägen der Geheimhaltung. Der zunehmenden und teils geheimen Vernetzung der Sicherheitsbehörden steht eine völlig zersplitterte Kontrolle der Parlamente hilflos gegenüber.

Auf unsere drängenden Fragen im Bundestag musste die Bundesregierung eingestehen, dass der Einsatz der Bundeswehr keineswegs kurzfristig geplant wurde. Das Amtshilfeersuchen zum G8-Gipfel wurde bereits im April 2006 durch die damalige rot-rote Landesregierung gestellt. Gleich nach der Fußball-WM wurde die BAO KAVALA entwickelt. In dieser integrierten Leitzentrale saßen Landespolizei, Bundespolizei, BKA, Bundesamt

und Landesamt für Verfassungsschutz, BND, Bundeswehr und zivile Kräfte wie THW und Feuerwehr einträchtig zusammen. Zwischen den sehr unterschiedlichen Aufgaben wie dem Schutz der *Airforce One* von US-Präsident Bush und der polizeilichen Bewältigung von Versammlungen wurde nicht klar getrennt. Einsatzmittel wie Tornados und Spähpanzer, die zum Schutz hochrangiger ausländischer Staatsgäste erforderlich und gerechtfertigt sein mögen, wurden gleichzeitig im Zusammenhang mit der Ausübung der grundgesetzlich verbrieften Versammlungsfreiheit eingesetzt. Schon durch die sichtbare Präsenz der Bundeswehr wurde Druck auf die Demonstrierenden ausgeübt. Der Tiefflug eines Tornados über einem Protestcamp war nur der Gipfel einer ganzen Reihe von Einschüchterungsversuchen.

G8-Protestler auf Feldern und Wiesen wurden wie feindliche Truppenbewegungen durch Spähpanzer mit der militärischen *Fennek*-Technik *aufgeklärt.* Über Satellitentelefone speisten die militärischen Aufklärer ihre Lageerkenntnisse direkt in die polizeilichen Infokanäle ein. Spähpanzer wurden zur Bewachung eines Gen-Versuchsfeldes eingesetzt, Polizisten wurden von Bundeswehrhubschraubern zu Demonstrationseinsätzen am Zaun geflogen, Bundeswehrsoldaten errichteten Sperren im Wald, die Bundeswehr übernahm den Objektschutz im Krankenhaus in Bad Doberan. Nie zuvor hat es so einen Einsatz der Bundeswehr im Inneren im Rahmen von Versammlungen gegeben. Über das ganze Ausmaß dieses Einsatzes wurde das Parlament belogen und getäuscht. Die Militarisierung der Innenpolitik ist ein schleichender Prozess. Ich will mich an den Anblick von Panzern bei Demonstrationen nicht gewöhnen.

Bedrohte Sicherheit – gefährdete Freiheit

Das Beispiel Heiligendamm zeigt, dass sich die Zeiten ändern, bestimmte Fragen aber bleiben. „Wir stehen gegenwärtig inmitten einer entscheidenden Auseinandersetzung um den Erhalt und die Durchsetzung demokratischer Rechte“. Dieses Zitat stammt aus dem ersten grünen Parteiprogramm von 1980. Ging es damals noch um die Auseinandersetzung zwischen Staat und RAF, um die Überwachung der Anti-Atombewegung oder den Radikalenerlass, so haben wir es heute mit einer ganz anderen Dimension von Bedrohung der Sicherheit auf der einen und staatlicher Überwachung auf der anderen Seite zu tun. Im Zeitalter moderner Informationstechnologien haben alle Seiten aufgerüstet. Das Internet fördert die globale Informationsfreiheit, gleichzeitig ist es ein Tatwerkzeug für Terrorismus und organisierte Kriminalität und ein Überwachungsinstrument für den Staat. Mit dem Handy können wir telefonieren und Bomben zünden; der Staat kann uns darüber jederzeit orten und überwachen. Wie wir die Bürgerrechte in der digitalen Informationsgesellschaft schützen können, und wie wir die Bevölkerung vor der realen Bedrohung durch terroristische Gewaltakte schützen wollen, muss neu diskutiert werden.

Bundesinnenminister Schäuble verlangt mit seinen aggressiven Forderungen außerhalb der Verfassung die Selbstaufgabe unserer demokratischen Werte. Das kann nicht unser Weg sein. Es reicht allerdings auch nicht aus, auf alle Sicherheitsmaßnahmen immer nur mit reflexartiger Abwehr zu reagieren. Wir dürfen die Definition der Bedrohung nicht den Schäubles überlassen, sondern müssen eigene und bessere Antworten finden.

Wir stehen erst am Anfang einer Sicherheitsdebatte. Ob die freien und offenen Gesellschaften Europas sich zu präventiven *Sicherheitsstaaten* entwickeln werden, ist noch nicht entschieden. Es wird auch davon abhängen, ob es – wie jüngst in London – gelingt, geplante Anschläge auf die Zivilbevölkerung zu verhindern.

Wie viel Überwachung verträgt die Demokratie?

Die täglich neuen Forderungen von Bundesinnenminister Schäuble müssen wir ernst nehmen. Gemeinsam mit anderen europäischen Innenministern will er sie Schritt für Schritt umsetzen. Ein europäisches System zur Erfassung aller Fluggastdaten ist in der Planung, und in England wird bereits sehr konkret ein zeitlich begrenzter Unterbindungsgewahrsam von *Gefährdern* diskutiert. Der polizeiliche Gewahrsam auf Verdacht soll hier auf 28 Tage verlängert werden. In der Großen Koalition wird die Online-Durchsuchung von privaten Computern verhandelt. Dabei sind die Fragen spannend, die nicht in der Öffentlichkeit diskutiert werden: Soll die Online-Durchsuchung ein Instrument der Strafverfolgung oder der Informationsgewinnung sein, oder beides? Für eine Beweissicherung sind hohe Anforderungen an die eingesetzte Technik zu stellen. Es muss zum Beispiel gesichert sein, dass die abgefischten Daten nicht manipuliert sind. Wo Daten heimlich entwendet werden können, ist es auch möglich Daten einzuspeisen und zu verändern. Sollen Daten über Betriebssysteme, über Mails oder über Schnittstellen eingeschleust werden, und wie werden Trojaner nach Beendigung der Maßnahme sicher deaktiviert? Eine weitere Möglichkeit ist das heimliche Eindringen in die Wohnung des *Gefährders* und die Manipulation direkt am heimischen Computer. Diejenigen, die eine Online-Durchsuchung ihres Computers befürchten, werden die ein und ausgehenden Datenmengen genau kontrollieren und sich gegen das heimliche Ausspähen schützen. Schon durch die anhaltende öffentliche Debatte über das staatliche Hacken nimmt die Demokratie Schaden. Staatliche Sicherheitsbehörden, die selbst wie Computerkriminelle agieren, verlieren das Vertrauen der Bevölkerung. Bleibt zu hoffen, dass die SPD sich nicht von Schäuble treiben lässt und die Legalisierung der Online-Durchsuchung verweigert.

Silke Stokar

Silke Stokar ist innenpolitische Sprecherin der Bundestagsfraktion BÜNDNIS 90/DIE GRÜNEN
www.stokar.de

Klaus Fuchs-Kittowski

Das hohe Gut der Menschen- und Bürgerrechte darf nicht angetastet werden!

Der hohe Anspruch, der mit dem Begriff Menschen- und Bürgerrechte verbunden ist, wurde erst in unserer Zeit realpolitisch konkretisiert. Mit der Deklaration der Menschenrechte der Generalversammlung der Vereinten Nationen 1948 bekannte sich die internationale Staatengemeinschaft zum Prinzip der überstaatlichen Rechte des Bürgers und somit zumindest indirekt zu einer übernational gültigen Rechtsordnung. Fast alle Staaten der Erde haben heute Verfassungen, die in der einen oder anderen Form auf die Menschenrechte Bezug nehmen. Nur einige Länder, die den Koran zur Grundlage ihrer Verfassung erklärt haben, machen hier eine Ausnahme.

Zwischen dem offiziellen Bekenntnis zu den Menschenrechten und der politischen Realität in sehr vielen Ländern auf unserer Erde besteht eine nicht zu übersehende Diskrepanz. Doch muss andererseits deutlich gesagt werden, dass der Gedanke der Menschenrechte – ihr hoher Anspruch – die politischen Gegebenheiten auf unserem Planeten verändert hat. So war das Recht zur Kriegsführung über Jahrhunderte der entscheidende Ausdruck staatlicher Souveränität. Schon mit den Nürnberger Kriegsverbrecherprozessen hatten die Alliierten das entscheidende Ziel verfolgt, eine Wende im Völkerrecht zu erreichen, so dass rechtmäßig kein Angriffskrieg mehr begonnen werden könnte.[1]

Der so wirkungsvolle Gedanke der Menschenrechte musste gegen den harten Widerstand reaktionärer Kräfte durchgesetzt werden. Dies war nicht nur für die internationale Ebene charakteristisch, sondern auch für die innere Entwicklung vieler Länder, besonders auch in Deutschland. Hier war der Menschenrechtsgedanke durch die entsetzlichen Erfahrungen in der Zeit des Faschismus erstarkt. Es soll hier aber auch an die Weimarer Republik[2] erinnert werden, deren Schicksal die Verfasser des Grundgesetzes zu der entscheidenden Festlegung veranlasste, dass das Militär nicht im Inneren des Landes eingesetzt werden darf. Dies bekommt besondere Aktualität, da sich jetzt auch die Bundeskanzlerin öffentlich für den möglichen Einsatz der Bundeswehr im eigenen Land geäußert hat.

Kann man wirklich so schnell vergessen, woher man kommt, Frau Bundeskanzlerin?

Die Frage stellt sich mir nicht so sehr bezogen auf Ihre Herkunft aus der DDR oder die frühere Arbeit an einem Institut der *Akademie die Wissenschaften der DDR,* ich möchte sie beziehen auf Ihre Herkunft aus einem Pfarrhaus und aus der Bürgerrechtsbewegung der DDR. Denn dies ist es doch wohl, was Ihnen bisher so starken Antrieb für Ihre sehr wohl von mir respektierten Leistungen in Ihrem hohen Amt gegeben hat.

Wie Ihnen sicher bekannt ist, haben führende Bürgerrechtler aus der DDR im Dezember 2001 schon scharf gegen den Abbau von Grundrechten durch die Antiterrorismusgesetze protestiert.[3] Entgegen diesen Protesten der Bürgerrechtler gehen Sie nun noch weiter und unterstützen sogar die Forderung nach einem Gesetz, welches der Bundeswehr Einsätze im Inneren unseres Landes ermöglichen soll. Ich bin dagegen der strikten Auffassung, dass der Einsatz von Militär im Inneren zwecklos im Kampf gegen den Terrorismus sein wird. Hier ist und bleibt wirkungsvoll der Einsatz der Polizei und wahrscheinlich auch der Geheimdienste. Der Einsatz von Militär könnte nur in sehr wenigen, juristisch genau festzulegenden Fällen gerechtfertigt sein. Die generelle Forderung nach Möglichkeiten des Militäreinsatzes kann allein einem weiteren Abbau unsere Grundrechte, der Verletzung unserer Verfassung, unserer Rechtsordnung dienen. Dies ist besonders gravierend, weil die in unsere Verfassung vorgesehene Trennung zwischen den Aufgaben der Polizei und des Militärs auf die bitteren Erfahrungen aus der Weimarer Republik zurückgeht. Diese Erfahrungen haben die Autoren des Grundgesetzes bewusst berücksichtigt. Es ist absolut unverständlich, wenn Sie, Frau Bundeskanzlerin, in Ihrer Stellungnahme in der Tagesschau formulieren, die alte Trennung von innerer und äußerer Sicherheit „sei von gestern."[4] Auch wenn Sie dies unter dem unmittelbaren Eindruck der entsetzlichen Ereignisse in London formulierten, muss doch mit aller Entschiedenheit gesagt werden, dass die aus den Erfahrungen der Weimarer Republik und vor allem des furchtbaren Machtmissbrauchs in der Zeit des deutschen Faschismus gelernte Machtbegrenzung durch die jetzige Verfassung auch heute noch gelten muss. Dies sollte speziell durch die Gewaltenteilung, durch den Föderalismus, durch die Gewährleistung der Menschen- und Bürgerechte und insbesondere eben auch dadurch erreicht werden, dass das Militär keine Befugnisse im Inneren hat, außer bei einem *Inneren Notstand*, gemäß Artikel 91 des Grundgesetzes. Aber auch im Fall des inneren Notstandes wird der Einsatz von Militär im eigenen Land meist problematisch sein.

Um die Bedeutung dieser Trennung von Innen und Außen anschaulich zu machen, möchte ich Ihnen Erfahrungen aus jener Zeit, in der die Reichswehr im Innern eingreifen durfte, aus einem anderen Pfarrhaus vor Augen führen.

Heinrich Vogeler, der berühmte Maler aus der Künstlerkolonie Worpswede, war zunächst Kriegsfreiwilliger im Ersten Weltkrieg und lehnte den Krieg dann kategorisch ab. Er wurde politisch aktiv im Arbeiter- und Soldatenrat und in der KPD u.a. linken Organisationen. In der Familiengeschichte von Pfarrer Emil Fuchs[5] wird berichtet, dass H. Vogeler von der Reichswehr gesucht wurde und im Pfarrhaus in Eisenach unter dem Esstisch, über dem eine lange Decke lag, versteckt wurde. Es war nicht die Polizei sondern das Militär, welches ihn suchte. Man fragt sich, wie geschichtsvergessen müssen Politiker sein.

In seiner Lebensbeschreibung berichtet Pfarrer Emil Fuchs über den Einsatz der Reichswehr in Eisenach in Thüringen: „Die Arbeiterschaft – zum Teil erwerbslos – war sehr erregt. So wurde eine durch meinen Westbezirk marschierende Reichswehrabteilung von Arbeitern angerufen, fühlte sich bedroht, schoss und tötete fünf Mann aus meinem Seelsorgebezirk. Sobald ich es

hörte, eilte ich hin und besuchte die Frauen ... Nun hatte ich die Beerdigung zu halten. Nur die Angehörigen durften dabeisein. Passierscheine waren ausgegeben, der Friedhof militärisch besetzt“[6] Es ist diese Erfahrung, wie schnell aufgehetzte und verängstigte, für den Polizeidienst nicht ausgebildete Soldaten in solchen Situationen geradezu versagen *müssen,* die zu der nicht anzutastenden Bestimmung im Grundgesetz geführt hat.

Die Ausnahme für den Einsatz von Militär, der innere Notstand, wird im Artikel 91 des Grundgesetzes klar definiert. Im Artikel 87a heißt es:

> *„(4) Zur Abwehr einer drohenden Gefahr für den Bestand oder die freiheitliche demokratische Grundordnung des Bundes oder eines Landes kann die Bundesregierung, wenn die Voraussetzungen des Artikels* 91 *Abs. 2 vorliegen und die Polizeikräfte sowie der Bundesgrenzschutz nicht ausreichen, Streitkräfte zur Unterstützung der Polizei und des Bundesgrenzschutzes beim Schutze von zivilen Objekten und bei der Bekämpfung organisierter und militärisch bewaffneter Aufständischer einsetzen. Der Einsatz von Streitkräften ist einzustellen, wenn der Bundestag oder der Bundesrat es verlangen.“*[7]

Durch keine angebliche Entlastung der Polizei oder mögliche Kostensenkung wäre also zu rechtfertigen, dass Militär polizeiliche Aufgaben im Inneren unseres Landes übernimmt. Eine politische Haltung, die sich auf christliche und humanistische Werte beruft, muss unbedingt an dem errungenen Verfassungsgrundsatz festhalten. Nur bei diesem bisherigen, nicht „wenn wir dieses neue Denken auch wirklich anwenden, bleiben Freiheit und Sicherheit angesichts dieser neuen Bedrohung in einer ausgewogenen Balance.“[8] Dieses *neue Denken* darf nicht das Denken von gestern und vorgestern sein!

„Spätestens seit den Anschlägen vom September 2001 muss in neuen Zusammenhängen gedacht werde.“ Ja, auf jeden Fall! Aber diese neuen Zusammenhänge legen doch eben nicht die alte Machtpolitik und den Einsatz militärischer Gewalt im Inneren nahe, sondern im Gegenteil den weiteren Ausbau des Sozial- und Rechtsstaats. Man darf nicht immer wieder sagen, dass dies in der gegenwärtigen Situation Utopie sei!

Neue Zusammenhänge sind zu beachten, sie sind schon dadurch gegeben, dass der sich selbst ermordende Attentäter den Tod nicht scheut und er auch bereit ist Hunderte, Tausende mit in den Tod zu reißen. Man kann und muss sich leider vorstellen, dass es nicht bei Sprengstoffanschlägen in U-Bahnen bleibt, die Terroristen sich im Extremfall sogar in den Besitz von Atomwaffen und/oder biologischen Waffen bringen könnten. Vielleicht wollten die radikalen Islamisten die die *Rote Moschee* in Islamabad besetzten, dies auch erreichen? Pakistan und Indien besitzen bekanntlich solche Waffen. Man kann daher den Fall nicht ausschließen, dass gefährliche Massenvernichtungswaffen mit dem Schiff oder Flugzeug herantransportiert werden. In diesem Fall wäre die Polizei machtlos und der militärische Eingriff erforderlich. Wie u.a. im Spiegel[9] detailliert beschrieben, wird der Flugverkehr sehr genau überwacht und schon die kleinste Abweichung vom vorgesehenen Kurs registriert. Hier gibt es alle Vollmachten zum Eingriff, wenn er erforderlich werden sollte.

Es bleibt also der besondere Fall, dass ein normales, nicht vom Kurs abweichendes Passagierflugzeug, für einen solchen Terroranschlag benutzt wird. In diesem Falle wäre man im Prinzip machtlos, es sei denn man würde durch andere Fluggäste oder Geheimdienst-Informationen in letzter Minute davon erfahren. In diesem besonderen Fall müsste das Militär reagieren dürfen. Das Bundesverfassungsgericht hat hier in der Tat zu prüfen, welche Handlungen des Militärs verfassungsgerecht sind, ob die Bestimmungen für den inneren Notstand nicht auch hier ausreichen, oder ob die Verfassung wirklich neu gefasst werden müsste.

Dieses Szenario zeigt jedoch zugleich, dass der Schutz der Bevölkerung nur auf einem unwahrscheinlichen glücklichen Zufall beruhen würde und die Passagiere geopfert werden müssten. Wirklicher Schutz kann nur auf der Grundlage einer allgemeinen Abrüstung und der Vernichtung aller Massenvernichtungswaffen erreicht werden. Vielleicht kann die allgemeine Abrüstung, die bei der Beendigung des Kalten Krieges versäumt wurde, gerade durch dieses sich abzeichnende Horrorszenarium erzwungen werden. Dies wäre dann wirklich ein *neues Denken*. Das alte und das heutige, welches leider zu einer verstärkten Rüstung geführt hat, führen nicht zur Überwindung des Terrorismus.

Der Autor der Titelgeschichte des Spiegel, Thomas Darnstädt[10], macht sehr klar, was auch hier herausgestellt werden soll, dass eine Militarisierung des Inneren die größte Erosion des Rechtsstaats bedeuten würde. Umso bedrohlicher ist es, wenn genau dieser Punkt parlamentarisch vorangetrieben werden soll und Vertreter verschiedener Parteien zu dieser zentralen Frage Zustimmung signalisieren. Laut Umfrage des Spiegel sind 71% der Befragten bei besonderen Gefährdungsmomenten für den Einsatz der Bundeswehr innerhalb Deutschlands und nur 26% dagegen. Das ist kaum gründlich bedacht, eine genaue Spezifizierung und juristische Definition dieses *besonderen Gefährdungsmoments* fehlt.

Klaus Fuchs-Kittowski

Prof. Dr. phil. habil. Klaus Fuchs-Kittowski ist Professor für Informationsverarbeitung und war Leiter des Bereichs Systemgestaltung und automatisierte Informationsverarbeitung der Sektion Wissenschaftstheorie und Wissenschaftsorganisation der Humboldt-Universität zu Berlin. Auszeichnung mit dem Silver Core der Internationalen Föderation für Informationsverarbeitung (IFIP) sowie Wahl zum Mitglied der Leibniz-Sozietät.

Die angestrebte weltweite Geltung der Menschenrechte ist gegen die Interessen der Kolonialmächte durchgesetzt worden, die noch bis zur Mitte des vergangenen Jahrhunderts versuchten, den Kolonialzustand zu erhalten.

Sollen nun die Menschen- und Bürgerrechte zur Geltung kommen, so bedeutet dies die Schaffung politischer Zustände, bei denen die Regierenden anerkennen, dass sie ihre Macht von den Regierten erhalten haben, und dass sie über ihre Machtausübung ihnen gegenüber rechenschaftspflichtig sind. Dies verlangt nicht nur ein System der Gewaltenteilung und Kontrolle durch die Wähler, es verlangt vor allem nach einer Haltung, die friedliche und demokratische Verhältnisse auch haben will und somit die Menschen- und Bürgerrechte als ein hohes Gut von vornherein unangetastet lässt. Aber genau diese Haltung lässt die gegenwärtige Diskussion über die Erhöhung der Sicherheit angesichts der gewachsenen Terrorismusgefahr bitter vermissen. Wie könnten sonst Vorschläge wie präventive Rasterfahndung, großer Lauschangriff, heimliche Computerausspähung überhaupt gemacht werden, und von Politikern, die dem Grundgesetz verpflichtet sind, weiter verfolgt werden, obwohl sie vom Bundesverfassungsgericht als verfassungswidrig zurückgewiesen wurden. In einer solchen Situation wird man den Verdacht nicht los, dass unter dem Deckmantel der Terrorismusbekämpfung bewusst die demokratischen Grundrechte abgebaut werden sollen.

Aber wo liegen dann die eigentlichen Gründe?

Man kann es nur vermuten. Sie könnten mit einer bestimmten Sicht auf die Prozesse der Globalisierung zusammenhängen. Unterstützt durch die lokalen und globalen digitalen Netze und die modernen Verkehrsmittel verändert die Globalisierung der Wirtschaft die internationale Arbeitsteilung, führt sie zu einer weltweiten Vereinheitlichung von gesellschaftlichen Prozessen, aber auch zu ihrer Differenzierung. Die wirtschaftlichen Chancen und der Zuwachs an zivilgesellschaftlichen Standards werden für viele offensichtlich. Zugleich wird aber auch deutlich, dass damit Probleme entstehen, die jetzt international gelöst werden müssen. Die Umweltbelastung nimmt zu, die Verteilungskonflikte zwischen den armen und den reichen Ländern und damit auch kulturelle Auseinandersetzungen haben sich verschärft. Diese Konflikte beruhen weitgehend darauf, dass das globale Handeln weiterhin vom individuellen Interesse der Länder wie der einzelnen handelnden Personen und Organisationen bestimmt wird. Sie handeln im Horizont ihrer subjektiven, lokalen Interessen, auch wenn die Wirkungen ihres Handelns über diese Sphäre hinaus globale Folgen haben. Statt internationale Lösungen anzustreben, bereitet man auf in dieser egoistischen Sicht in der Tat kaum vermeidbare Konflikte vor.

Wenn also verstärkt Videoüberwachung, Lauschangriffe, Maut-Daten, Vorratsdatenspeicherung, Online-Durchsuchung und biometrische Daten zur Erkennung und Überwachung genutzt werden sollen, geht es nur vordergründig um Terrorismusbekämpfung. Es geht letztlich um die Machterhaltung der heute mächtigen Länder, um die Machterhaltung heute einflussreicher und klar bestimmbarer Interessengruppen. Auch der Einsatz des Militärs im Inneren ist doch nur sinnvoll, wenn man sich auf größere innenpolitische Auseinandersetzungen vorbereiten will und damit eigentlich eingesteht, dass die Politik der Umschichtung des Reichtums von unten nach oben künftig zu stärkeren sozialen Auseinandersetzungen führen wird. Das heimliche Ausspähen von Computern im großen Stil leuchtet doch nur ein, wenn ein Unterdrückungsapparat gegenüber einem großen Teil der Bevölkerung aufgebaut werden soll. Das Sammeln von Daten aller Fluggästen in die USA und ihre Aufbewahrung über 15 Jahre mögen potenzielle Terroristen veranlassen, sich ganz sichere Papiere zu beschaffen und diese zu wechseln. Aber für die Sicherung des Landes genügt die Passkontrolle bei der Ein- und Ausreise auf dem Flughafen. Die weltweite Verteilung und langjährige Aufbewahrung der Flugdaten kann sich nur gegen die Bevölkerung, gegen die Bürger anderer Länder richten, allein mit der Absicht, staatliche Macht zu demonstrieren.

Maßnahmen gegen den Terrorismus sind notwendig. Es ist die Pflicht des Staats, die Sicherheit der Bürger zu garantieren, nicht minder aber auch ihre Freiheit. Die Gewährleistung der Sicherheit muss daher in einem ausgewogenen Verhältnis zur Garantie der Menschen- und Bürgerechte stehen, damit nicht das zerstört wird, was geschützt werden soll. Die berechtigte Angst der Bürger vor Terroranschlägen, ihr Recht davor geschützt zu werden, die Notwendigkeit der Terrorismusbekämpfung, dürfen nicht zur Aufrechterhaltung alter oder zum Aufbau neuer eigennütziger Herrschaftsstrukturen oder gar einer Weltherrschaft einzelner Länder missbraucht werden.

Quellen

1 *Dokumentation Spiegel TV, Der Nürnberger Prozess, DVD*
2 *Erwin Eckert / Emil Fuchs, Blick in den Abgrund – Das Ende der Weimarer Republik im Spiegel zeitgenössischer Berichte und Interpretationen, herausgegeben von Friedrich-Martin Balzer und Manfred Weißbecker, Pahl- Rugenstein, Bonn, 2002*
3 *Vergl. Rolf Gössner, Menschenrechte im Zeichen des Terrors – Kollateralschäden an der „Heimatfront", Konkret Literatur Verlag, Hamburg, 2007, S. 29*
4 *Berliner Zeitung, Dienstag den 3. Juli 2007, S. 5*
5 *Pfarrer Emil Fuchs erhielt mit 45 Jahren (1914) den Ehrendoktor der Universität Gießen, der zu seinem 90. Geburtstag, im Zusammenhang mit der Verleihung der Ehrendoktorwürde der Humboldt-Universität (1964) erneuert wurde. In der Widmung heißt es: „Dem treuen Freund des arbeitenden deutschen Volkes, dem wissenschaftlichen Dolmetsch des deutschen Idealismus, dem tapferen Kämpfer für deutsches Christentum." Er gehörte zu den ersten Pfarrern, die Mitglied der Sozialdemokratie wurden, er wurde Mitbegründer der „Religiösen Sozialisten", die mit als erste gegen die drohende Gefahr des Faschismus öffentlich auftraten. Daher wurde er auch gleich nach der Machtergreifung der Nationalsozialisten von seinem Lehramt in Kiel entfernt. Als Professor für Religionssoziologie an der Leipziger Universität (1949) setzte er sich nachdrücklich für die Möglichkeit zur Kriegsdienstverweigerung in der DDR ein, die dort als einzigem Land des Ostblocks, in Form der Bausoldaten ermöglicht wurde. Seit kurzem hat Emil Fuchs ein Ehrengrab der Stadt Berlin.*
6 *Emil Fuchs, Mein Leben, zweiter Teil, Köhler & Amelang, Leipzig 1959, S. 131-132*
7 *Grundgesetz für die Bundesrepublik Deutschland*
8 *Union dringt auf Reform, ebenda*
9 *Thomas Darnstädt, Im Vorfeld des Bösen. In: Der Spiegel: Der Preis der Angst – Wie der Terrorimus den Rechtsstaat in Bedrängnis bringt, Nr. 28/9.7.07, S. 18- 30*
10 *ebenda*

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: 92 79 29
BLZ 250 905 00
IBAN: DE05 2509 0500 0000 9279 29
BIC: GENODEF1S09

FIfF im Netz

Das ganze FIfF:
www.fiff.de

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

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

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

Beirat

Michael Ahlmann (Bremen); **Peter Bittner** (Berlin); **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); **Dr. Eva Hornecker** (Milton Keynes; UK); **Prof. Dr. Michael Grütz** (Konstanz); **Ulrich Klotz** (Frankfurt); **Prof. Dr. Herbert Kubicek** (Bremen); **Prof. Dr. Klaus-Peter Löhr** (Berlin); **Dipl.-Ing. Werner Mühlmann** (Oppburg); **Prof. Dr. Frieder Nake** (Bremen); **Prof. Dr. Rolf Oberliesen** (Bremen); **Prof. Dr. Arno Rolf** (Hamburg); **Prof. Dr. Alexander Rossnagel** (Kassel); **Prof. Dr. Gerhard Sagerer** (Bielefeld); **Prof. Dr. Dirk Siefkes** (Berlin); **Prof. Dr. Marie-Theres Tinnefeld** (München); **Dr. Gerhard Wohland** (Waldorfhäslach)

FIfF-Vorstand

- **Prof. Dr. Hans-Jörg Kreowski (Vorsitzender)** – Bremen
- **Stefan Hügel (stellv. Vorsitzender)** – München
- **Carsten Büttemeier** – Münster
- **Andreas Hofmeier** – Erfurt
- **Werner Hülsmann** – Konstanz
- **Prof. Dr. Dietrich Meyer-Ebrecht** – Aachen
- **Michael Riemer** – Bremen
- **Jens Rinne** – Kaiserslautern
- **Prof. Dr. Britta Schinzel** – Freiburg
- **Jakob Schröter** – Bremen
- **Prof. Dr. Joseph Weizenbaum** – Berlin
- **Joerg Zeltner** – Köln

Überregionale Arbeitskreise des FIfF

AK »Videoüberwachung und Bürgerrechte«
Peter Bittner,
bittner@fiff.de

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

AK »Kampagne gegen Datensammelwut«
Werner Hülsmann,
werner@fiff.de

Regionalgruppen und regionale Ansprechpartner

Aachen
Prof. Dr.-Ing.
Dietrich Meyer-Ebrecht
Tel. (0241) 8949 8959
dme@fiff.de

Berlin
Peter Bittner
Arndtstr. 19
12489 Berlin
bittner@fiff.de

Bremen
Prof. Dr. Hans-Jörg Kreowski
Universität 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
klaus.thielking-riechert@nefkom.net

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

Hamburg
Sebastian Jekutsch
22083 Hamburg
fiff-hh@fiff.de
Mailing-Liste: http://lists.fiff.de/mailman/listinfo/fiff-hh

Heilbronn
Michael Müller
Hochschule Heilbronn
Fakultät W1
Max-Planck-Straße 39
74081 Heilbronn
Tel.: (07131) 50 43 64
michael.mueller@hs-heilbronn.de

Jena
Prof. Dr. Eberhard Zehendner
Institut für Informatik
Friedrich-Schiller-Universität
07737 Jena
Tel.: (03641) 9463-85
Fax: (03641) 9463-72
nez@uni-jena.de

Kaiserslautern
Jens Rinne
67655 Kaiserslautern
rinne@fiff.de

Karlsruhe
Prof. Dr. Thomas Freytag
Paul-Ehrlich-Str. 24
76133 Karlsruhe
Tel.: (0721) 81 54 16 (p)
fiff@thomas-freytag.de

Koblenz
Dr. Michael Möhring
Uni Koblenz-Landau
Campus Koblenz
FB Informatik
Universitätsstraße 1
56070 Koblenz
Tel.: (0261) 287 2668
Fax: (0261) 287 100 2668
moeh@uni-koblenz.de

Konstanz
Werner Hülsmann
Obere Laube 48
78462 Konstanz
Tel.: (07531) 365 90 56
werner@fiff.de
Mailing-Liste: http://lists.fiff.de/mailman/listinfo/bodensee

München
Bernd Rendenbach
Leerbichlallee 19
82031 Grünwald
Tel.: (089) 641 05 47
Bernd.Rendenbach@web.de
Mailing-Liste: majordomo@lists.lrz-muenchen.de

Münster
Carsten Büttemeier
Mindener Str. 22
48145 Münster
fiff@buettemeier.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) 870 13 09
0171 3101372
Fax: (0711) 5406 5984
pi@c0mplx.org

Ulm
Bernhard C. Witt
Reuttier Str. 15
89231 Neu-Ulm
bcw@bc-witt.de

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 1/2008
„Wissen"
Stefan Hügel, Stephanie Porschen, Dagmar Boedicker
Redaktionsschluss: 3.2.2008

Heft 2/2008
„???"
Schwerpunktredaktion gesucht
Redaktionsschluss: 3.5.2008

Heft 3/2008
voraussichtlich **„QS in der Software-Entwicklung"**
Redaktionsschluss: 4.8.2008

Die Termine für den Redaktionsschluss gelten für aktuelle Beiträge. Schwerpunktartikel haben einen früheren Termin

Artikel zu aktuellen Themen sind immer 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 unserer Webseite *http://www.fiff.de*.

Wichtiger Hinweis:

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

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
Schwerpunktredaktion	Dagmar Boedicker
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*
Fachschaften	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder
Titelbild	C. Antonius, Berlin
Druck	Meiners Druck, Bremen

Die FIfF-Kommunikation ist die Zeitschrift des „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V." (FIfF). Die Beiträge sollen die Diskussionen unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige AutorInnen-Meinung wieder.

Nachdruckgenehmigung wird nach Rücksprache mit der Redaktion in der Regel gerne erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Schluss FIfF

Ingo T. Storm

Hereinspaziert, die Tür ist schon offen!

Während meines Sommerurlaubs hatte mein Nachbar einen Schlüssel, zum Blumengießen und zum Leeren des Briefkastens. Und außerdem könnte es ja sein, dass Polizei oder Stadtwerke nach einem Ein- oder Rohrbruch dringend ins Haus müssen.

So viel Vertrauen genießt auch Microsoft, hat die Firma doch erst Anfang September ein Datenschutzgütesiegel erhalten - und zwar für die WGA-Funktion alias „ohne Gesichtskontrolle keine Updates". Welche Ironie, denn Windows Update schickt selbst dann eine eindeutige Kennung meines Rechners nach Hause, wenn ich die Installation dieser „Windows Genuine Advantage Notification" explizit ablehne. Hey, mein Nachbar kontrolliert auch nicht, ob ich Brief- oder Beate-Uhse-Rabattmarken sammle, nur damit er weiß, worauf er eigentlich aufpassen soll!

Bei so viel Vertrauen fühlte sich Microsoft offenbar verpflichtet, in Zukunft besonders akribisch auch nach meinem Vista-Rechner zu sehen. Unter „Update-Verlauf" findet sich folgender Eintrag: „Windows Update 7.0.6000.381. Installationsdatum: 12.9.2007 12:03. Installationsstatus: Erfolgreich. Updatetyp: Wichtig." Offenbar so wichtig, dass ich nicht gefragt werden musste, obwohl ich ausdrücklich Mitsprache gefordert hatte: „Updates herunterladen, aber Installation manuell durchführen" hatte ich angeklickt.

Nate Clinton, Program Manager für Windows Update, erklärt dazu, dass Microsoft keineswegs „manuell" mit „heimlich und automatisch" verwechselt habe. Es sei schon lange dokumentiert, dass die Update-Funktion sich selbst jederzeit ungefragt aktualisieren darf. Und es sei zwingend nötig gewesen, da Windows Update sonst keine Windows-Updates mehr bemerkt hätte. Hmm. Woher wusste Windows Update dann, dass es selbst nicht mehr aktuell ist? Wenn das Update wirklich so wichtig und unaufschiebbar war, warum gab es dann kein Security Bulletin für jedermann zum Nachlesen? Und warum hat Microsoft sich dann nicht getraut, dieses Zwangs-Update auch den Firmenkunden unterzuschieben? Für mich fühlt sich das so an, als hätte mein Nachbar sich heimlich einen Nachschlüssel angefertigt. Rein sicherheitshalber, falls ich vor meinem nächsten Urlaub vergesse, ihm das Original zu geben.

Echte Sicherheit kann es mit Windows so nicht mehr geben. Früher lag das an naiver Programmierung, heute an der Einstellung: Microsoft liefert viele Updates nur noch an Systeme aus, die die WGA-Prüfung bestehen, also auch „Windows Update" ausführen. Im Klartext: Wer sicher sein will, dass sein Rechner sicher ist, muss für Microsoft eine Tür offen lassen. Als Codenamen für die nächste Fassung von Windows Update schlage ich konsequenterweise Lenin vor: „Dowjerai, no prowjerai!"* Und da Microsoft ja ohnehin gerade mit Brüssel zu tun hat: Warum nicht gleich einen EU-Trojaner daraus machen – in 22 Sprachen, verhökert an 25 EU-Innenminister? Mindestens einer von ihnen wäre dem gegenüber recht aufgeschlossen - so viel ist sicher.

*„Vertraue, aber prüfe nach."

Editorial aus c't 21/2007, *http://www.heise.de/ct/07/21/003/*
Wir danken dem Autor und der c't für die freundliche Genehmigung

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