H 7625

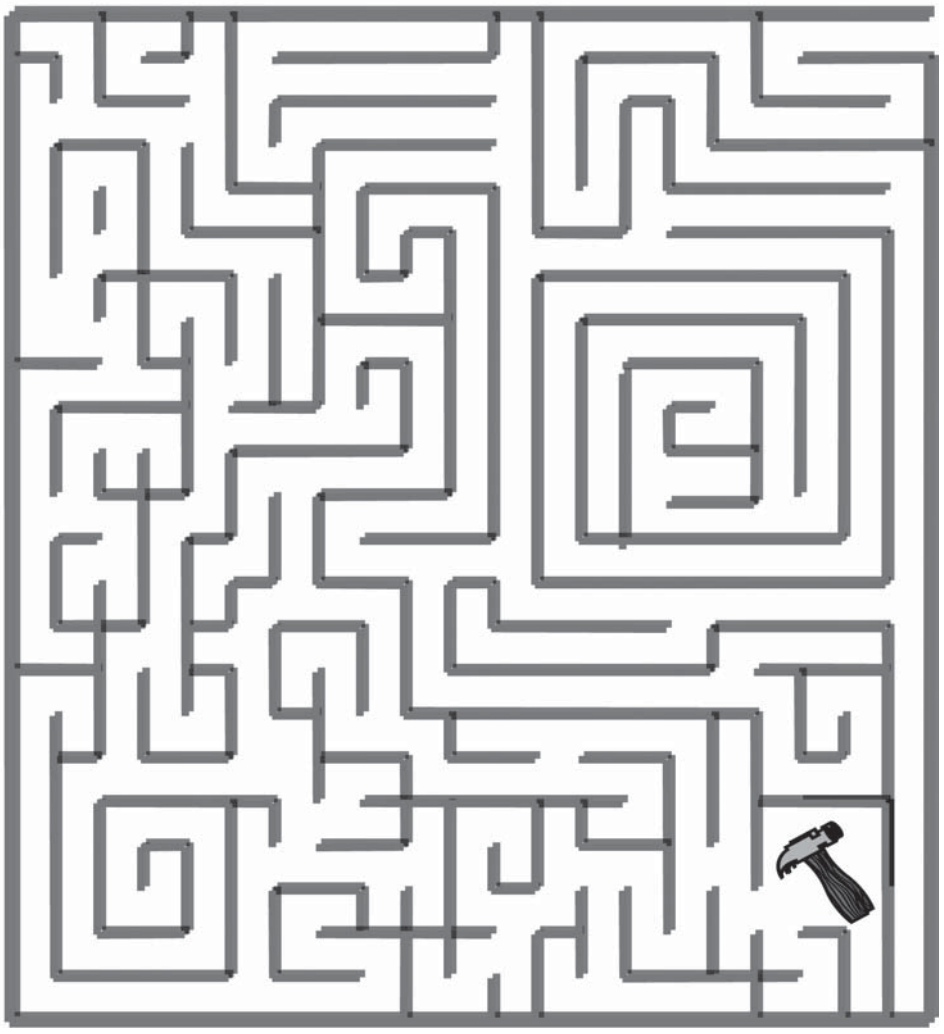
FIfF Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

26. Jahrgang 2009 Einzelpreis: 7 EUR

4/2009 - Dezember 2009

Heraus-



-forderungen

ISSN 0938-3476

FIfF-Kommunikation

Titelbild: ??

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Inhalt

Ausgabe 4/2009

inhalt

FIfF e.V.

Aktuelles

Rubriken

Schwerpunkt „Herausforderungen“

Editorial

Bei dem Stichwort *Herausforderungen* können sich verschiedene Bilder aus der Mythologie aufdrängen. Die einen denken vielleicht an Sisyphos, der angestrengt einen großen Felsblock einen Hügel hinaufrollt, kurz vor dem Ziel aber den Griff verliert. Der Stein rollt hinunter, und Sisyphos muss von vorn beginnen. Andere fühlen sich möglicherweise an den Gordischen Knoten erinnert, der sich nicht anders lösen lässt als durch einen Schlag mit dem Schwert. Wieder anderen mag Herkules in den Sinn kommen, der mehrere gigantische Aufgaben zu lösen hatte wie die Ausmistung der Ställe Augias, für die er zwei Flüsse umleitete – eine Lösung, die geradezu modern anmutet. Die Redaktion dieser FIfF-Kommunikation hat ein Labyrinth als Titelbild gewählt. Die Herausforderung besteht darin, von innen den Ausgang zu finden. Der Minotaurus hat es nicht geschafft, das Labyrinth, in dem er gefangen war, zu verlassen. Seinem Bezwinger Theseus ist es mit dem Ariadne-Faden gelungen. Es ist seit den Arbeiten von Lothar Budach aus den 1970er Jahren bekannt, dass auch drei Markierungssteine immer reichen. Wenn allerdings vom Standpunkt im Inneren des Labyrinths aus gar kein Weg zum Ausgang führt, hilft keine mathematische Lösung, sondern nur ein Vorgehen nach Art des Gordischen Knotens.

Die gesellschaftlichen Herausforderungen in der Informatik einschließlich der Informations- und Kommunikationstechnologie sind wohl weniger poetisch als die mythologischen Vorbilder. Was die Schwierigkeit angeht, können sie den Vergleich aufnehmen. Wie die drei Ausgaben der FIfF-Kommunikation in diesem Jahr ist auch das vierte Heft auf das 25-jährige Bestehen des FIfF ausgerichtet. Dabei geht es vor allem darum, den Blick in die Zukunft zu richten und die Themen zu identifizieren, die im Kontext von Informatik und Gesellschaft heute und morgen anstehen. Wir erheben dabei keinen Anspruch auf Vollständigkeit, aber einige wichtige Problemfelder werden behandelt.

Datensammelwut und Überwachungswahn, mangelnder Datenschutz in Staat und Wirtschaft und damit die Gefährdung der grundgesetzlich garantierten informationellen Selbstbestimmung und anderer Grundrechte stehen schon lange auf der Tagesordnung. Da werden sie aber noch lange bleiben und bleiben müssen, denn echte Fortschritte sind nicht absehbar. Drei der Beiträge in diesem Heft sind diesem Komplex zugeordnet und behandeln unterschiedliche Aspekte. Niels Lepperhoff und Björn Petersdorf stellen eine Studie vor, die zeigt, dass es selbst die Parteien, die im Bundestag vertreten sind, in ihrer Parteiarbeit mit dem Datenschutz nicht allzu genau nehmen. Karin Schuler kommentiert den Umgang der neuen Bundesregierung mit der Datenschutz-Problematik, die eher auf eine Vermeidungsstrategie hinausläuft, als die eklatanten Herausforderungen anzugehen. Und Marie-Theres Tinnefeld setzt sich mit dem Verhältnis von Technik und Grundrechten und dem Konflikt zwischen Sicherheit und Freiheit auseinander.

Drei weitere Beiträge behandeln, wie sich der Einsatz von Informations- und Kommunikationstechnik auf die Gesellschaft auswirken. Alex Klein stellt sich die Frage, ob damit Armutsbekämpfung möglich wird. H.- Peter Neitzke, Dieter Behrendt, Silke Kleinbückelkotten, Eckhard Steinmüller und Dagny Vedder haben untersucht, welche Risiken die Allgegenwart dieser Technik birgt. Viola Bräuer schließlich diskutiert den Unterschied zwischen dem Denken von Menschen und dem Wissen, das technisch als Datensammlung aufgehäuft wird.

Die letzten beiden Beiträge zum Schwerpunkt Herausforderungen betreffen Bildung und Wissenschaft. Wolfgang Coy analysiert das Verhältnis von Berechenbarkeit zu Denken und lebenslanger Bildung. Und Jürgen Altmann skizziert die „Segnungen", die die Nanotechnologie bringen wird. Zum Thema Bildung passen auch die Uni-Sammelbilder von Caro von Totth, die sie anlässlich einer Protestaktion gegen drastische Sparmaßnahmen an der Universität Bremen gezeichnet hat und die durchaus Elemente der aktuellen Protestbewegung an den deutschen Hochschulen illustrieren und karikieren.

Neben den Beiträgen im Schwerpunktteil enthält dieses Heft auch viele aktuelle Informationen rund um die Arbeit des FIfF und die üblichen Rubriken. Wir wünschen allen Leserinnen und Lesern interessante Einsichten und viel Vergnügen.

Schwerpunktredaktion

Stefan Hügel, Frankfurt am Main
Hans-Jörg Kreowski, Bremen
Ralf Streibl, Bremen

Pro »Informatik und Gesellschaft«

FIfF-Mitgliederversammlung beschließt die Einrichtung eines Studienpreises

Der Gedanke war schon länger unterwegs. Bereits vor der Jahrestagung vergangenes Jahr in Aachen war Raffael Rittmeier an den damaligen Vorstand mit der Idee herangetreten, das FIfF könne regelmäßig einen Preis für besonders gute Abschlussarbeiten im Themenkontext von *Informatik und Gesellschaft* vergeben. Die Idee stieß auf breite Zustimmung, allein die Diskussion und Ausformulierung der Vergabebedingungen erforderte noch einige Zeit. Um die besondere Bedeutung dieses Preises herauszustellen und seine Einrichtung auf eine breitere Basis zu stellen, wurde schließlich die abschließende Diskussion auf die Tagesordnung der Mitgliederversammlung 2009 gesetzt. Ein im Vorfeld erarbeiteter und in kleinerem Kreise diskutierter Entwurf, der die Vergabe dieses Studienpreises regelt, wurde vorgestellt und nach einigen Anpassungen durch die Mitgliederversammlung einstimmig verabschiedet.

Das Gebiet *Informatik und Gesellschaft* steht **hochschulpolitisch** in einer Verteidigungshaltung. Vakant werdende I&G-Professuren werden gar nicht oder mit anderen Aufgabenbeschreibungen wiederbesetzt. Der Stellenwert von I&G-Veranstaltungen in Prüfungsordnungen und Studienplänen ist – dort, wo es dieses Gebiet überhaupt gab – durch den Bologna-Prozess angegriffen. Bei den im Zuge des Umbaus vom Diplom zum Bachelor erforderlichen inhaltlichen Kürzungen im Studium haben die Gebiete der »Kerninformatik« – das ist wenig überraschend – eine weitaus stärkere Lobby.

Umso wichtiger ist es, Studierenden sowie Wissenschaftlerinnen und Wissenschaftlern in der Qualifikationsphase deutlich zu machen, dass es eine **gesellschaftliche** Anerkennung für fundierte und differenzierte Auseinandersetzungen mit Fragen aus dem Gebiet *Informatik und Gesellschaft* gibt. Das FIfF möchte mit der Einrichtung dieses Studienpreises herausragende Leistungen des wissenschaftlichen Nachwuchses in diesem Bereich würdigen und die Aufmerksamkeit der Öffentlichkeit auf das Thema der Arbeit sowie die besonderen Leistungen des Autors bzw. der Autorin lenken.

Der Preis soll erstmals auf der nächsten FIfF-Jahrestagung im November 2010 vergeben werden. Bis *31. März 2010* können hierfür Qualifikationsarbeiten (Bachelor-, Master-, Diplomarbeiten oder Dissertationen) vorgeschlagen bzw. eingereicht werden, die in den letzten zwei Jahren vor Nominierungsschluss abgeschlossen wurden. Weitere Details zum Ablauf des Einreichungs- und Vergabeverfahrens sind den von der Mitgliederversammlung beschlossenen Regelungen zu entnehmen, die nachstehend abgedruckt werden.

Wir bitten alle Mitglieder und Freundinnen und Freunde des FIfF, die Existenz dieses Studienpreises weiträumig bekannt zu machen und für Einreichungen zu werben. Eine elektronische Fassung der Regelungen findet sich unter:

www.fiff.de/studienpreis

(Ralf E. Streibl)

Studienpreis
des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V.

§1 Zweck

(1) Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. vergibt gemäß Beschluss der Mitgliederversammlung vom 15.11.2009 jährlich einen Studienpreis für herausragende Arbeiten im Themenfeld »Informatik und Gesellschaft«.

(2) Der Preis soll erstmals 2010 vergeben werden. Die Einrichtung des Studienpreises erfolgt zunächst für drei Jahre. Danach entscheidet der Vorstand über eine Weiterführung und berichtet hierüber der Mitgliederversammlung.

(3) Der Preis wird mit 333 Euro für den ersten Platz, 222 Euro für den zweiten und 111 Euro für den dritten Platz dotiert. In späteren Jahren können durch Vorstandsentscheidung die Preisgelder angepasst werden. Eine Vergabe an mehrere Preisträgerinnen/Preisträger sowie eine Teilung des Preisgeldes ist möglich.

(4) Mit dem Preis sollen herausragende Leistungen des wissenschaftlichen Nachwuchses in diesem Bereich gewürdigt und die Aufmerksamkeit der Öffentlichkeit auf das Thema der Arbeit sowie die besonderen Leistungen des Autors / der Autorin gelenkt werden.

(5) Es wird angestrebt, dass Preisträgerinnen / Preisträger ihre Arbeit im FIfF selbst präsentieren (Jahrestagung, FIfF-Kommunikation etc.).

§2 Gegenstand

(1) Der Preis wird vergeben für herausragende Qualifikationsarbeiten (i.d.R. Bachelor-, Master- oder Diplomarbeiten sowie Dissertationen).

(2) Thema und inhaltliche Ausrichtung der Arbeit muss den Zielen des Forums InformatikerInnen für Frieden und gesellschaft-

liche Verantwortung e.V. entsprechen, die in der Satzung des Vereins festgeschrieben sind.

(3) Neben Arbeiten aus der Informatik kommen auch Arbeiten aus anderen Disziplinen in Betracht, sofern in der Arbeit Themen aus dem Bereich »Informatik und Gesellschaft« interdisziplinär mit einem klaren Bezug zur Informatik behandelt werden.

§3 Vorschläge

(1) Vorgeschlagen werden können Arbeiten, die in den letzten zwei Jahren vor dem jeweiligen Nominierungsschluss abgeschlossen wurden (bei Verschiebung einer Preisvergabe verlängert sich der Zeitraum von zwei Jahren um den Zeitraum der Verschiebung).

(2) Vorschlagsberechtigt sind sowohl die Autorinnen/Autoren selbst als auch Dritte (z.B. Betreuerinnen/Betreuer, Gutachterinnen/Gutachter der Arbeit etc.). Sofern die Arbeit einer anderen Person als Vorschlag eingereicht wird, ist eine Einverständniserklärung der Autorin / des Autors hinzuzufügen.

(3) Soweit vorliegend sollten dem Vorschlag auch die dazugehörigen Gutachten beigefügt werden (nach Zustimmung der Verfasserinnen / Verfasser des Gutachtens). Sofern noch keine abschließenden Gutachten vorliegen, kann auch eine Stellungnahme der Betreuerin / des Betreuers oder einer anderen Hochschullehrerin / eines anderen Hochschullehrers beigefügt werden.

(4) Vorschläge sind einzureichen bei der Geschäftsstelle des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., Goetheplatz 4, 28203 Bremen bis spätestens 31. März des Vergabejahres. Dem Vorschlag ist eine Begründung der Nominierung sowie ein Exemplar der nominierten Arbeit beizufügen, welches in das Eigentum des FIfF übergeht. Zur Erleichterung des Auswahlprozesses sollte die Arbeit auch in digitaler Form (als PDF-Dokument) beigefügt werden. Das FIfF und die Mitglieder der Auswahlkommission werden ohne Absprache mit dem Verfasser / der Verfasserin die eingereichte Arbeit keinen weiteren Dritten zugänglich machen.

§4 Auswahlverfahren

(1) Der Vorstand des FIfF benennt eine Auswahlkommission bestehend aus fünf bis sieben Mitgliedern. Der Vorstand des FIfF bestimmt aus seinen Reihen ein Mitglied, das die Geschäftsführung übernimmt. Die Konferenz der Informatik-Fachschaften wird eingeladen, ein studentisches Mitglied für die Auswahlkommission zu benennen. Mindestens zwei Personen der Auswahlkommission sollten in der Informatik-Lehre an Hochschulen tätig sein. Die Auswahlkommission sollte in Bezug auf beruflichen Status, Geschlecht und fachliche Ausrichtung ausgewogen besetzt sein. Der FIfF-Vorstand kann eine oder mehrere Partnerorganisationen um Vorschläge für Mitglieder der Auswahlkommission bitten.

(2) Wenn ein Mitglied der Auswahlkommission feststellt, dass ihm eine unparteiliche Mitwirkung im Auswahlverfahren aufgrund besonderer Umstände nicht möglich ist (Befangenheit z.B. auf Grund von Verwandtschaft, persönlichen Bindungen, Konflikten, enger wissenschaftlicher Kooperation, unmittelbarer wissenschaftlicher Konkurrenz mit eigenen Projekten oder Plänen, Angehörigkeit zur selben wissenschaftlichen Einrichtung o.ä.), teilt es diese Bedenken dem FIfF-Vorstand umgehend mit und prüft gemeinsam mit dem Vorstand des FIfF, ob eine Beteiligung in diesem Auswahlverfahren möglich ist. Im Falle des Ausscheidens eines Mitglieds der Auswahlkommission benennt der FIfF-Vorstand umgehend ein entsprechendes Ersatzmitglied.

(3) Die Mitglieder der Auswahlkommission verpflichten sich hinsichtlich des Auswahlverfahrens zur Vertraulichkeit.

(4) Nach Sichtung der eingereichten Vorschläge bereitet die Jury bis zum 31. August des Vergabejahres eine Empfehlung zur Vergabe des Studienpreises an den FIfF-Vorstand vor. Die Auswahlkommission muss ihre Empfehlung begründen. Sofern die Auswahlkommission keine Arbeit für preiswürdig erachtet, kann sie auf die Ausübung des Vorschlagsrechtes verzichten. Sofern die Auswahlkommission der Ansicht ist, dass zu wenige Arbeiten eingereicht wurden, kann sie dem FIfF-Vorstand vorschlagen, den Vergabezeitraum um ein Jahr zu verlängern, die bislang eingereichten Arbeiten bleiben in diesem Fall alle weiterhin im Auswahlprozess. Die Empfehlung der Auswahlkommission kann auch eine Teilung des Preises vorsehen.

(5) Die Auswahlkommission prüft, ob die eingereichten Arbeiten den Vorgaben nach §2 entsprechen. Bei ihrer Entscheidung über den Vergabevorschlag berücksichtigt die Auswahlkommission die wissenschaftliche Originalität und den Innovationswert der eingereichten Arbeiten, d.h. insb. die Leistung für die Weiterentwicklung des Fachgebietes, sowie die Verständlichkeit der Darstellung.

§5 Vergabe

(1) Der Vorstand des FIfF beschließt aufgrund der Empfehlung der Auswahlkommission über die Vergabe des Studienpreises des FIfF.

(2) Die Preisvergabe ist mit einer Urkunde sowie einem Preisgeld (vgl. §1) verbunden.

(3) Die Bekanntgabe der Preisverleihung soll möglichst im Rahmen der FIfF-Jahrestagung erfolgen. Ferner sollen die Preisträgerinnen und Preisträger mit ihren Arbeiten in der FIfF-Kommunikation vorgestellt werden.

Weitere Informationen:

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V.

Goetheplatz 4
D-28203 Bremen
Tel.: 0421 - 33 65 92 55
fiff@fiff.de
www.fiff.de

Mitgliederversammlung des FIfF

Bremen, Villa Ichon

15. November 2009, 10:00-14:00 Uhr

– Beschlussprotokoll –

Sitzungsleitung: Hans-Jörg Kreowski als Vorsitzender des FIfF

1. Begrüßung und Feststellung der Beschlussfähigkeit und der Protokollführung

Die Versammlung ist beschlussfähig und dass Protokoll führt: Jens Rinne

2. Beschlussfassung über Tages- und Geschäftsordnung

Die TO wird in vorliegender Form genehmigt, Pkt. 10.1 wird als Pkt. 3 vorgezogen.

3. Antrag: Förderung eines Studienpreis für Abschlussarbeiten im Bereich Informatik und Gesellschaft

Der der MV vorgelegte Entwurf wird diskutiert und mit Änderungen einstimmig genehmigt.

4. Bericht des Vorstands (einschl. Kassenbericht)

Stefan Hügel berichtet über die Vorstandsarbeit und Hans-Jörg Kreowski über den Kassenbericht.

5. Bericht der Kassenprüfer

Für die am 24.07.09 in Bremen durchgeführte Kassenprüfung berichtet Kurt Fussangel der MV. Aus dem Kassenprüfungsprotokoll: „Dem Vorstand wird eine dem Vereinszweck entsprechende, ordnungsgemäße und sparsame Kassenführung bescheinigt." Die Kassenprüfer schlagen die Entlastung des Vorstands vor.

6. Diskussion der Berichte

Es werden keine Beschlüsse gefasst.

7. Entlastung des Vorstands

Der Vorstand wird einmütig bei 5 Enthaltungen entlastet.

8. Wahl des neuen Vorstands

8.1 Wahl der Wahlleitung

Peter Bittner (einmütig bei einer Enthaltung)

8.2 Wahl der/des Vorstandsvorsitzenden:

vorgeschlagen: Stefan Hügel

stimmberechtigt:	27 Mitglieder		
gültige Stimmen:	27		
	davon:	ja:	25
		nein:	0
		enthalten:	2

Stefan Hügel nimmt die Wahl an.

8.3 Wahl der/des stellvertretenden Vorstandsvorsitzenden

vorgeschlagen: Jens Rinne

stimmberechtigt:	27 Mitglieder		
gültige Stimmen:	26		
	davon:	ja:	22
		nein:	0
		enthalten:	4

Jens Rinne nimmt die Wahl an.

8.4 Wahl der Beisitzerinnen und Beisitzer

Vorschläge (ja/nein/enth.)

Stimmberechtigt: 27

Carsten Büttemeier
25/0/2
ja

Damit sind alle Kandidierenden gewählt und alle Anwesenden nehmen die Wahl an. Die Zustimmung der Abwesenden (Dietrich Meyer-Ebrecht, Britta Schinzel, Dirk Siefkes, Julia Stoll) wird nachträglich eingeholt werden.

Sylvia Johnigk
23/0/4
ja

Hans-Jörg Kreowski
26/0/1
ja

Dietrich Meyer-Ebrecht
25/0/2

Kai Nothdurft
25/1/1
ja

Raffael Rittmeier
25/1/1
ja

Stimmberechtigt: 27

Britta Schinzel
23/1/3

Damit sind alle Kandidierenden gewählt und alle Anwesenden nehmen die Wahl an. Die Zustimmung der Abwesenden (Dietrich Meyer-Ebrecht, Britta Schinzel, Dirk Siefkes, Julia Stoll) wird nachträglich eingeholt werden.

Dirk Siefkes
25/0/2

Julia Stoll
24/0/3

Ralf E. Streibl
26/0/1
ja

Joerg Zeltner
23/0/4
ja

Stefan Hügel übernimmt als neuer Vorsitzender des FIfF die Sitzungsleitung.

9. Neuwahl der Kassenprüfer

Michael Ahlmann, Kurt Fussangel und Gernot Lucks einmütig bei zwei Enthaltungen.

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

Katharina Just-Hahn berichtet über die Arbeit der Regionalgruppe Köln und die Pläne für die nächste Jahrestagung vom 05.-07.11.10 in Köln.

Kurt Fussangel berichtet über seine Teilnahme an einer Veranstaltung der Friedrich-Ebert-Stiftung über Grundrechte und informationelle Selbstbestimmung in Brüssel.

Raffael Rittmeier berichtet über die Bremer Regionalgruppe und wiki.fiff.de.

11. Anträge an die Mitgliederversammlung

Es liegen keine weitere Anträge der MV vor.

12: Verschiedenes

Die Anwesenden danken für die tolle Organisation dieser Jahrestagung:

13. Genehmigung des Protokolls

Das Protokoll wird einstimmig genehmigt.

Bremen, den 15. November 2009

Der neue FIfF-Vorstand


Stefan Hügel

Jens Rinne


Carsten Büttemeier


Sylvia Johnigk


Hans-Jörg Kreowski


Dietrich Meyer-Ebrecht

Kai Nothdurft

Raffael Rittmeier

Britta Schinzel


Dirk Siefkes

Julia Stoll


Ralf E. Streibl


Joerg Zeltner

Verantwortung 2.0

Erste Impressionen von der 25. FIfF-Jahrestagung

Vom 13.-15.11.2009 – nur wenige Stunden vor Drucklegung dieser FIfF-Kommunikation – fand die diesjährige FIfF-Tagung in Bremen statt. Zum vierten Male (nach 1994, 2001 und 2006) lud das FIfF damit seine Mitglieder in die Hansestadt ein, die seit 2001 ja auch Sitz der FIfF-Geschäftsstelle ist. 25 Jahre sind ein Anlass zur Rückschau, doch gleichermaßen eine Ermutigung, den Blick nach vorne zu richten. In diesem Sinne war auch das Motto *Verantwortung 2.0* zu verstehen.

Impression von der FIfF-Jahrestagung, Dagmar Boedicker

Auftaktveranstaltung

Die Tagung begann mit einer öffentlichen Auftaktveranstaltung im zentral in der Stadt gelegenen Haus der Wissenschaft. Unter dem Motto »Netz_aktiv« begann die Tagung mit zwei Beiträgen zu den Chancen , Herausforderungen und Gefahren des heutigen Internets. Stefan Pulß (Radio Bremen), der als Moderator durch die Veranstaltung führte, merkte dazu in seiner Einleitung an, dass das Thema des Abends auch illlustriere, wie sich die Themen in den letzten 25 Jahren geändert haben. Den ersten Vortrag hielt Hendrik Speck, Professor für Digitale Medien an der Fachhochschule Kaiserslautern. In seinem Vortrag stellte er mögliche gesellschaftliche Auswirkungen sozialer Netzwerke wie StudiVZ, Facebook o.ä. dar. Er stellte die Freiwilligkeit heraus, mit der die Nutzer eine Fülle privater Daten von sich preisgeben. Man wisse nicht, was mit diesen Daten passiere, sagte Speck, der zum einen auf die technische Verletzlichkeit solcher Systeme hinwies, zum anderen aber auch auf die Begehrlichkeiten, die dieser Datenschatz bei Betreibern und Wirtschaft weckt. »Wem gehören die Daten? Wer darf was? Und wer nimmt die Nutzerinteressen war?«, seien wesentliche Fragen, die gerade vor dem Hintergrund der globalen Vernetzung nur schwer bis gar nicht zu beantworten seien. Im zweiten Beitrag des Eröffnungsabends beschäftigte sich der Hamburger Journalist und Buchautor Lars Reppesgaard mit dem Unternehmen Google und seinen Strategien: Das Ziel von Google bestehe darin, die auf der Welt vorhandenen Informationen zu organisieren – diese Aussage sei keine verrückte Utopie, sondern ernst gemeinter Ausdruck von Optimismus, Technikgläubigkeit und einem gewissen Idealismus. Google habe es damit geschafft zu einer weltweiten Marke zu werden, wie Coca Cola oder Tempo. Und deren Bedeutung ist enorm: »Große Teile, die unser Leben ausmachen, sind inzwischen im Netz«, stellt er fest und unterscheidet dabei zwischen Daten, die von Nutzerinnen und Nutzern von Google-Diensten explizit hochgeladen wurden, und Daten, die bei der Benutzung von Google anfallen (= beim Betrieb gesammelt werden). Oftmals würden dabei rechtliche Grenzen in Frage gestellt oder auch überschritten. Das Prinzip „Google macht erst mal" habe dabei durchaus seine positiven Seiten, da bestimmte Bereiche sonst gar nicht angegangen würden. Dennoch gebe es Grenzen, die nicht überschritten werden sollten. Reppesgaard: Die Anhäufung von Datensammlungen habe die »das Potenzial für ganz, ganz große Katastrophen«. Im Grunde – so sein Fazit – könne man sich so eine Art von Gefährdung gesellschaftlich gar nicht leisten.

Weitere Vorträge

Am Samstag wurde die Tagung an der Universität Bremen fortgesetzt. An diesem Tag gab es drei Vorträge und fünf Arbeitsgruppen:

Constanze Kurz (HU Berlin) sprach über Möglichkeiten, anhand von Szenarien ethische Dilemmata in der Lehre zu diskutieren. Sie bezog sich dabei v.a. auf Beispiele aus dem gerade frisch erschienenen Buch »Gewissensbisse – Ethische Probleme der Informatik« von Debora Weber-Wulff, Christina Class, Wolfgang Coy, Constanze Kurz und David Zellhöfer. Es war wohl kaum ein Zufall, dass in der Diskussion zu diesem Beitrag schnell auch auf das Thema »Bologna-Prozess« und die daraus resultierenden Veränderungen im Studium zu sprechen kam, die eine kritische Auseinandersetzung mit Aspekten des eigenen Faches üblicherweise gegenüber eher »verwertbaren« Aspekten weiter in den Hintergrund drängen.

Die Ethnologin *Eliane Fernandes Ferreira* (Hamburg) berichtete über die Internetnutzung einiger indigener Gemeinschaften in Brasilien. Informationen über Projekte, welche indigenen Gemeinschaften den Zugang zum Internet ermöglicht, ergänzte sie sehr anschaulich mit ihren eigenen Erfahrungen von mehreren Aufenthalten in einigen dieser Gemeinschaften. Hierbei wurde gleichermaßen die Notwendigkeit dieser Vernetzung deutlich, wie auch die vielfältigen Schwierigkeiten und Probleme, die technisch, politische und kulturell damit verbunden sind.

Den Nachmittagsvortrag schließlich hielt der scheidende FIfF-Vorsitzende Hans-Jörg Kreowski, der gebeten worden war, das

Jubiläum des FIfF zu thematisieren. In seinem Beitrag »... vorher – 25 Jahre Informatik mit FIfF – nachher ...« stellte er zum einen Verbindungen zwischen gesellschaftlichen Entwicklungen und der Entwicklung des Faches Informatik sowie des FIfF her, zum anderen thematisierte er, was aus seiner Sicht »Verantwortung 2.0« für Informatikerinnen und Informatiker heißen könnte. Unter anderem fordert er hier ein Gegengewicht zur in vielen Zusammenhängen oftmals herrschenden Technikeuphorie und in diesem Sinne auch eine faire Chance für kritische Wissenschaft.

Arbeitsgruppen

Vier Arbeitsgruppen waren im Vorfeld der Tagung geplant und angekündigt worden (vgl. FIfF-Kommunikation 3/2009):

- Spiele ohne Grenzen (*Ulrike Erb, Heidi Schelhowe, Karin Vosseberg, Margita Zallmann*) – zu den Erlebniswelten junger Computer(rollen)spielerinnen und –spieler;
- Computer aus dem Sweatshop ... (*Dagmar Boedicker, Sebastian Jekutsch*) – zu den Arbeitsbedingungen bei der Herstellung von IT- und Elektronikprodukten, bei denen Menschenrechte ignoriert und verletzt werden;
- Informatik und Gesellschaft in der Lehre (*Karl-Heinz Rödiger, Karsten Weber*) – zur derzeitigen Situation und Möglichkeiten zur Verbesserung der Lehre in Informatik und Gesellschaft;
- Commons und Peer-Produktion (*Christian Siefkes*) – zur Frage, wie eine Gesellschaft aussehen könnte, die auf Peer-Produktion beruht und ob und wie eine Übernahme dieses Konzepts von der immateriellen in die materielle Welt möglich sei.

Eine weitere Arbeitsgruppe wurde erst kurzfristig auf der Tagung angeboten:

- INDECT (*Sylvia Johnigk, Kai Nothdurft*) – Mit dem EU-Projekt »INDECT« (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment) soll eine Überwachungsplattform zur Unterstützung der internationalen Polizeiarbeit geschaffen werden, Damit werden folgende Ziele verfolgt: Terrorismusbekämpfung, Entdeckung abnormalen Verhaltens und Bekämpfung illegaler Einwanderung. Daten, Bilder und Videos, die in realen Räumen", wie auf Straßen, Plätzen, Bahnhöfen und Flughäfen erhoben werden, sollen mittels neuartiger Suchmaschinen mit Daten aus virtuellen „Räumen", wie Chats, Foren, sozialen Netzwerken und Webseiten verknüpft werden. Eine Zusammenfassung des Projekts findet man auf den Projektseiten *www.indect-project.eu*. Einen kurzen kritischen Artikel findet man unter *http://www.zeit.de/digital/datenschutz/2009-09/indect-ueberwachung*.

Im nächsten Heft der FIfF-Kommunikation sollen die meisten Beiträge der Tagung ausführlich dokumentiert werden, so dass an dieser Stelle die kurze Umschau enden kann. An der Bremer Tagung nahmen insgesamt ca. 100 bis 120 Personen teil – allerdings verteilt über die Tage, so dass z.B. die Hauptvorträge jeweils zwischen rund 40 und 80 Personen Zuhörerinnen und Zuhörer verzeichnen konnten.

Nächste FIfF-Jahrestagung:
5. bis 7. November 2010

Auf der Mitgliederversammlung am Sonntag in der Villa Ichon wurde von Seiten der FIfF-Regionalgruppe Köln bereits auf den Termin der kommenden Jahrestagung hingewiesen, die sich dann schwerpunktmäßig Fragen des Arbeitnehmerdatenschutzes widmen soll.

(Die Redaktion)

Arbeitskreis INDECT

Nach unseren ersten Recherchen berührt das Projekt INDECT Kernthemen wie Datenschutz, Informationelle Selbstbestimmung, etc., zu denen das FIfF Stellung beziehen sollte.

Da bislang eine kritische Auseinandersetzung nur in Ansätzen erkennbar ist und scheinbar wenig Austausch stattfindet, wurde ein Arbeitskreis gebildet, welcher der weiteren Informationsbeschaffung und insbesondere der Vernetzung mit anderen Kritikern dienen soll.

Menschen, die sich am Arbeitskreis beteiligen möchten, können sich bei uns melden:

Sylvia Johnigk sylvia@fiff.de und Kai Nothdurft kai@fiff.de

Tagungsplakat, FIfF 2009

Stefan Hügel

Brief an das FIfF

„Veränderungen“

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

wenn ich diesen Brief schreibe, ist gerade eine spannende Jahrestagung zu Ende gegangen – eine Tagung, die neben interessanten inhaltlichen Vorträgen und Diskussionen auch Neuerungen im FIfF mit sich gebracht hat.

Vor allem wurde turnusgemäß ein neuer Vorstand gewählt. Nachdem **Hans-Jörg Kreowski**, wie bereits angekündigt, nicht mehr für den Vorsitz kandidiert hat – dem Vorstand bleibt er weiter erhalten – musste es hier einen Wechsel geben. Die Mitgliederversammlung hat mich zum neuen Vorsitzenden des FIfF gewählt – für das mir damit entgegengebrachte Vertrauen bedanke ich mich herzlich. Ebenso bedanke ich mich bei Hans-Jörg Kreowski für die in den letzten Jahren geleistete Arbeit, die das FIfF in einer kritischen Phase wesentlich voran gebracht hat.

Man kann diesen Wechsel – wenn man möchte – auch als Generationswechsel begreifen: Erstmals hat das FIfF einen Vorsitzenden, der die (nicht nur) friedenspolitischen Debatten im FIfF der 80er Jahre – der Gründerjahre, sozusagen – nicht mehr selbst aktiv miterlebt hat.

Auch an den anderen Positionen gab es Veränderungen – die Zusammensetzung des neuen Vorstands findet Ihr am Ende des Hefts. Bei den ausgeschiedenen Vorstandsmitgliedern möchte ich mich im Namen des FIfF für ihre jeweiligen Tätigkeiten und Aktivitäten bedanken. Besonders hervorheben möchte ich hier **Werner Hülsmann**, der als langjähriges Vorstandsmitglied wesentliche Beiträge für das FIfF geleistet hat. Er hat sehr aktiv die Arbeit im AK Vorratsdatenspeicherung im Namen des FIfF mitgestaltet und vertritt das FIfF seit vielen Jahren in der Jury der BigBrotherAwards – eine Funktion, die er auch weiterhin ausfüllen wird. Vielen Dank dafür.

Auch **Michael Riemer**, der vor seiner Vorstandstätigkeit auch als Geschäftsführer für das FIfF aktiv war, scheidet aus dem Vorstand aus.

Es gilt auch – etwas verspätet – unsere neue **Geschäftsführerin** willkommen zu heißen. **Barbara Oechsler** wird nun gemeinsam mit Christian Lilienthal unsere Geschäftsstelle betreuen. Sie hat damit **Anja Riemer** abgelöst, die sich beruflich verändern wollte und der ich dafür alles Gute wünsche.

Doch Personen sind die eine Sache, Inhalte die andere, wichtigere. Die Mitgliederversammlung hat in Bremen beschlossen, einen **Studienpreis** für herausragende Arbeiten auf dem Gebiet **Informatik und Gesellschaft** zu vergeben. Wir wollen damit ein Zeichen setzen und das Themengebiet in Lehre und Forschung fördern – ein Themengebiet, dem aus meiner Sicht viel zu wenig Bedeutung beigemessen wird. Durch die Sparzwänge im Bildungsbereich, die damit einhergehenden Verteilungskämpfe und die jüngsten Studienreformen wird es weiter marginalisiert – selbst an den Hochschulen, an denen es überhaupt als Teil des Studiums vorgesehen war.

Erfreulich ist, dass ein Appell Hans-Jörg Kreowskis im letzten Heft auf fruchtbaren Boden gefallen ist: Die Regionalgruppe Köln plant, 2010 die nächste **Jahrestagung** auszurichten. Auch für die weitere Zukunft (nach 2011) wurde schon entsprechende Bereitschaft signalisiert. Damit dürfen wir uns auf weitere interessante Tagungen freuen, Tagungen die häufig mehr Zuspruch verdient hätten, als sie letztendlich, gemessen an den Besucherzahlen, bekommen.

Auch sonst haben wir es mit Veränderungen zu tun. Wenn auch unsere Bundeskanzlerin dieselbe bleibt, so gibt es auch Veränderungen durch den Wahlsieg des **christlich-liberalen Lagers**. Zumindest im Bereich der Bürgerrechte können wir die Übernahme des Amts der Justizministerin durch eine profilierte Bürgerrechtlerin begrüßen. Aber auch hier heißt es: weiter wachsam sein! Betrachtet man die Ergebnisse der Koalitionsverhandlungen genauer, findet man wenig substanzielle Verbesserungen; stattdessen werden Regelungen als Fortschritt angepriesen, die bei genauerer Betrachtung lediglich den Status Quo festschreiben. Wir werden also die weiteren Entwicklungen genau beobachten und uns frühzeitig einmischen müssen.

Eine andere wichtige Veränderung liegt jetzt genau 20 Jahre zurück. Wir feiern in diesen Wochen den **Fall der Mauer** und damit das Ende eines Regimes, das Überwachung durch die Staatssicherheit zum Prinzip erhoben hat. Doch auch heute geht ein Risiko ein, wer zu viel von sich und seinen Meinungen preisgibt. Soziale Netze beispielsweise, die von potenziellen Arbeitgebern durchforstet werden, um Informationen über Bewerber zu sammeln und Einstellungen davon abhängig zu machen. Freiheit hat nicht nur staatliche, sondern auch wirtschaftliche Voraussetzungen – dieser Zusammenhang wird freilich selten hergestellt.

Ein anderer wichtiger Termin steht, wenn ich diesen Brief schreibe, kurz bevor – wenn er veröffentlicht wird, werden wir bereits das Ergebnis kennen: Das Bundesverfassungsgericht fällt am 15. Dezember 2009 sein **Urteil über die Vorratsdatenspeicherung**. Spekulationen über das Urteil spare ich mir: sie werden, wenn Ihr dieses Heft in Händen haltet, veraltet sein ...

Eins hat sich leider nicht verändert: Auch in den letzten Wochen lesen wir – manchmal fast täglich – von Datenpannen, „verlorenen“ Daten und einer skandalösen Überwachungspraxis.

Wir sehen – es bleibt noch viel zu tun: Für den neugewählten Vorstand, für das FIfF als Ganzes und für alle, die sich in diesen Themen engagieren. Ich freue mich auf ein spannendes FIfF-Jahr 2010 und wünsche allen Leserinnen und Lesern dieser FIfF-Kommunikation dafür alles Gute.

Mit fiffigen Grüßen

Stefan Hügel

Sebastian Jekutsch

Mythen und Missverständnisse über die ~~eCard~~ eGK

Nachdem die Agenturen früh von einem „Moratorium für die elektronische Gesundheitskarte“ schrieben, im Koalitionsvertrag aber ziemlich unklar ein „Überprüfen der Strukturen“ gefordert wurde, hat sich der neue Gesundheitsminister inzwischen dafür ausgesprochen, dass der im Oktober begonnene Rollout der ersten Version weitergehen soll. Die bisherigen Funktionen, so das Argument, entsprächen der altbekannten Krankenversicherungskarte und die sei ja unkritisch. Neu geprüft werden sollen also vor allem die neuen Funktionen der Karte, Patientenakte, Notfallausweis, eRezept, Arztbrief, sowohl aus Anwendersicht – siehe Probleme mit der PIN und der Langsamkeit, die FIfF-Kommunikation berichtete – als auch aus Datenschutzsicht. Vielleicht ist es also an der Zeit, über ein paar Mythen und Missverständnisse aufzuklären, wobei wir mal so tun, als seien alle versprochenen bzw. angedrohten Funktionen schon Realität.

Mythos: Meine Gesundheitsdaten stehen auf der Karte

Oft wird von „auf die Karte speichern" geschrieben, aber es kommt nur wenig auf die Karte, sie hat auch nur wenig Speicherplatz. Direkt auf der Karte stehen nur die üblichen Versichertendaten und – wenn gewünscht – die Notfalldaten. Der Rest sind lediglich Verweise auf Daten, die verschlüsselt in großen Rechenzentren irgendwo im Land gespeichert sind. Dazu braucht es zwei wichtige Datensätze ebenfalls auf der Karte: Den Schlüssel zum Ver- und Entschlüsseln und ein Logbuch der Zugriffe auf die Karte und damit indirekt auf die Daten.

Missverständnis: Meine Gesundheitsdaten sind im Internet gespeichert

So hat es sogar die Gesellschaft für Informatik in einer Stellungnahme aus dem Jahr 2005 formuliert. „Im Internet gespeichert“ ist natürlich ähnlich simpel gedacht wie „das Internet ausdrucken“. Wahr ist, dass kein neues physikalisches Netz aufgebaut wurde für die Gesundheits-Telematik, das wäre viel zu teuer geworden, genutzt werden daher genau die Wege, die auch ein Internetzugang nutzt. Die Kommunikation findet aber nicht mit den üblichen Internetanwendungsprotokollen (http, ftp) statt, auch wenn die Kommunikationsbasis in der Tat TCP/IP ist. Realisieren tut das der *Konnektor* beim Arzt, der zwischen Lesegerät und Internetzugang geschaltet wird, sobald die Karte Online-Funktionen haben wird. Dass man sich später die Gesundheitsdaten des Nachbarn er-google-n können wird, ist ein Märchen.

Ungenau: Die Daten liegen auf einem zentralen Server

Das ist fast richtig. Oben wurde schon erwähnt, dass fast nichts auf der Karte selbst steht. Verteilt werden die anderen Daten auf verschiedene Server, die eRezepte zum Beispiel woanders als die Patientenakten. Im Grunde macht es auch keinen Unterschied, *wo* etwas gespeichert ist, wichtig ist, ob es einen von allen Stellen aus einheitlichen Zugriff auf die Daten gibt. So sind all die Webseiten auf der Welt auf wer weiß wie vielen Servern verteilt, die Infrastruktur erlaubt es aber, dass ich mit http einen homogenen Zugriff auf alle Seiten habe. Das ist quasi zentral, und die Kritik daran greift: Eingebrochen wird auf Datenbanken ja auch nicht, indem man die Festplatten klaut, sondern man schafft sich Zugriff von außen über die Datenleitungen.

Mythos: Wenn der zentrale Server gehackt wird, sind die Daten aller Patienten bekannt

Das geht nicht, weil auf den Servern praktisch nur Datenmüll steht. Die Gesundheitsdaten sind nämlich verschlüsselt – und jeder Patient hat einen eigenen Schlüssel. Selbst der kritischste Informatiker wird nicht behaupten, dass man einen dieser Schlüssel knacken könnte, geschweige denn alle. Man muss pro Patient also an den Schlüssel ran. Der Schlüssel ist nur auf der Karte des Patienten. (Genauer steht es beim nächsten Mythos.) Er verlässt auch nie die Karte, denn die Karte verschlüsselt die Daten selbst, sie ist ein kleiner Computer. Somit ist zwingende Vor-

aussetzung für das Entschlüsseln der Daten eines Patienten der zumindest kurzfristige Besitz seiner Karte. Die anderen Voraussetzungen sind: PIN, Lesegerät plus Konnektor und der Heilberuflerausweis.

Mythos: Wenn ich die Karte verliere, sind meine Daten weg

Die reine Lehre der IT-Sicherheit sagt: Ja, natürlich! Denn die Daten auf den Servern sind zwar nicht weg, aber mit der Karte ist die einzige Stelle weg, auf der der Schlüssel zum Entschlüsseln gespeichert ist. Die Realität ist leider anders: Das eGK-Gesetz schreibt vor, dass die Daten wiederherstellbar sein müssen. Das heißt, die Schlüssel aller Patienten müssen noch woanders gespeichert sein; dies ist sicherlich die größte Sicherheitslücke der elektronischen Gesundheitskarte. Wenn die Karte weg ist, sollen Daten damit umgeschlüsselt werden können, d.h. der Patient bekommt eine neue Karte mit neuem Schlüssel. Die altverschlüsselten Daten müssen dann vorher mit einem zentralen Dienst passend neu verschlüsselt worden sein.

Dabei ist diese Sicherheitslücke eigentlich gar nicht nötig, denn die Gesundheitsdaten sind noch woanders gespeichert: Bei den Ärzten. Die schaffen ihre Akten und ihre Praxis-IT nämlich nicht ab, dort bleibt alles wie es war. Verliert man seine Daten, könnte man sie sich also bei den Ärzten wieder zusammensuchen, die eRezepte eingeschlossen. Weg wären dann nur die Notfalldaten, die evtl. speziell gesetzten Zugriffsrechte für die Daten und die Daten, die Patienten selbst auf der Karte gespeichert haben.

Missverständnis: Die PIN ist der Schlüssel

Die PIN ist ein weiteres Sicherheitsmerkmal. Man kennt das von der EC-Karte: Wenn man die Karte verliert oder sie geklaut wird, dann hilft das dem Dieb erstmal nicht, denn die Server rücken die Daten nur raus, wenn eine passende PIN mitgeschickt wird. Die Daten kommen weiterhin verschlüsselt in der Arztpraxis an und werden erst in der Karte entschlüsselt, weil auf dieser der Schlüssel steht. Die PIN steht selbstredend nicht auf der Karte. PIN und Schlüssel haben rein gar nichts miteinander zu tun.

Mythos: Die Krankenkasse kann meine Daten lesen

Das stimmt nicht. Mit Ausnahme der so genannten Versichertenstammdaten (also etwa der Daten, die auch jetzt schon auf der Krankenversichertenkarte stehen), die die Kasse selbst auf die Karte schreiben lässt, kann die Krankenkasse nichts lesen, wenn der Patient es nicht will. Die Kassen haben nicht einmal einen Heilberuflerausweis, geschweige denn, dass sie die Schlüssel zu den Daten ihrer Kunden hätten. Die Kasse bekommt aber dennoch wegen der Abrechnungsnotwendigkeit mit dem Arzt ziemlich viel von den Patienten mit. Das ist heute auch schon so.

Mit dem Gesetz, das auch die Karte einführte, ist die Möglichkeit neu entstanden, dass die Kassen bessere Statistiken über ihre Patienten führen können. Dazu werden einige der Gesundheitsdaten pseudonymisiert, d.h. ein Patient taucht nur noch als Geschlecht + Alter + Wohngegend +... auf. Die endgültige Festlegung dieses Pseudonyms steht noch aus, die bisherigen Ideen geben aber einigen Anlass zur Kritik. Dies sollten wir kritisch beobachten.

Missverständnis: Die Krankenkasse bekommt jedesmal sofort mit, wenn ich beim Arzt bin

Dieses Gerücht basiert auf der Tatsache, dass bei jedem Einstecken der Gesundheitskarte in das Lesegerät eines Arztes oder Apothekers die oben erwähnten Versichertenstammdaten geprüft werden. Es könnte nämlich sein, dass die Karte gesperrt ist oder dass der Zuzahlungsstatus sich geändert hat oder einfach nur die Adresse des Patienten. Deshalb werden die Daten auf der Karte von zentraler Stelle aus aktualisiert. Die aktuellen Daten stellen in der Tat die Krankenkassen zur Verfügung, nicht aber die Anwendung und den Server, die dieses Update übernehmen.

Diese Überprüfung der Stammdaten ist übrigens nicht Teil des derzeitigen Rollouts, also des Release 1. Die erste Version der Gesundheitskarte kommt noch komplett ohne Netzzugang aus.

Unsinn: Meine Gesundheitsdaten sind sicher

Nur nicht existierende Daten sind sicher vor Missbrauch. Das klappt in unserem Fall jetzt und in Zukunft nur, wenn man nie zum Arzt geht.

Ungenau: Wenn meine Karte geklaut wird, hat der Dieb Zugriff auf meine Daten

Der Dieb braucht auch einen Heilberuflerausweis, deren PIN, die dazu passenden Zugriffsrechte, Lesegerät plus Konnektor – all dies ist bei einem Arzt des Patienten – und die PIN der Gesundheitskarte. Aber dann kann es losgehen. Leichter wird ein Missbrauch, wenn die private Nutzung der Karte am heimischen PC oder an speziellen öffentlichen Terminals, so genannten Kiosken, ermöglicht werden sollte. Auch hier sind die Pläne noch nicht konkret genug, dass man sich ein klares Bild des Risikos machen könnte.

Sebastian Jekutsch

Sebastian Jekutsch ist FIfF-Mitglied. Wen noch Unklarheiten plagen oder wer weitere Mythen vermutet, der nutze bitte den Kontakt: *sj@fiff.de*.

Unwahrscheinlich: Wenn ich nicht mitmache bei der Patientenakte und anderem, dann erhöht die Kasse zur Strafe die Beiträge

Laut Gesetz ist das verboten. Es wird oft als Argument benutzt, dass man Gesetze verändern kann, siehe Pläne mit den Mautdaten. Damit lässt sich natürlich jedes Gesetz diskreditieren. Wir sollten aufpassen, wen wir in die Legislative wählen.

Gefahr: Wenn das Internet zusammenbricht, bricht auch das Gesundheitssystem zusammen

Es soll stets einen konventionellen, papierbasierten Ersatzbetrieb geben. Allerdings ist wohl zu erwarten, dass sich früher oder später die Telematik-basierten Geschäftsprozesse derart verfestigen, dass eine Abhängigkeit entsteht. Das gilt jetzt schon für viele andere Bereiche.

Verwechslung: Die Abkürzung für die elektronische Gesundheitskarte ist e-Card

e-Card bezeichnet eigentlich eine Signaturkarte für die Bürger für eGovernment-Prozesse, d.h. eine Möglichkeit, Dokumente elektronisch zu unterschreiben und somit behördliche Vorgänge (z.B. Steuererklärungen) elektronisch und online erledigen zu können. Für die Gesundheits-Telematik ist eine solche Signaturfunktion lediglich bei den Heilberuflerausweisen (HBA) vorgesehen (Arzt unterschreibt eRezepte u.ä.), nicht bei der *eGK* des Patienten. Sie soll laut Gesetz allerdings technisch dafür geeignet sein.

Die eGK kann also noch zur e-Card werden. Dann würde sie in Konkurrenz treten zum elektronischen Personalausweise (ePA) und der so genannten JobCard, die als elektronischer Sozialversicherungsausweis z. B. ALG-II-Anträge noch effizienter ablehnbar machen wird. Es gibt also noch viele Anlässe, der IT-Industrie staatlicherseits weitere Konjunkturpakete zu verschaffen.

Stefan Hügel

BigBrotherAwards 2009

Auch 2009 wurden die BigBrotherAwards vergeben – zum zehnten Mal. Die Favoriten, vor allem aus der Politik, konnten die in sie gesetzten Erwartungen erfüllen.

1984 – Sinnbild für allgegenwärtige Überwachung durch einen immer präsenten Staat. George Orwell beschrieb in seinem Roman eine Staatsmacht, der sich niemand entziehen kann. Auch wenn seine Negativ-Vision – inspiriert durch Faschismus und Stalinismus – in dieser Form nicht Wirklichkeit wurde, leben wir heute unter einer immer umfassenderen Überwachung. Dabei ist es nicht nur der Staat, sondern auch Wirtschaftsunternehmen, die Daten über uns sammeln. Die Möglichkeiten hätte sich Orwell vermutlich nicht träumen lassen – auch wenn unsere Wohnungen nicht mit einem Televisor ausgestattet sind, schreitet Überwachungstechnik immer weiter fort.

Besonders herausragende Beispiele wurden auch 2009 wieder durch die BigBrotherAwards in Bewusstsein der Öffentlichkeit geholt. In den Kategorien Sport, Arbeitswelt, Wirtschaft, Politik und Lebenswerk wurden die diesjährigen Preise verliehen. Zusätzlich gab es wie jedes Jahr den Publikumspreis.

Grußwort von Gerhart Baum

Gerhart Baum, ehemaliger Innenminister und profilierter Bürgerrechtler konnte zwar nicht persönlich anwesend sein, er ließ den Organisatoren aber ein Grußwort zukommen. Er beglückwünschte die Organisatoren zu 10 Jahren BigBrotherAwards für ihren Beitrag, Gefährdungen der Grundrechte sichtbar zu machen und schrieb:

Sie haben mit Ihrem Einsatz für die Bürgerrechte und für den Datenschutz in den letzten Jahren Pionierarbeit geleistet, und zwar bevor viele andere das Thema entdeckt hatten. Die Zivilgesellschaft muss die Politiker aufrütteln. Es muss Bewusstsein dafür geschaffen werden, dass der Schutz der Privatheit für die Qualität unserer demokratischen Ordnung unverzichtbar ist.

10 Jahre BigBrotherAwards – eine Bilanz

Eine Bilanz von zehn Jahren BigBrotherAwards zog danach Rena Tangens. Dabei ging sie auf die Themen ein, die teilweise erst durch einen BigBrotherAward öffentliche Aufmerksamkeit auf sich gezogen haben – und auf die Reaktionen der Preisträger. Wenige hatten den Mut, zur Preisverleihung zu erscheinen – so ist auch dieses Jahr keiner der Preisträger gekommen. Stattdessen wurde versucht, den BigBrotherAward zu ignorieren oder gar dagegen zu klagen. Wesentlicher Erfolg der BigBrotherAwards ist das Bewusstsein für Datenschutz, dass dadurch in der Öffentlichkeit entstanden ist:

Das Thema Datenschutz ist heute in der Mitte der Gesellschaft angekommen. Heißt das, die BigBrotherAwards haben sich überholt? Wohl kaum, denn der unsichtbare, unfühlbare, anonyme, digitale „Große Bruder" legt sich wie eine riesige Datenkrake über das Land. Dagegen helfen nur Aufklärung, Transparenz, gute Gesetze und – die Leidenschaft, sich für Freiheit und Bürgerrechte einzusetzen.

Kategorie „Sport“

Erstmals wurde ein Award in der Kategorie Sport vergeben. Gewinner war das **Berliner Organisationskomitee der Leichtathletik-WM** für die umfassende Überprüfung von Journalisten durch die Sicherheitsbehörden, die Voraussetzung für eine Akkreditierung bei der Veranstaltung war. Fredrik Roggan von der Humanistischen Union hielt die Laudatio.

Für eine Akkreditierung bei der Leichtathletik-WM war die schriftliche Zustimmung dazu notwendig, dass der Polizeipräsident von Berlin Auskünfte über sie aus Datenbanken der Landeskriminalämter erteilen und die Personalien auch an Verfassungsschutz und Bundesnachrichtendienst weiterleiten dürfe. Bei Vermerken wäre das Berliner Organisationskomitee der WM über diese Tatsache informiert worden. Damit werden Sportjournalisten pauschal als potentiell Kriminelle, zumindest aber mit Verfassungsfeinde verdächtigt, die innere oder äußere Belange der Bundesrepublik gefährden könnten.

Eine solche Überprüfung kollidiert heftig mit der Pressefreiheit, die im Grundgesetz, Art. 5 Abs. 1 garantiert wird: „Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.“ Für Journalisten muss es ausreichen, dass sie ihren Presseausweis vorlegen, um von öffentlichen Veranstaltungen berichten zu können.

Kategorie „Arbeitswelt“

Den BigBrotherAward in der Kategorie Arbeiswelt erhielt – stellvertretend für viele Unternehmen, die die Überwachung ihrer Mitarbeiter immer mehr vorantreiben – die **Claas Landmaschinen GmbH**.

Das Unternehmen erhält den Preis stellvertretend für alle, die glauben, man erhielte produktive und motivierte Mitarbeiterinnen und Mitarbeiter durch möglichst flächendeckende und umfassende Überwachung und Messung ihrer Leistung, so Laudatorin Karin Schuler von der Deutschen Vereinigung für Datenschutz.

Mähdrescher der Firma Claas sind mit einem satellitengestützten Trackingsystem ausgestattet. Damit können die Maschinen ständig per Google Earth-Karte verfolgt und jede Unterbrechung der Fahrt registriert werden. Der Hersteller wirbt für die Überwachung so: Man wolle „gute Fahrer noch besser machen.“

Doch die Claas Landmaschinen GmbH erhielt den Preis auch stellvertretend für eine ganze Reihe weiterer Unternehmen, die in den letzen Monate durch ihre Überwachungspraxis Schlagzeilen gemacht haben. Alles Beispiele für eine stete Aushöhlung der Persönlichkeitsrechte von Arbeitnehmerinnen und Arbeitnehmern.

Kategorie „Politik“

Viel Publicity erhielt in diesem Jahr die Bundesministerin für Familie, Senioren, Frauen und Jugend, Dr. Ursula von der Leyen, für ihren Vorstoß, mit dem sie sich den Bürgern als wackere Kämpferin wider die Kinderpornographie präsentieren wollte. Dazu und für ihren persönlichen Wahlkampf benutzte sie das Leid sexuell missbrauchter Kinder, ohne tatsächlich irgendetwas gegen Missbrauch zu unternehmen. Dies betonte Laudator Alvar Freude vom Förderverein Informationstechnik und Gesellschaft (Fitug).

Allein – die Publicity, die sie bekam, war nicht überall die, die sie sich vielleicht erhofft hatte. Unter anderem war ihre Initiative der Anlass für die bisher erfolgreichste Internet-Petition: 134.000 Bürgerinnen und Bürger wandten sich gegen ihre Pläne, Kinderpornographie durch ein Stoppschild zu verhängen.

Für die Ablehnung solcher Internet-Sperren gibt es zwei wesentliche Gründe:

- Die Sperren sind für den Schutz von Kindern vor sexuellem Missbrauch und die Verminderung der Verbreitung entsprechender Darstellungen nicht nur untauglich, sondern sogar kontraproduktiv. Gleichzeitig gäbe es bessere und wirksamere Methoden, die freilich im Wahlkampf nicht so viel Aufmerksamkeit erzeugen.
- Die Sperren etablieren eine technische Infrastruktur zur Internet-Zensur, mit der beliebige Inhalte kontrolliert und blockiert werden können. Ein solches Überwachungsinstrument greift nicht nur in unsere freiheitlich-demokratischen Grundrechte ein, sondern ist auch ein erster Schritt der Politik, sich den virtuellen Raum Internet zu unterwerfen.

Die Begründungen Frau von der Leyens halten kaum einer Überprüfung stand: weder die angeblichen Milliardenumsätze, noch die offene Zugänglichkeit für jedermann, noch die Wirksamkeit der Stoppschilder als Maßnahme gegen den Missbrauch. Die Bundesregierung musste in einer Stellungnahme einräumen, keine genauen Kenntnisse über den gesamten Themenbereich zu haben. Nicht über die Verbreitungswege, die Ursprungsländer oder die Umsätze beim oft zitierten massenhaften kommerziellen Vertrieb. Die Behauptung, Kinderpornographie würde aus Indien verbreitet und sein dort nicht verboten musste von der Leyen kurz darauf zurücknehmen – Kinderpornographie ist in Indien schon lange verboten. Die Server stehen auch nicht in so genannten „failed states“, sondern mehrheitlich in den USA und Westeuropa einschließlich Deutschland.

Dafür, dass sie im Internet eine Zensurinfrastruktur errichten wollte, und gleichzeitig auf dem Rücken missbrauchter Kinder Wahlkampf betrieb, wurde Ursula von der Leyen der BigBrotherAward in der Kategorie Politik verliehen.

Kategorie „Wirtschaft“

Eine ganze Reihe von Preisträgern gab es in der Kategorie Arbeitswelt: Gewonnen haben die **Firmen, die Überwachungstechnik für Internet und Telefon anbieten** und damit gutes Geld verdienen, aber am liebsten im Verborgenen bleiben möchten. Frank Rosengart vom Chaos Computer Club zählte in seiner Laudatio unter anderem auf:

- Die Firma Quante Netzwerke GmbH bietet Internetprovidern die technische Abwicklung und die juristische Prüfung von behördlichen Überwachungsanordnungen an.
- Die Data Retention Suite der Firma Utimaco Safeware aus Oberursel ist spezialisiert auf die Umsetzung der Vorratsdat enspeicherung.

- Auf das Mitlauschen im Internet ist die Firma Datakom in Ismaning spezialisiert.
- Syborg liefert vor allem Systeme zum Mitschneiden von Gesprächen zur amtlichen Datenerhebung und Ausleitung.

Diese und weitere Produkte tragen dazu bei, dass unser aller Grundrechte weiter unterlaufen und sukzessive ausgehebelt werden. Deswegen wurde den Herstellerfirmen der BigBrotherAward verliehen.

Kategorie „Lebenswerk"

Seit Jahren ganz vorne in den Favoritenlisten ist der scheidende Bundesinnenminister Dr. Wolfgang Schäuble. Obwohl ihm vor zwei Jahren eigens eine „Nicht-Laudatio" gewidmet wurde, war er bisher bei den BigBrotherAwards nicht erfolgreich. Dieses Jahr wurde ihm nun der Preis für sein Lebenswerk verliehen.

Laudator Rolf Gössner von der Internationalen Liga für Menschenrechte hob die durch Schäuble betriebene Enttabuisierung hervor, die weiterer Entfesselung staatlicher Gewalt den Weg ebne. Indizien dafür seinen seine Bemühungen, „Terroristen" ihre Rechte abzusprechen und die rechtsstaatlich garantierte Unschuldsvermutung in Abrede zu stellen. Der Mensch mutiere in Schäubles Sicherheitskonzeption zum reinen Sicherheitsrisiko.

Als zwei wesentliche Ansätze Schäubles nannte er:
- die Zentralisierung, Vernetzung und Verzahnung von Polizei und Geheimdiensten, die Schäuble vor allem mit den Intrumenten der Antiterrordatei, dem Umbau des Bundeskriminalamts zur einem deutschen „FBI" mit weitreichenden Befugnissen und der Einrichtung einer Bundesabhörzentrale verfolgt,
- die Militarisierung der inneren Sicherheit durch den Einsatz der Bundeswehr im Inneren gegen das grundgesetzlich gebotene Trennungsgebot von Militär und Polizei und durch das Konzept des „Quasi-Verteidigungsfalls", mit dem er den Abschuss von Zivilflugzeugen ermöglichen will – gegen das verfassungsrechtliche Gebot der Menschenwürde, wie das Bundeverfassungsgericht in seinem Urteil feststellte.

Bemerkenswert nannte Laudator Gössner die Verachtung gegenüber Entscheidungen des Bundesverfassungsgerichts und deren Unterlaufen mit Hilfe von Grundgesetzänderungen. Sein Vermächtnis als Bundesinnenminister ist ein Papier, in dem er u.a. die Freigabe der LKW-Mautdaten zur Strafverfolgung, den genetischen Fingerabdruck als erkennungsdienstliche Standardmaßnahme, den erweiterten Bundeswehreinsatz im Innern, die abermalige Verschärfung des Terrorismusstrafrechts sowie die „Fortentwicklung des Verfassungsschutzes" zu einer neuen Geheimpolizei fordert.

Für seinen Beitrag zum Abbau der Bürgerrechte erhielt Wolfgang Schäuble zusätzlich den Publikumspreis.

Quellen

BigBrotherAwards Deutschland, http://www.bigbrotherawards.de

Stefan Hügel

Ereignis-Log 4/09

Immer häufiger gibt es Ereignisse, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau von Bürgerrechten stehen. Wir dokumentieren hier einige davon. Die Aufzählung kann nicht vollständig sein; die Aufzählung einiger besonders bedeutsamer Ereignisse soll aber auf die weiterhin besorgniserregende Entwicklung hinweisen.

August 2009

21. August 2009: Nach einer Umfrage des Dimap-Instituts wird das Internet immer mehr von Personalabteilungen als als Quelle für Informationen über Bewerber genutzt. Dabei werden Bewerber auf Hobbies, Interessen, Meinungsäußerungen und private Vorlieben getestet. In der Folge werden viele erst gar nicht zu einem Bewerbungsgespräch eingeladen (Quellen: Berliner Zeitung, Heise).

22. August 2009: Nach einer umfassenden Kontrolle der Videokameras an öffentlich zugänglichen Orten kommt der niedersächsische Landesdatenschutzbeauftragte, Joachim Wahlbrink, zu dem Ergebnis, dass die Zahl der von Firmen und Behörden installierten Kameras erheblich zugenommen habe. Dabei fehlten häufig die vorgeschriebenen Verfahrensbeschreibungen und Hinweisschilder; häufig seien die Kameras auf Wohn- und Firmenräume gerichtet (Quelle: Heise).

25. August 2009: Ein interner Bericht der Metropolitan Police in London stellt fest, dass pro 1000 Überwachungskameras in Großbritannien lediglich eine Straftat aufgeklärt wird. Grund dafür sei die mangelhafte Auswertung des Materials; häufig würden die aufgezeichneten Daten überhaupt nicht gesichtet (Quellen: Heise, netzpolitik.org).

28. August 2009: Umsetzungsvorgaben für Web-Sperren sollen geheimgehalten werden. Laut Amtsblatt 16/2009 wird die Richtlinie als nur für den Dienstgebrauch verwendbare Geheimakte eingestuft. Nach öffentlicher Kritik wird die Geheimhaltung später zurückgenommen (Quelle: Heise).

September 2009

4. September 2009: Diebold hat seinen Geschäftsbereich für Wahlsysteme an den bisherigen Konkurrenten Election Systems

& Software (ES&S) verkauft. Bei den Wahlmaschinen von Diebold wurden immer wieder Sicherheitslücken oder Designmängel aufgedeckt; die Hersteller sahen sich wiederholt Regressforderungen ausgesetzt (Quellen: Heise, netzpolitik.org).

6. September 2009: Bei der CDU-Fraktion im Rat der Stadt Geldern wurden persönliche E-Mails zur Fraktionsspitze „umgeleitet". Betroffene haben Strafanzeige gestellt. Die Fraktionsvorsitzende verglich das Einsehen der privaten E-Mails mit dem Lesen von Postkarten und sieht deshalb keine rechtlichen Probleme (Quelle: Heise).

12. September 2009: Zehntausende Teilnehmer haben in Berlin gegen Überwachung in Staat und Wirtschaft demonstriert. Zu der Demonstration unter dem Motto „Freiheit statt Angst – Stoppt den Überwachungswahn" hatte ein breites Bündnis – unter anderem das FIfF – aufgerufen (Quellen: Arbeitskreis Vorratsdatenspeicherung, Heise, netzpolitik.org).

13. September 2009: Nach der Demonstration „Freiheit statt Angst" wurde das überharte Vorgehen der Polizei gegen Überwachungsgegner kritisiert. Ein Video zeigt, wie Polizeibeamte einen Demonstranten ins Gesicht schlagen, zu Boden zerren und treten. Gegen die Beamten wurden Ermittlungen wegen Körperverletzung im Amt eingeleitet (Quellen: Chaos Computer Club, Heise, netzpolitik.org).

16. September 2009: Das Verwaltungsgericht Köln hat einen Antrag von Hansenet zur Brefreiung von Vorratsdatenspeicherung abgelehnt. Das Unternehmen wollte eine Ausnahme von der Verpflichtung zur verdachtsunabhängigen Vorratsdatenspeicherung erreichen (Quelle: Heise).

19. September 2009: Bei der Deutschen Bank wurde per Rasterfahndung nach einer undichten Stelle gesucht. Das Unternehmen glich die von Anschlüssen der Bank aus gewählten Zielrufnummern mit bekannten Telefonnummern von Journalisten ab (Quellen: Spiegel, Heise).

21. September 2009: Der Koalitionsvertrag der sächsischen CDU-FDP-Koalition sieht die Ausdehnung der Überwachung der Internet-Telefonie vor. Die dabei eingesetzte Technik ist vergleichbar mit der Technik für heimliche Online-Durchsuchungen (Quellen: FDP, Heise).

23. September 2009: Web-Seiten von MySpace und weiteren Plattformen in der Türkei gesperrt. Die Sperre gegen die Webseiten von MySpace sowie Lastfm.com.tr und die Online-Videoplattform Akilli.tv seit dem 19. September wurden durch einen Istanbuler Staatsanwalt in einem Urheberrechtsverfahren am 26. Juni dieses Jahres angeordnet (Quellen: Heise, netzpolitik.org, Deutschlandfunk).

23. September 2009: Das Verwaltungsgericht München hat eine Klage gegen automatisches Scannen von Kfz-Kennzeichen abgelehnt. Die Kammer widersprach der Auffassung des Klägers, dass die Vorschriften im Bayerischen Polizeiaufgabengesetz (PAG) zu unbestimmt und überdies unverhältnismäßig seien (Quellen: Heise, netzpolitik.org, daten-speicherung.de).

23. September 2009: Zahl der Verfahren, bei denen Telefon- und Computerkommunikation überwacht wurde, ist um 11% gestiegen. 2007 waren es noch 4806 solcher Verfahren; diese Zahl betrug im vergangenen Jahr 5348 (Quellen: Süddeutsche Zeitung, Heise).

23. September 2009: Bei den Österreichischen Bundesbahnen (ÖBB) wurden jahrelang rechtswidrig Krankendaten der Mitarbeiter gesammelt und bei der Entscheidung über die Karriereentwicklung zugrunde gelegt. Dabei wurden Beschäftigte zur Auskunft über Krankheiten und Diagnosen unter Androhung der Kündigung gezwungen (Quelle: Heise).

25. September 2009: Ein Papier aus dem Bundesinnenministerium sieht erhebliche Erweiterung staatlicher Befugnisse für die innere Sicherheit vor. Unter sieht das Papier die Erweiterung der Befugnisse des Verfassungsschutzes in Bereiche vor, die bisher Domäne der Polizei waren. Der genetische Fingerabdruck soll als erkennungsdienstlicher Standard etabliert werden (Quellen: Heise, netzpolitik.org).

27. September 2009: Die Wahlen zum 17. Deutschen Bundestag ergeben eine Mehrheit für eine christlich-liberale Koalition aus CDU, CSU und FDP. Datenschützer erhoffen sich von einer Regierungsbeteiligung der FDP Verbesserungen bei den Bürgerrechten. Diese Hoffnungen werden genährt, als Sabine Leutheusser-Schnarrenberger – profilierte Bürgerrechtlerin an der Seite von Gerhart Baum und Burkhard Hirsch – das Justizministerium übertragen wird. Die Koalitionsvereinbarungen enthalten aber viele nur scheinbare Verbesserungen, die bei genauer Betrachtung lediglich den Status Quo festschreiben (Quellen: Zeit, Spiegel, Heise, netzpolitik.org).

28. September 2009: Die chinesischen Behörden beginnen, Knoten des Anonymisierungsdienstes Tor zu blockieren. Am darauffolgenden Tag erklärt die Vereinigung „Reporter ohne Grenzen", dass das Internet in China zunehmend zensiert werde (Quelle: Heise).

Oktober 2009

5. Oktober 2009: In der New York Times wird über Vermutungen berichtet, dass die olympischen Sommerspiele 2016 unter anderem wegen der rigiden Grenzkontrollen in den USA nicht an Chicago vergeben wurden (Quelle: New York Times, netzpolitik.org).

10. Oktober 2009: Das Rumänische Verfassungsgericht hat die Umsetzung der Vorratsdatenspeicherung in Rumänien für verfassungswidrig erklärt. Nur auf eine richterliche Anordnung hin und unter staatsanwaltlicher Aufsicht sei die Speicherung von Daten zulässig (Quellen: Heise, netzpolitik.org).

10. Oktober 2009: Bundesinnenminister Schäuble fordert mehr Reglementierung des Internet und verstärkten Einsatz von Videokameras. Videokameras seien sinnvoll, wenn weniger soziale Kontrolle zu einem geringeren Schutz führe. Auch das Internet solle stärker regelmentiert werden. Er räumte gleichzeitig ein, dass die Idee für das Zugangserschwerungsgesetz – die Einführung von Internet-Sperren – im Wahlkampf entstanden sei (Quelle: Heise).

15. Oktober 2009: Widerstand des EU-Parlaments gegen Internet-Sperren bei Urheberrechtsverletzungen nimmt ab. Ein neuer

Vorschlag soll den Änderungsantrag 138 ersetzen. Mit dem Änderungsantrag hatten sich die Abgeordneten dafür ausgesprochen, dass Eingriffe in die Grundrechte der Nutzer – wie das Sperren von Internetverbindungen – nur per Gerichtsentscheidung möglich sind (Quelle: Heise).

15. Oktober 2009: Das Bundeskriminalamt hat seit der Novelle des BKA-Gesetzes noch keine Online-Durchsuchung durchgeführt. Dies teilte ein Sprecher auf Anfrage der taz mit. Gegen das Gesetz hat der frühere Bundesinnenminister Gerhart Baum eine Verfassungsbeschwerde angestrengt (Quellen: taz, Heise).

16. Oktober 2009: Dem NDR sind ca. 27.000 Datensätze des Finanzdienstleisters AWD mit Personendaten und Angaben zu ca. 60.000 Verträgen zugespielt worden. Die Daten enthalten Abschlussdatum der Verträge, Laufzeit und die vom Kunden zu zahlenden Beträge (Quellen: NDR, netzpolitik.org).

16. Oktober 2009: Auf gemischte Reaktionen treffen die Koalitionsabsprachen zur Innenpolitik. Insbesondere die Festlegungen zu Bürgerrechten gehen kaum über die ohnehin garantierten Rechte hinaus. So wird beispielsweise der Zugriff der Bundesbehörden auf die gespeicherten Vorratsdaten der Telekommunikationsunternehmen bis zur Entscheidung des Bundesverfassungsgerichts ausgesetzt und bis dahin auf Zugriffe zur Abwehr einer konkreten Gefahr für Leib, Leben und Freiheit beschränkt – eine ohnehin vom Bundesverfassungsgericht im wesentlichen bereits vorgegebene Einschränkung (Quellen: Heise, netzpolitik.org).

16. Oktober 2009: Die BigBrotherAwards 2009 wurden im Rahmen eines Festakts in Bielefeld verliehen. Der scheidende Bundesinnenminister Wolfgang Schäuble wurde für sein Lebenswerk ausgezeichnet; Familienministerin Ursula von der Leyen erhielt einen Preis für Ihre Pläne zur Internet-Zensur (Quellen: Heise, netzpolitik.org).

17. Oktober 2009: Bei dem sozialen Netzwerk SchülerVZ werden über 1 Million Datensätze von Nutzern ausgelesen. Die Daten wurde dem Blog netzpolitik.org zugespielt. Ein unter dem Vorwurf der Erpressung verhafteter Mann begeht später in der Untersuchungshaft Selbstmord; der gegen ihn erhobene Vorwurf wird verschiedentlich angezweifelt. Der Fall offenbart erhebliche Sicherheitslücken bei SchülerVZ (Quellen: Zeit, Heise, netzpolitik.org).

20. Oktober 2009: Gegen die Deutsche Bahn AG wird wegen schwerwiegenden Verstößen gegen das Datenschutzrecht eine Bußgeld in Höhe von €1,1 Millionen verhängt – das bisher höchste Bußgeld wegen Datenschutzverstößen. Die Bahn akzeptiert den Bußgeldbescheid. Unter anderem hatte sie per Rasterfahndung verdachtsunabhängig nach Fällen von Korruption gesucht (Quelle: Heise).

24. Oktober 2009: Zentraler Server beim irischen Ableger von Lidl war zeitweise offen zugänglich. Dabei waren vertrauliche Daten öffentlich einsehbar. Darunter waren Umsatzzahlen, Einkaufsplanungen, Krankmeldungen oder Abmahnungen von Beschäftigten. Lidl war bereits zuvor wegen Datenschutzverstößen aufgefallen (Quellen: Spiegel, Heise).

26. Oktober 2009: Nach einem Bericht der Stiftung Warentest gewährt die Postbank freien Beratern Zugriff auf die Girokontendaten ihrer Kunden. Dabei hätten ca. 4.000 Berater Einsicht in alle Kontobewegungen der Kunden gehabt. Nach den Berichten sperrt die Postbank den Zugriff auf die Daten (Quellen: Heise, netzpolitik.org).

27. Oktober 2009: Einbrecher in die Online-Stellenbörse der britischen Tageszeitung „Guardian" haben sich Zugriff auf ca. eine halbe Million Datensätze von Bewerbern einschließlich deren Lebensläufe verschafft (Quelle: Heise).

28. Oktober 2009: Der Daimler-Konzern verlange Bluttest von seinen Stellenbewerbern, so berichtet NDR Info. Bei Arbeitsrechtlern stößt dieses Vorgehen auf scharfe Kritik, da damit in das Persönlichkeitsrecht eingegriffen werde. Obwohl es nicht zulässig ist, Bewerber zu Gesundheitstests zu zwingen, können sie sich kaum entziehen, ohne mit dem Ausschluss aus dem Bewerbungsverfahren rechnen zu müssen (Quellen: NDR, taz).

29. Oktober 2009: Bei der Online-Buchhandlung Libri.de war es möglich, online Rechnungen von Kunden einzusehen. Dazu reichte es aus, bei der URL in der Adresszeile des Browsers eine variierende Rechnungsnummer einzugeben (Quellen: Heise, netzpolitik.org).

30. Oktober 2009: Bei der englischen Rural Payments Agency wurden zwei Backup-Speicher verloren, auf denen sich Kontodaten von ca. 100.000 britischen Landwirten befanden (Quellen: Farmers Weekly, netzpolitik.org).

November 2009

3. November 2009: Kunden des Deutschen Sparkassenverlags konnten die Rechnungen anderer Kunden einsehen. Durch Ändern einer ID konnten angemeldete Nutzer sich die Rechnungen anzeigen lassen. Dadurch konnte auf fast 350.000 Rechnungen zugegriffen werden (Quellen: Zeit, Heise, netzpolitik.org).

4. November 2009: Beschäftigte des Norddeutschen Rundfunks (NDR) berichten, dass sie sich im Bewerbungsverfahren einem Bluttest hätten unterziehen müssen. Der NDR hat das bestätigt. Nur wenige Tage zuvor hatte der NDR seinerseits Bluttests bei Daimler angeprangert (Quellen: taz, netzpolitik.org).

4. November 2009: Das insolvente Versandhaus Quelle hat angekündigt, im Rahmen der Geschäftsauflösung möglicherweise auch die Kundendaten zu verkaufen, sofern kein Widerrufsvermerk vorliege. Dabei solle das Listenprivileg zur Anwendung kommen. Laut Bundesverband der Verbraucherzentralen ist die Anwendung des Listenprivilegs im Insolvenzfall ausgeschlossen; der Verband forderte den Konkursverwalter von Quelle auf, alle Kundendaten nach der Abwicklung der Vertragsbeziehungen zu löschen (Quellen: Süddeutsche Zeitung, netzpolitik.org).

11. November 2009: Eine Berliner Firma hat missbräuchlich auf Daten aus Systemen der Bundesagentur für Arbeit zugegriffen. Dazu wurden ca. 2.500 fingierte Stellenangebote eingestellt. Die Bundesagentur betonte, dass es sich um Einzelfälle gehandelt habe; ca. 3.000 von 200.000 Angeboten seien unseriös gewesen. Der Bundesdatenschutzbeauftragte Peter Schaar hatte zuvor datenschutzrechtliche Bedenken bei einzelnen Systemen geäußert (Quellen: Speigel, Heise).

Schwerpunkt: Herausforderungen

Niels Lepperhoff, Björn Petersdorf

Nur ein Vollzugsdefizit? – Parteien vernachlässigen den Datenschutz

Das Thema Datenschutz klettert immer weiter nach oben auf der Agenda der Politik in Deutschland. In den Wahlprogrammen der Parteien zur Bundestagswahl 2009 wird „Datenschutz mit Augenmaß"[1] verlangt und dass der Bürger darauf vertrauen können muss, „dass seine Daten vor Missbrauch geschützt sind."[2] Die Grünen verlangen sogar die Verankerung des Datenschutzes als Bürgerrecht im Grundgesetz.[3]

Die Autoren der Studie „Parteien und Datenschutz - Datenschutzpraxis deutscher Parteien und parteinaher Organisationen" nahmen die Bundestagswahl 2009 zum Anlass, um zu untersuchen, wie die Parteien selbst mit dem Datenschutz umgehen. Analysiert wurden u. a. die Verfahren bei Online-Spenden oder das Vorhandensein eines datenschutzrechtlich vorgeschriebenen Verfahrensverzeichnisses. Das Ergebnis der Studie besagt, dass keine der im Deutschen Bundestag vertretenen Parteien beim Thema Datenschutz uneingeschränkt gesetzeskonform handelt. Insgesamt wurden rund ein Drittel der messbaren Verstöße von Parteien und deren verwandten Organisationen auch begangen und somit entsprechende gesetzliche Vorschriften missachtet.

Einleitung: Parteien und Datenschutz

Meldungen über Datenschutzverstöße gehören heute schon zur Tagesordnung. Der besorgte Bürger fragt sich zu Recht, was mit seinen persönlichen Daten geschieht, die er Unternehmen, Behörden oder Krankenkassen mitteilt und wie er sich gegen den potenziellen Missbrauch schützen kann. Die Rufe nach durchgreifenden politischen Maßnahmen und entsprechender Gesetzgebung werden ebenso lauter, wie die nach geeigneten Kontrollmechanismen und Sanktionen für die Gesetzesbrecher.

Parteien formen den Datenschutz in Deutschland maßgeblich, weshalb der Umgang der Parteien mit dem Datenschutz als ein Indikator für das Datenschutzniveau in Deutschland gesehen werden kann. Die Autoren untersuchten in der Studie „Parteien und Datenschutz – Datenschutzpraxis deutscher Parteien und parteinaher Organisationen", wie ernst die Parteien den Datenschutz in der Praxis nehmen.[4] Insgesamt untersuchten die Autoren drei Aspekte:

1. Die Abwicklung von Online-Spenden: Welche Möglichen bieten Parteien, online zu spenden? Wie sicher sind diese Verfahren?

2. Den Umgang mit personenbezogenen Daten im Internet: Wie legen Parteien ihren Besuchern offen, welche Daten erhoben werden und was mit diesen geschieht?

3. Das Vorhandensein von Grundlage für datenschutzkonformes Handeln: Verfügen die Parteien über ein Verfahrensverzeichnis?

Der folgende Text stellt eine gekürzte Fassung der Studie dar.

Parteien prägen das Datenschutzniveau in Deutschland

Der Einfluss von Parteien auf den Datenschutz in Deutschland ist groß: Abgeordnete des Bundestags und der Landtage gehören fast ausnahmslos einer Partei an und sind damit auch der Partei- und Fraktionsdisziplin unterworfen. Sowohl Bundestag als auch Landtage erlassen – vereinfacht dargestellt – Gesetze mit Datenschutzbezug. Diese Gesetze bestimmen das Datenschutzniveau, das der Gesetzgeber wünscht.

Um den Datenschutzgesetzen Nachdruck zu verleihen, überwachen Aufsichtsbehörden die Ministerien, Gemeinden, Unternehmen, Vereine und natürlich auch die Parteien. Die Ausstattung der Aufsichtsbehörden legen Bundestag und Landtage durch die Mittelausstattung fest. Je geringer diese ausfällt, desto weniger Kontrollen der Gesetze sind faktisch möglich. Viele Gesetzesverstöße bleiben so ungeahndet.

Die Einflussnahme der Parteien ist noch unmittelbarer, denn der Bundesdatenschutzbeauftragte und die Landesdatenschutzbeauftragten werden auf Zeit von den zuständigen Parlamenten gewählt. Als Leiter der jeweiligen Aufsichtsbehörde sind sie für die Datenschutzkontrolle von Ministerien, Behörden und anderen öffentlichen Einrichtungen verantwortlich. In einigen Bundesländern kontrollieren die Landesdatenschutzbeauftragten auch nicht-öffentliche Stellen, wie Parteien, privatwirtschaftliche Unternehmen und Vereine.[5]

Über ihre Abgeordneten bestimmen Parteien also einerseits die Datenschutzgesetzgebung mit und legen andererseits das Kontrollniveau der Aufsichtsbehörden fest.

Untersuchte Parteien und Stiftungen

Um den Umgang von Parteien mit dem Datenschutz zu untersuchen, betrachteten die Autoren verschiedene Parteiorganisationen und bekannte parteinahe Stiftungen. Parteien sind mit Stiftungen und anderen parteinahen Organisationen durch vielfältige personelle Verflechtungen verbunden und profitieren von deren Arbeit. Neben der Bundesebene untersuchten die Autoren auch die Landesverbände von Brandenburg, Nordrhein-Westfalen, Saarland, Sachsen und Thüringen. Parteinahe Organisationen, wie die „Mittelstands- und Wirtschaftsvereinigung der CDU/CSU", die von zwei Parteien getragen werden, rechneten wir der größeren Partei zu.

Spenden sammeln im Internet

Online-Spenden stellten im Bundestagswahlkampf 2009 eine wichtige Säule in den Online-Auftritten der Parteien dar. Die Autoren untersuchten die Online-Spendenmöglichkeit der sechs wichtigsten Bundesparteien im August 2009. Einige Befunde können heute nicht mehr nachvollzogen werden, da die betreffenden Seiten zum Teil aufgrund der öffentlichen Berichterstattung über die Studie verändert oder abgeschaltet worden sind. Gleichwohl wollen wir an dieser Stelle die damaligen Ergebnisse dokumentieren.

Neben reinen Geldspenden boten Parteien an, Plakate für sie zu spenden. Hierbei bezahlt der Spender dafür, dass ein Plakat für eine gewählte Zeitspanne an einem, i. d. R. vom Spender gewünschten, Ort aufgestellt wird.

Online-Spenden setzen voraus, dass sensible Daten, wie Kontonummern oder Kreditkartennummern, im Internet übertragen werden. Für die Erstellung der Spendenquittung sind außerdem die Daten des Spenders notwendig. Deshalb eignen sich Online-Spenden gut, um zu untersuchen, wie verantwortungsvoll Parteien mit den ihnen anvertrauten Daten umgehen.

Bei der Analyse wurden die Bundesebene der sechs großen Parteien – CDU, CSU, Die Linke, FDP, Grüne und SPD – sowie deren Angebot, online zu spenden, betrachtet. Drei Parteien offerieren die Bezahlung mit Kreditkarte, vier durch Lastschrifteinzug und drei durch den Bezahldienst PayPal.

Partei	Kreditkarte	Lastschrift	PayPal
SPD	✓	✓	
CDU	✓		
CSU			✓
FDP	✓	✓	✓
Die Grünen		✓	
Die Linke		✓	✓
Gesamt	**3**	**4**	**3**

Tabelle 1: Möglichkeiten online zu spenden[6]

Die drei Bezahlmethoden unterscheiden sich danach, wie viele Dritt-Unternehmen mit der Abwicklung beauftragt werden (Abbildung 1). Eine Erlaubnis zum Lastschrifteinzug übermittelt die Partei oder ihr technischer Dienstleister direkt an die Bank des Spenders zur Ausführung. Sowohl bei Kreditkartenzahlungen wie auch bei PayPal wird ein weiteres Unternehmen einbezogen. Wer sein PayPal-Konto mittels Kreditkarte ausgleicht, bezieht sogar zwei Unternehmen mit ein. Zahlungen via PayPal werden immer über die USA abgewickelt. Dies kann – je nach Unternehmen – auch bei Kreditkartenzahlungen der Fall sein. Damit können US-Behörden Einblick in Spenden an deutsche Parteien erhalten. PayPal ist eine Tochter von eBay. Wer mit PayPal zahlt, vertraut seine Daten letztlich eBay an. Keine der

Stefan Hügel

Mangelnde Durchsetzung des Datenschutzes

Auch an den Universitäten Karlsruhe und Regensburg wurde im Rahmen einer Studie untersucht, in welchem Umfang gesetzliche Datenschutzbestimmungen auf Internetportalen eingehalten werden. Dazu wurden 100 Portale unter rechtlichen Gesichtspunkten untersucht. Ausgewählt wurden Portale mit hohem Marktanteil und einer breiten Auswahl von angebotenen Dienstleistungen von sozialen Netzen bis zu Webshops. Alle Portale werden unter deutschem Recht betrieben.

Bei der Untersuchung wurden Kriterien zugrundegelegt, die auf Bestimmungen des Telemediengesetzes zurückgehen:

- Auffindbarkeit und Informationsgehalt der Datenschutzrichtlinie,
- Abfrage des Einverständnisses zu Datennutzung,
- Auskunft über die verarbeiteten Daten,
- Löschung der Daten.

Obwohl die Studie auf deutschem Recht basiert, kann sie auf alle EU-Staaten übertragen werden, da dort die EU-Richtline 95/46/EC gilt, die analoge Bestimmungen enthält.

Alle diese Kriterien wurden unter mehreren Aspekten untersucht. Dabei wurde in vielen Fällen festgestellt, dass Webportale die gesetzlichen Anforderungen an den Datenschutz nicht ausreichend erfüllen. Datenschutzrichtlinien sind lükkenhaft oder unpräzise, die Genehmigung zur Verarbeitung schutzwürdiger Daten wird nicht eingeholt. Auskunft zu gespeicherten Daten wird zwar häufig schnell erteilt, ist aber ebenfalls unvollständig.

Im Ergebnis stellt die Studie fest, dass die gesetzlichen Bestimmungen des Datenschutzes nur unzureichend durchgesetzt werden.

Literatur

Thorben Burghardt, Klemens Böhm, Erik Buchmann, Jürgen Kühling, Anastasios Sivridis (2009): A Study on the Lack of Enforcement of Data Protection Acts, Universität Karlsruhe und Universität Regensburg, http://dbis.ipd.uni-karlsruhe.de/download/bu09edemocracy.pdf

untersuchten Parteien wies bei der Bezahlung mittels PayPal auf die Datenübermittlung in die USA hin.

Solange eine Partei mehrere Möglichkeiten der Bezahlung anbietet, hat ein Online-Spender eine Wahlmöglichkeit gemäß seiner Datenschutzinteressen. Vorausgesetzt, er kennt und versteht die genannten Zahlungswege. Die CSU bietet durch die Beschränkung auf PayPal keine Auswahlmöglichkeit bei der Online-Spende an.

Nur CDU und Grüne handeln beim Übertragen der Daten im Internet vorbildlich

Die Grünen und die CDU handeln vorbildlich, indem sie verschlüsseln und dem Spender mit Hilfe eines erweiterten Zertifikats anzeigen, dass die Webpräsenz authentisch ist. Die FDP und Die Linke verschlüsseln zwar, verzichten aber auf eine Authentizitätsanzeige. Darüber hinaus übertrug Die Linke zum Zeitpunkt der Untersuchung Daten für Plakatspenden unverschlüsselt und gefährdete so ihre Spender. Durch die Berichterstattung über unsere Studie schaltete die Partei die Plakatspendemöglichkeit ab.[7] Die CSU überlässt die Absicherung PayPal.

Die SPD verspricht ihren Spendern eine Sicherung nach dem „neuesten technischen Stand“[8], was eine SSL-verschlüsselte Datenübertragung wäre. Diese scheint aber nicht aufgebaut zu werden. Tatsächlich aber werden die Daten, für den Spender unsichtbar, verschlüsselt übermittelt, jedoch nicht an die SPD. Die SPD wickelt die Spendenzahlung über einen externen Dienstleister ab, ohne dessen Identität offenzulegen. Deshalb bindet sie die Webseiten des Dienstleisters per „iFrame“ ein. Ein Spender merkt deshalb nicht, dass seine Finanzdaten gar nicht an die SPD übermittelt werden, sondern an die „infin – Ingenieurgesellschaft für Informationstechnologien mbH & Co. KG“. Diese Technik wird auch von Kriminellen eingesetzt, um Finanzdaten auszuspähen, während der Besucher glaubt, auf der Webseite seiner Bank zu sein.

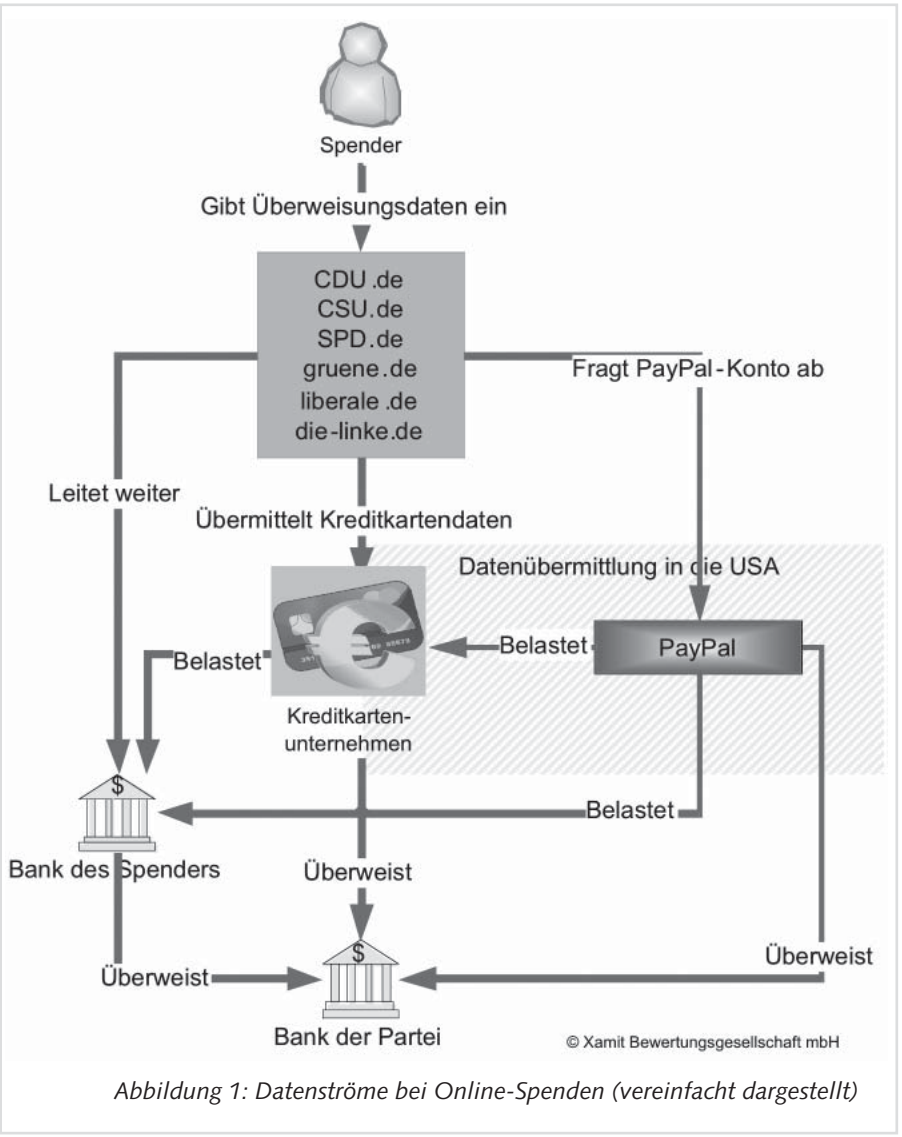


Abbildung 1: Datenströme bei Online-Spenden (vereinfacht dargestellt)

Datenschutz im Internet: Webstatistiken und Nutzerhinweis

Eine maschinelle Quellcode-Analyse der Webpräsenzen von Parteien und parteinahen Organisationen im August 2009 bildete die Grundlage, um den Umgang mit personenbezogenen Daten im Internet zu untersuchen. Analysiert wurden jeweils maximal 1.000 Webseiten pro Webpräsenz. Hierbei wurde untersucht,

- ob und welche Webstatistiken erstellt werden und
- ob Kontaktformulare vorhanden sind.

In diesem Zusammenhang wurde auch das Vorhandensein von Datenschutzerklärungen geprüft. Welche Regelungen in einer Datenschutzerklärung enthalten waren, blieb aus methodischen Gründen unberücksichtigt.

Eine Erfolgskontrolle von Webseiten ist für wirtschaftlich arbeitende Organisationen und Unternehmen unverzichtbar. Mit Hilfe von Webstatistiken – auch Web Tracking, Web Analytics oder Webcontrolling genannt – messen Unternehmen das Verhalten ihrer Besucher. Entweder erstellt ein externer Dienstleister Webstatistiken oder der Webseitenbetreiber wertet das Verhalten der Besucher auf seinem Internetangebot intern aus.

Webstatistiken geben aggregierte Informationen über die Besucher von Webseiten wieder. Sie beantworten u.a. folgende Fragen:

- Über welche Wege betreten Besucher die Webpräsenz?
- Wie viele Besucher hat die Webpräsenz?
- Was unternehmen Besucher auf der Webpräsenz?

Jeder Statistik-Ersteller bindet eine charakteristische Zeichenfolge in die überwachten Webseiten ein, um den Seitenaufruf protokollieren zu können. Aus methodischen Gründen wurden lediglich diejenigen Statistikersteller berücksichtigt, die eine eigene Datenerhebung durchführen.

In früheren Untersuchungen hatten die Autoren Google Analytics bereits als Marktführer identifiziert.[9] In seiner Stellung-

nahme vom Januar 2009 wertet das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) den Einsatz von Google Analytics in Deutschland jedoch als nicht mit dem deutschen Datenschutzrecht vereinbar. Laut ULD ist die Nutzung von Google Analytics auf deutschen Webpräsenzen also illegal. Zu den Gründen zählen

- die Datenübermittlung in die USA,
- die ewige Datenspeicherung ohne Löschmöglichkeit und
- die Möglichkeit, durch Datenverknüpfung ein Nutzerprofil zu erstellen.10

Google verlangt in § 8.1 seiner Nutzungsbedingungen[11], die Nutzung von Google Analytics an „prominenter" Stelle des Webauftritts zu dokumentieren. Google legt den Wortlaut dieser Information fest und behält sich auch ein Kontrollrecht vor. Ob die von Google vertraglich vorgeschriebenen Formulierungen auf einer Webpräsenz, die Google Analytics nutzt, vorkommen, untersuchten die Autoren ebenfalls.

Bis auf Die Linke nutzen Bundesparteien einen identifizierbaren Webstatistikanbieter (siehe Abbildung 2). Bei Landesparteien und parteinahen Vereinigungen konnte nur bei jeweils einer Webpräsenz ein Webstatistikanbieter identifiziert werden. 27% der Stiftungen verwenden Google Analytics und 9% einen anderen Anbieter.

10% der untersuchten Webpräsenzen von Parteien und parteinahen Organisationen nutzen Google Analytics und 13% einen anderen Anbieter. Alle untersuchten und der CSU zugerechneten Webseiten nutzen Google Analytics (Abbildung 3).

Bis auf eine der CDU zugerechneten Webpräsenz besitzen alle übrigen Webpräsenzen mit Webstatistik eine Datenschutzerklärung.

Zwei Webpräsenzen verstoßen gegen die Nutzungslizenz von Google Analytics

Jeweils eine Webpräsenz mit Google Analytics, die der CDU und der CSU zugerechnet wurde, verzichtet auf den vorgeschriebenen Passus aus der Lizenzvereinbarung mit Google. Dies ist ein klarer Verstoß gegen die Nutzungslizenz.

Hier zeigt sich ein klarer Trend: auf Bundesebene sind Webstatistiken stark verbreitet, während die Nutzung auf Landesebene stark abnimmt.

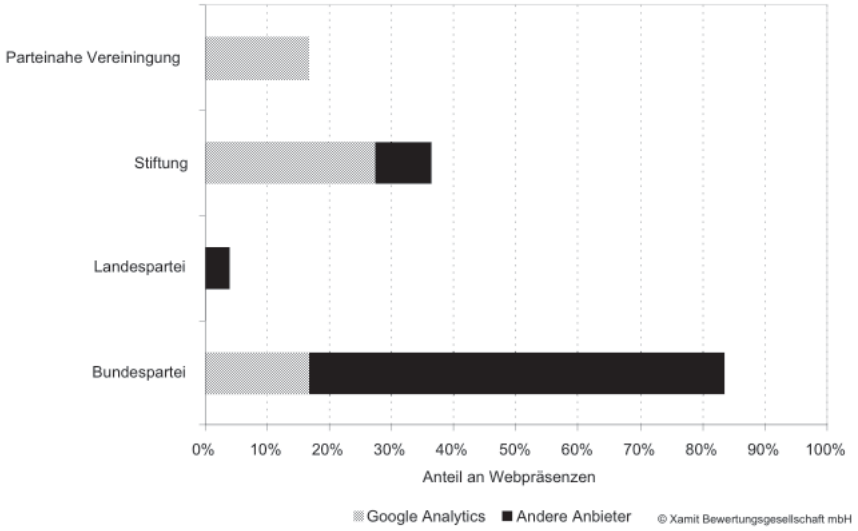


Abbildung 2: Nutzung von Webstatistiken nach Organisationen

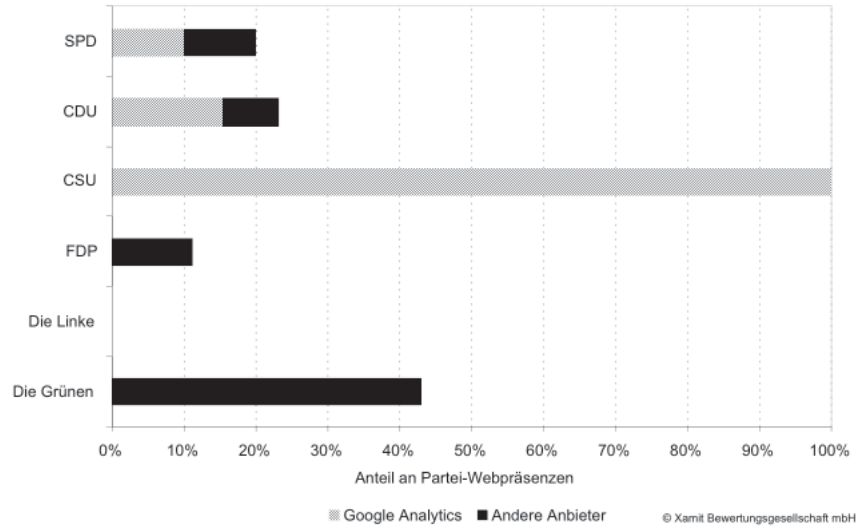


Abbildung 3: Nutzung von Webstatistiken nach Parteien

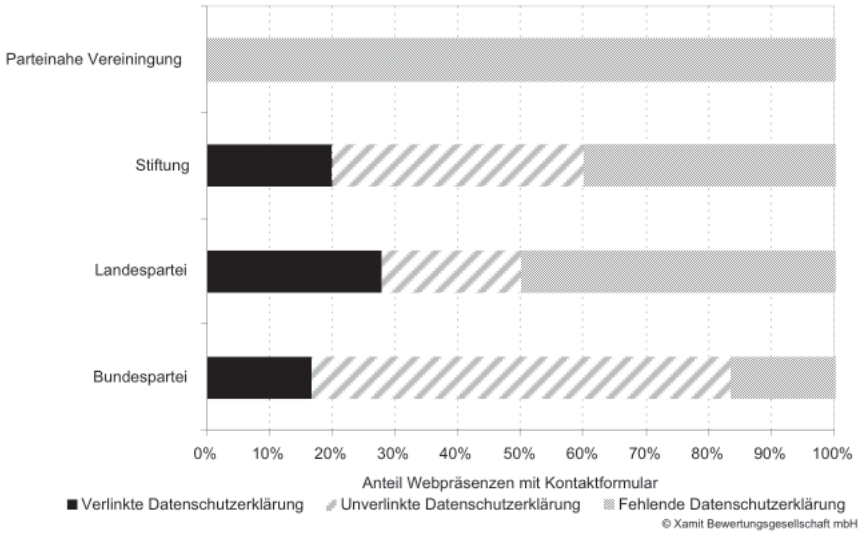


Abbildung 4: Nutzung von Kontaktformularen nach Organisationen

Einbindung von Kontaktformularen: Viele Besucher werden über die Verwendung ihrer Daten nicht informiert

Für jede Webpräsenz wurde untersucht,

- ob Eingabefelder personenbezogene Daten abfragen, z. B. bei Kontaktformularen,
- ob eine Datenschutzerklärung auf der Webpräsenz vorliegt,
- ob die Datenschutzerklärung einfach und mit maximal einem Klick vom Formular aus direkt erreichbar ist.

Lediglich die Bundes-SPD gibt keine Datenschutzerklärung zu ihrem Kontaktformular an (Abbildung 4). Parteinahe Vereinigungen nutzen generell Kontaktformulare ohne Datenschutzerklärung. D.h. sie erläutern Besuchern, die das Kontaktformular verwenden, nicht, wie die erhaltenen Daten verwendet werden.

Insgesamt verfügen 81% der untersuchten Webpräsenzen über ein Kontaktformular oder eine Bestellmöglichkeit für einen E-Mail-Newsletter. 21% der Webpräsenzen mit Kontaktformular verlinken direkt auf die Datenschutzerklärung, weitere 31% verfügen über eine nicht direkt erreichbare Datenschutzerklärung. Die restlichen 49% nutzen das Kontaktformular ohne Datenschutzerklärung. Die Grünen und die CSU sind die einzigen Parteien, die vorbildlich bei Kontaktformularen immer auch eine Datenschutzerklärung vorweisen (Abbildung 5).

Zentrum des Datenschutzes: das Verfahrensverzeichnis

Die Kontrolle des Datenschutzes wird durch drei miteinander verbundene Zentren wahrgenommen: Eigenkontrolle, Fremdkontrolle und Selbstkontrolle.

Die Eigenkontrolle verpflichtet die verantwortlichen Stellen zu größtmöglicher Transparenz bei der Datenverarbeitung. Sie schreibt vor, dass Betroffene, wie z.B. Interessierte oder Mitglieder, darüber informiert werden sollen, welche Daten über sie zu welchem Zweck verarbeitet werden.

Die Fremdkontrolle bildet das zweite Kontrollzentrum: Staatliche Aufsichtsbehörden kontrollieren, ob Daten ordnungsgemäß verarbeitet werden. Sie gehen auch Beschwerden von betroffenen Bürgern nach.

Die Selbstkontrolle verpflichtet Unternehmen, Parteien und andere Organisationen, das eigene Handeln auf Datenschutzkonformität hin zu kontrollieren. Das BDSG sieht als betriebliche Kontrollinstanz den betrieblichen Datenschutzbeauftragten[12] oder die Geschäftsleitung vor. Als Arbeitsgrundlage dient ein Verfahrensverzeichnis. Das Verfahrensverzeichnis beschreibt

- den Zweck der Datenverarbeitung,
- die Rechtsgrundlage,
- wer die Daten verarbeitet,
- welche Daten verarbeitet werden,
- von wem Daten verarbeitet werden und
- wohin die Daten übermittelt werden.

Das Verfahrensverzeichnis dient als Arbeitsgrundlage der Selbstkontrolle

Der Gesetzgeber sieht mit dem Verfahrensverzeichnis ein zentrales Arbeitswerkzeug vor, um Datenschutzrechte sicherzustellen und ihre Einhaltung zu kontrollieren. Das Verfahrensverzeichnis gibt es in zwei Versionen (vgl. § 4e BDSG): Im öffentlichen Verfahrensverzeichnis stehen allgemeine Informationen darüber, welche Daten zu welchen Zwecken verarbeitet werden. Dieses muss jedermann auf Verlangen zugänglich gemacht (§ 4g Abs. 2 S. 2 BDSG). Das interne Verfahrensverzeichnis enthält sensible Informationen, wie z.B. IT-Sicherheitsmaßnahmen, und braucht außer an die Aufsichtsbehörde an niemanden herausgegeben zu werden.

Ohne ein Verfahrensverzeichnis fehlt einem Unternehmen oder einer Partei der Überblick, welche personenbezogenen Daten verarbeitet werden. In der Folge wird die Selbstkontrolle unmöglich. Auskunftsersuchen können nur schwer beantwortet werden und Datenschutzverstöße werden so erleichtert.

Niels Lepperhoff und Björn Petersdorf

Dr. **Niels Lepperhoff** ist Geschäftsführer und Mitgründer der Xamit Bewertungsgesellschaft mbH, Düsseldorf, sowie TÜV-geprüfter Datenschutzbeauftragter. Als Datenschutz- und IT-Sicherheitsexperte unterstützt er Unternehmen und andere Organisationen z.B. als externer betrieblicher Datenschutzbeauftragter oder bei der Erstellung und Umsetzung von Datenschutzkonzepten. Er war mehrere Jahre als Wissenschaftler und Politikberater tätig und veröffentlichte wissenschaftliche Bücher, Artikel und Studien zu Aspekten der Sicherheitspolitik, des Datenschutzes und IT-Sicherheit.

Björn Petersdorf ist Geschäftsführer und Mitgründer der Xamit Bewertungsgesellschaft mbH, Düsseldorf. Als externer IT-Sicherheitsbeauftragter ist er in vielfältigen Branchen tätig und berät Unternehmen seit über zehn Jahren zu Sicherheits- und Datenschutzfragen. Hierzu gehört u.a. die Prüfung existierender Schutzmaßnahmen. Er veröffentlichte zahlreiche Studien, u.a. zu den Themen Web Tracking, Datenschutz und Datensicherheit.

Nur ein Viertel der Befragten schickte ein Verfahrensverzeichnis

Im Zuge der Untersuchung hat eine Testperson per E-Mail an die im Impressum auf der Webseite angegebene Adresse bei jeder Partei, Stiftung oder parteinahen Vereinigung um die Zusendung des öffentlichen Verfahrensverzeichnisses gebeten. Die Zusendung konnte elektronisch oder postalisch erfolgen.

Zwei Bundesparteien reagierten auf die Anfrage nach einem Verfahrensverzeichnis überhaupt nicht (Abbildung 6). 36% der Stiftungen reagierten ebenfalls nicht.

9% der Stiftungen stellten eine Rückfrage, 18% verstanden die Anfrage nicht. Lediglich 16% der Landesparteien schickten ein Verfahrensverzeichnis zu. Parteinahe Vereinigungen sandten entweder keines zu oder boten eine andere Möglichkeit zur Kenntnisnahme an. Insgesamt stellten nur 25% der angeschriebenen Institutionen ein Verfahrensverzeichnis zur Verfügung.

Weitere 25% der angeschriebenen Organisationen hatten die Frage nicht verstanden oder ausweichend reagiert.

4% hatten Rückfragen und wollten eine Begründung für das Interesse, obwohl für die Zusendung des öffentlichen Verfahrensverzeichnisses keine weiteren Angaben, wie z.B. ein Rechtsgrund, notwendig sind. Von diesen Organisationen haben die Autoren bis heute kein Verfahrensverzeichnis erhalten.

46% antworteten gar nicht. Zwei Parteien und die ihnen nahe stehenden Institutionen haben kein Verfahrensverzeichnis zugesandt (Abbildung 7).

Zusammengefasst wurde dem Recht auf Einsicht in das öffentliche Verfahrensverzeichnis von 75% der Parteien und parteinahen Organisationen nicht Genüge getan.

Häufige Irrtümer und Wissenslücken

Nachfolgend klären die Autoren die drei häufigsten Irrtümer und Fehlvorstellungen auf, die in den erhaltenen Antworten genannt wurden.

> *„… Wir sind die XXX (Landespartei) und keine datenverarbeitende Stelle im Sinne des Datenschutzgesetzes. …“*

Das BDSG gilt für alle nicht öffentlichen Stellen unabhängig von ihrer Größe und Aufgabe, d.h. auch für Parteien und die öffentlichen Stellen des Bundes. Für die öffentlichen Stellen der Län-

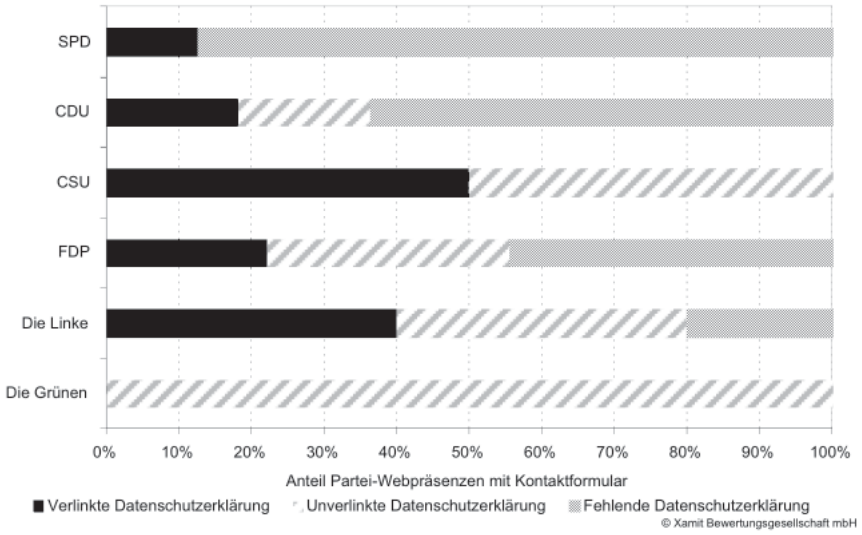


Abbildung 5: Nutzung von Kontaktformularen nach Parteien

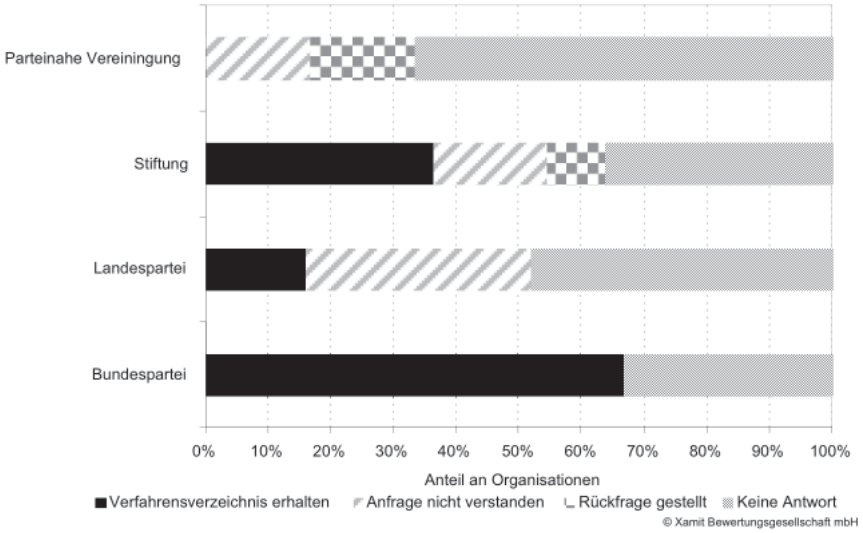


Abbildung 6: Reaktion auf Anfrage nach Verfahrensverzeichnis nach Organisationen

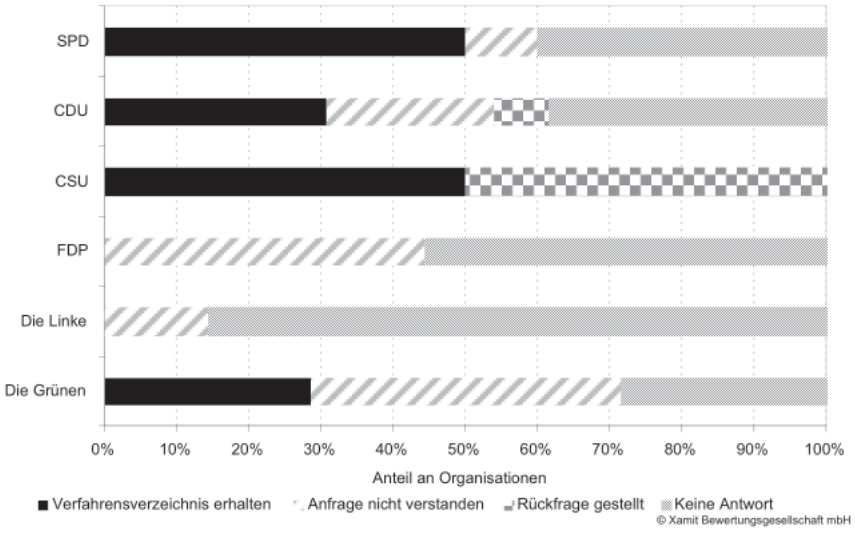


Abbildung 7: Reaktion auf Anfrage nach Verfahrensverzeichnis nach Parteien

der, z.B. Ministerien, gelten die Datenschutzgesetze der Länder. Einzig Familien fallen weder unter das BDSG noch unter die Datenschutzgesetze der Länder.

> *„… Nun ist XXX keine Gliederung, in der zehn oder mehr Menschen personenbezogene Daten einsehen oder bearbeiten können, deshalb haben wir leider auch kein Verfahrensverzeichnis. …"*

So einfach ist das nicht. Wenn kein Datenschutzbeauftragter bestellt werden muss, übernimmt die Geschäftsführung die entsprechenden Pflichten (§ 4g Abs. 2a BDSG):

> *„Soweit bei einer nichtöffentlichen Stelle keine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz besteht, hat der Leiter der nichtöffentlichen Stelle die Erfüllung der Aufgaben nach den Absätzen 1 und 2 in anderer Weise sicherzustellen."*

Zu den Pflichten zählt auch, ein Verfahrensverzeichnis, das in § 4e Satz 1 Nr. 1 bis 8 BDSG beschrieben ist, auf Antrag zur Verfügung zu stellen (§ 4g Abs. 2 S. 2 BDSG). Kurz: Die Unternehmensgröße schützt nicht vor datenschutzrechtlichen Verpflichtungen.[13]

> *„… Ihre Anfrage müssten Sie an den Datenschutzbeauftragten des Landes richten. …"*

Das ist nicht richtig. Jede verantwortliche Stelle, d.h. jede Partei oder jedes Unternehmen, muss ein Verfahrensverzeichnis pflegen (vgl. § 4g Abs. 2a BDSG). Der Datenschutzbeauftragte des Landes ist die zuständige Aufsichtsbehörde für die öffentlichen Stellen, wie z.B. Ministerien. Je nach Bundesland ist der Datenschutzbeauftragte des Landes auch für nicht-öffentliche Stellen, wie z.B. Unternehmen, verantwortlich. Zu seinen Aufgaben gehört zwar die Kontrolle, jedoch nicht die Pflege von Verfahrensverzeichnissen für Parteien und Unternehmen. Führt eine Partei oder ein Unternehmen kein Verfahrensverzeichnis, kann die Aufsichtsbehörde ein Bußgeld von bis zu 50.000 Euro verhängen.

Fazit

Parteien bestimmen mit, was erlaubt und was verboten ist und legen gleichzeitig die Kontrolldichte fest. Die Untersuchung des Umgangs der sechs großen Parteien mit Online-Spenden offenbarte jedoch eklatante Sicherheits- und Datenschutzmängel:

- Die CSU hat für Online-Spender ausschließlich die Nutzung von PayPal vorgesehen. Eine Übermittlung und Datenverarbeitung in den USA ist damit inbegriffen.
- Die FDP verzichtet auf erweitere SSL-Zertifikate, d.h. ein Spender kann nicht sicher sein, dass die angezeigte Webseite authentisch ist.
- Die Linke übertrug bis zur Berichterstattung sensible Finanzdaten, wie Kontonummern, bei Plakatspenden unverschlüsselt.
- Die SPD informiert ihre Spender nicht über den Empfänger der übermittelten Finanzdaten.

Darüber hinaus wurden folgende Praktiken festgestellt:

- Betrieb von Webstatistiken ohne Datenschutzerklärung,
- Einsatz von Google Analytics in Widerspruch zum BDSG und TMG,
- Kontaktformulare ohne Datenschutzerklärung und
- fehlende Verfahrensverzeichnisse.

Die 48 untersuchten Organisationen begingen zusammen 32% der möglichen Verstöße. Abbildung 8 zeigt, dass die Verstöße bei Bundesparteien mit 17% im Vergleich gering ausfallen. Landesparteien und Stiftungen begingen 30% bzw. 32% der möglichen Verstöße, parteinahe Vereinigungen sogar 54%.

Spitzenreiter bei den Verstößen unter den Parteien sind die Volksparteien CDU (37%), CSU (38%) sowie die FDP (36%),

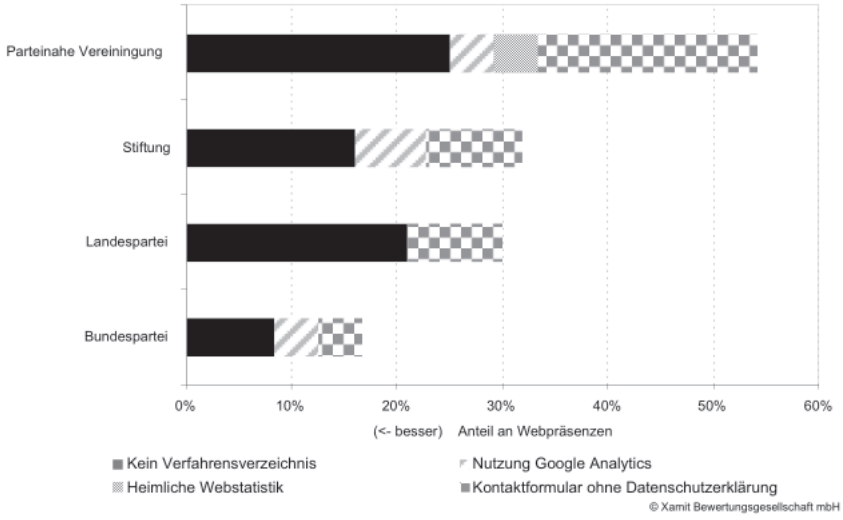


Abbildung 8: Anteil maximal möglicher Verstöße pro Organisation

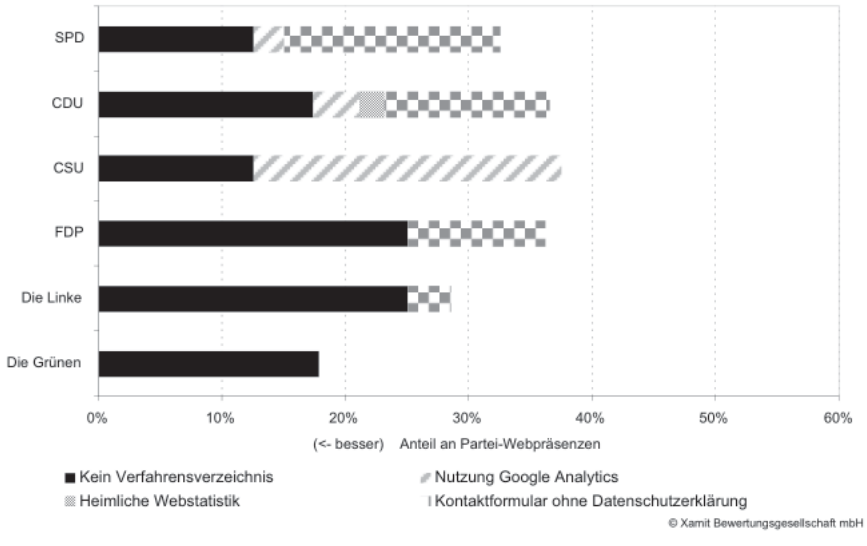


Abbildung 9: Anteil maximal möglicher Verstöße pro Partei

dicht gefolgt von der SPD (33%) (Abbildung 9). Die Linke kommen auf 29% und die Grünen auf 18% mögliche Gesetzesverstöße.

Insbesondere die Antworten auf die Fragen der Testperson enthüllten eine weitverbreitete Unkenntnis datenschutzrechtlicher Bestimmungen bei den Parteien. In etlichen Fällen war darüber hinaus eine deutliche Abwehrhaltung gegenüber legalen Auskunftsersuchen zu spüren. Es ist anzunehmen, dass diese beiden Faktoren zusammen den Nährboden für die zahlreichen und vielfältigen Datenschutzverstöße bildeten.

Endnoten

1 Bundesvorstand der CDU, Parteivorstand der CSU: Wir haben die Kraft – gemeinsam für unser Land. Regierungsprogramm 2009-2013. 28.06.2009, S. 81.

2 Ebd.

3 Bündnis90/Die Grünen: Der grüne Gesellschaftsvertrag. Klima, Arbeit, Gerechtigkeit, Freiheit. 8. -10.05.2009, S. 145.

4 Kostenfrei erhältlich unter http://www.xamit-leistungen.de/studienundtests/index.php.

5 Wenn Datenschutzbeauftragte zu engagiert die Datenschutzbelange von Bürgern vertreten, können sie dadurch ihre Wiederwahl gefährden: Vgl. die Debatte um die Wiederwahl von Dr. Thilo Weichest, Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) in Heise Online (2009): Debatte um Datenschutzposten in Schleswig Holstein. URL: http://www.heise.de/newsticker/meldung/print/135605. Letzter Zugriff: 2009-08-07.

6 Zeitpunkt der Erhebung 10. bis 17. August 2009 über die Webseiten der Parteien.

7 Siehe auch Zeit Online (2009): Studie: Parteien vernachlässigen Datenschutz. URL: http://www.zeit.de/newsticker/2009/9/2/iptc-bdt-20090902-610-22282128xml. Letzter Zugriff: 2009-10-26.

8 URL: http://www.spd.de/de/partei/mitmachen/onlinespenden/index.html. Letzter Zugriff: 2009-08-19.

9 Xamit (2008): Datenschutzbarometer 2008 - Datenschutz im Internet. URL: http://www.xamit-leistungen.de/studienundtests/index.php.

10 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (2009): Datenschutzrechtliche Bewertung des Einsatzes von Google Analytics. URL: https://www.datenschutzzentrum.de/tracking/20090123_GA_stellungnahme.pdf. Letzter Zugriff: 2009-08-05.

11 Google (2007): Google Analytics Bedingungen. URL: http://www.google.com/analytics/de-DE/tos.html. Stand: 2007-10-01.

12 Bei Organisationen, in denen mehr als neun Personen personenbezogene Daten automatisiert verarbeiten oder Einsicht in diese Daten haben, muss ein Datenschutzbeauftragter bestellt werden.

13 Hinweis: Der Artikel „Verfahrensverzeichnis“ auf Wikipedia mit Stand 2009-08-20 gibt den Sachverhalt falsch wieder. URL: http://de.wikipedia.org/wiki/Verfahrensverzeichnis.

Stefan Hügel

EDRi – European Digital Rights

Kurzbericht von der Generalversammlung

Bereits seit fünf Jahren ist das FIfF nun Mitglied bei EDRi – European Digital Rights. Die Vereinigung wurde 2002 mit dem Ziel gegründet, Bürgerrechte in der Informationsgesellschaft auf europäischer Ebene zu fördern und durchzusetzen. Mitglieder können Organisationen werden, die die Ziele von EDRi unterstützen. EDRi hat derzeit 27 Mitgliedsorganisationen aus 17 Ländern; 11 weitere Einzelpersonen – die als solche nicht Mitglied werden können – haben Beobachterstatus. Der immer für zwei Jahre gewählte Vorstand von EDRi besteht derzeit aus sechs Personen; Präsident ist Andreas Krisch vom Verein für Internet-Benutzer Österreichs (VIBE!AT). EDRi veröffentlicht alle zwei Wochen das EDRi-gram, einen Newsletter mit aktuellen Berichten aus dem Bereich der digitalen Bürgerrechte.

Die Generalversammlung 2009 von EDRi fand am 24./25. Oktober in Wien statt. Auf den ein- bis zweitägigen Generalversammlungen wird neben den formal notwendigen Entscheidungen über Vereinsinterna vor allem Entscheidungen über neue Mitglieder getroffen, von Seiten des Vorstands Bericht über die Aktivitäten des vergangenen Jahrs erstattet und die weitere Strategie von EDRi diskutiert.

In diesem Jahr wurden keine neue Mitglieder aufgenommen; drei Personen erhielten Beobachterstatus. Aktivitäten und Kampagnen von EDRi gibt es unter anderem zu den Themenbereichen:

- *Telekom-Paket einschließlich des Änderungsantrags 138*, der Eingriffe in die Rechte von Internet-Nutzern nur aufgrund einer Gerichtsentscheidung zulassen will; unter anderem wurde ein offener Brief an die Mitglieder des Europaparlaments gerichtet,

- *Freiwillige Vorratsdatenspeicherung im Rahmen des Telekom-Pakets*, die es Providern erlauben würde, eine fast unbegrenzte Menge an sensiblen Kommunikationsdaten zu speichern, bis hin zu den Seiten, die wir im Internet besuchen,

- *Prozessen bei WIPO, EuroDIG, ICANN und weiteren Strukturen* durch Mitarbeit in Arbeitsgruppen und Positionspapiere.

Zusätzlich ist EDRi an einer Reihe von Projekten im Umfeld der Bürgerrechte in der Informationsgesellschaft, wie Privatheit oder Zugang zu Wissen beteiligt. Dazu kommt eine Reihe von Aktivitäten der einzelnen Mitgliedsorganisationen.

Details finden sich auf der EDRi-Web-Seite (*http://www.edri.org*), die auch das EDRi-gram enthält. Eine deutsche Übersetzung des EDRi-grams gibt es bei (*http://unwatched.org*). Aktuelle Meldungen kann man auch über Twitter (*@EDRi_org*) abrufen.

Karin Schuler // Deutsche Vereinigung für Datenschutz e.V., Bonn

Und wenn man nicht mehr weiter weiß...

Der Spruch hat einen Bart. Er beschreibt ein beliebtes Delegationsverfahren: Selbst keine Ahnung – Arbeitskreis gründen – Verantwortung abschieben – Puh, nochmal gut gegangen! Die vermeintlich edlere Variante lässt sich im Koalitionsvertrag nachlesen: Zur Entwicklung eines Datenschutzaudits, zur Prüfung der Datenschutzfreundlichkeit von Produkten und Dienstleistungen und zur Beförderung der Datenschutzbildung beabsichtigt diese Koalition eine Stiftung Datenschutz zu gründen. Aha!
Dirk Fox, unter anderem Herausgeber der Zeitschrift „Datenschutz & Datensicherheit"[1] ätzte im Newsletter Secorvo Security News[2] seines eigenen Hauses „Soweit sind wir also schon gekommen: weil eigene ordnungspolitische Vorstellungen fehlen, wird das Primat der Politik an eine Stiftung delegiert."
Im Grunde kann einen diese Entwicklung nicht wirklich wundern. Seit Jahren beobachten engagierte Datenschützer die zunehmende Hilflosigkeit des Gesetzgebers, dem es nicht gelingt, zwischen Innerer Sicherheit und Persönlichkeitsrecht angemessen abzuwägen. Und ausgerechnet von einer Partei wie der FDP die Kehrtwende zu erwarten, die zwar den Bürgerrechtsschutz seit neuestem wieder demonstrativ vor sich her trägt, sich aber lieber nicht mit der Wirtschaft anlegt, wenn es um den Datenschutz von Beschäftigten geht, wäre doch wohl sehr naiv.
Aber welches sind eigentlich die Datenschutz-Herausforderungen, derer man sich annehmen müsste? Viele Wunschlisten vieler Organisationen haben sich über die Jahre angesammelt. Sie enthalten unzählige formale und inhaltliche Verbesserungsforderungen. Wo in der jetzigen Situation anfangen? Zur Erreichung eines gleichermaßen betroffenenorientierten und handhabbaren Datenschutzes scheinen mir einige Aspekte grundlegender als andere.

Flickenteppich Bundesdatenschutzgesetz

Seit Jahren schon ist in der Fachwelt unbestritten, dass das derzeitige Datenschutzrecht eine, mindestens formale, Zumutung darstellt. Das BDSG ist so wenig von interessierten Laien zu erfassen, dass von Normenklarheit, dem verfassungsrechtlichen Gebot für jegliche gesetzliche Regelung, keine Rede mehr sein kann. Vielmehr ist im Laufe der Jahre bei immer neuen Novellierungen ein Regelwerk zusammengestoppelt worden, dessen ursprüngliche Form 1977 noch zu Zeiten der Großrechner-IT entstand und 1990 an wesentliche verfassungsrechtliche Anforderungen angepasst wurde. Trotz vieler Absichtserklärungen hat es kein Gesetzgeber seitdem verstanden, eine grundlegende Modernisierung des Datenschutzrechts vorzunehmen.

Schon 2001 verfassten Alexander Roßnagel, Andreas Pfitzmann und Hansjürgen Garstka im Auftrag der damaligen Regierung ein Gutachten zur Modernisierung des Datenschutzrechts[3]. Es sollte eine grundlegende Novellierung vorbereiten, ist jedoch, wie so viele andere Schriften und Vorhaben, in der berühmten Schublade verschwunden.

Altlast Arbeitnehmerdatenschutzgesetz

In dieser liegt wohl seit wenigen Wochen auch der erste brauchbare Entwurf für ein Arbeitnehmerdatenschutzgesetz[4]. Warum der scheidende Arbeitsminister Olaf Scholz mit dessen Veröffentlichung bis wenige Wochen vor Ende der Legislaturperiode wartete, wird sein Geheimnis bleiben. Es wird gemunkelt, man habe sich ohnehin keine Chancen auf Umsetzung in einer schwarz-roten Koalition ausgerechnet und das Werk daher lieber zu Wahlkampfzwecken verbreitet. Dabei stellt gerade der Arbeitnehmerdatenschutz eine der wichtigsten Herausforderungen des Datenschutzes dar, wie uns die Skandale des vergangenen Jahres deutlich vor Augen geführt haben.

Eigentlich ist der vorgelegte Entwurf ein Lichtblick. Sowohl strukturell als auch inhaltlich ist es der erste, der aufgrund seiner handwerklichen Solidität eine konstruktive Diskussionsgrundlage darstellt. Er reduziert Begriffskomplexität, wo sie nicht erforderlich ist und nähert sich stärker an die Begriffe der IT-Sicherheit an, als die Datenschutzgesetzgebung dies bisher jemals getan hat. In Zusammenhang mit Anforderungen an die Sicherheit der verwendeten Systeme und Daten wird ausdrücklich auf die in der IT-Sicherheit etablierten Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität Bezug genommen.

Inhaltlich zeugt der Entwurf von dem deutlichen Bemühen, den Anforderungen des Datenschutzes auch in den heute anzutreffenden Konzernstrukturen und trotz des Einsatzes moderner IT-Technologie gerecht zu werden. Ob zu Videoüberwachung, zu Ortungssystemen oder zu biometrischen Verfahren – die Autoren haben durchgängig Regelungen vorgeschlagen, die als vernünftige Grundlage des weiteren Diskurses dienen können. Ob, wie vorgeschlagen, ein eigener Datenschutzbeauftragter für Beschäftigtendaten bestellt werden muss, um die Mitbestimmung zu sichern, mag zunächst dahingestellt bleiben, schmälert aber den Wert des Textes nicht.

Weniger von Sacherwägungen und Betroffeneninteressen geleitet war dann jedoch offensichtlich die neue Koalition. Sie nahm in den Koalitionsvertrag die Absicht auf, den Arbeitnehmerdatenschutz in „einem eigenen Kapitel im Bundesdatenschutzgesetz" abzuhandeln. Die Folge wäre entweder ein noch überladeneres Gesetz oder die Reduktion der Arbeitnehmerdatenschutzes auf wirtschaftsfreundliche Allgemeinplätze.

Emanzipation des Datenschutzes

Wie vor allem Abgeordnete der CDU und CSU ticken, konnte man in der öffentlichen Anhörungen zu BDSG-Novellierungspa-

ket (Innenausschuss)[5] und zum Arbeitnehmerdatenschutz (Ausschuss Arbeit und Soziales)[6] im Frühsommer letzten Jahres erleben: Obwohl in dem nach den ersten großen Datenschutzskandalen eilig einberufenen Datenschutzgipfel verschiedene Vereinbarungen zum Schutz von Verbrauchern und Arbeitnehmern getroffen wurden, wurden diese nach massiver und intriganter Lobbyarbeit von Wirtschaftsverbänden gar nicht oder nur ihrer Substanz beraubt umgesetzt. Weder überlebte das Opt-In-Prinzip die Beratungen im Ausschuss noch wurde den Arbeitgebern konkrete Vorgaben zur Vermeidung ungerechtfertigter Arbeitnehmerüberwachung zugemutet. Der lächerliche § 32 des novellierten BDSG ist, je nach Auslegungs- oder Lesart, einfach nur überflüssig oder steht in Widerspruch zu bestehenden Regelungen.

Den Datenschutz den Händen der Wirtschaftslobbyisten zu entringen wird daher eine weitere Herausforderung der nächsten Jahre sein. Solange mit dem Argument drohenden Arbeitsplatz-Abbaus schamlos die Verletzung der Persönlichkeitsrechte von Betroffenen begründbar ist, stimmt mit der parlamentarischen Einsortierung des Datenschutzes etwas nicht.

Wenn aber von den parlamentarischen Akteuren keine angemessenen Aktivitäten erfolgen, stellt sich die Frage nach Möglichkeiten der Einflussnahme durch Betroffene: Bürgerinnen und Bürger, Beschäftigte, Verbraucherinnen und Verbraucher. Wenn der Gesetzgeber öffentliche Unterstützung benötigt, um sich von Wirtschaftsverbänden zu emanzipieren, müssen Diskussionen möglichst medienwirksam geführt werden. Zumindest in dieser Frage haben sich in den letzten Jahren deutliche Änderungen ergeben.

Grundlagen bürgerrechtlichen Engagements

Zu Demonstrationen gegen den staatlichen Überwachungswahn gehen inzwischen jedes Jahr Zehntausende auf die Straße, bei Petitionen zu Datenschutz-Themen werden Tausende aktiv. Der Verfassungsbeschwerde gegen die Vorratsdatenspeicherung haben sich rund 35.000 Personen angeschlossen. Wir lesen fast täglich über neue Datenschutzskandale in den Medien. Dies liegt nicht etwa daran, dass auf einmal ständig gegen Datenschutz verstoßen würde, sondern daran, dass die ständigen Verstöße auf einmal medientauglich scheinen.

Wer heute einen Datenschutz-Skandal aufdecken oder über fragwürdige Praktiken informieren möchte, trifft bei Journalisten auf großes Interesse. Das war vor einigen Jahren noch deutlich anders. Wer vor 10 Jahren Missstände anprangern wollte, musste sich an Bürgerrechtsorganisationen wenden, die nur beschränkte Mittel hatten um Öffentlichkeit zu erzeugen. Datenschutz galt den etablierten Medien als trockene Materie und Langweilerthema. In diese Lücke stießen 2000 die Aktivisten des FoeBud[7], die die britische Idee der BigBrotherAwards (BBA) für Datensünder nach Deutschland holten.

Die BBA mauserten sich innerhalb von 10 Jahren von einem Geheimtipp für Datenschutzaktivisten zu einer in fast allen Medien wahrgenommenen Veranstaltung. In den Anfangszeiten der BBA stand die Aufdeckung datenschutzunfreundlichen Verhaltens stärker im Vordergrund als heute. Vieles wäre nicht bekannt geworden, hätten die „Datenkraken“ keinen Preis erhalten. Dies ist heute anders, wie sich schon an den Nominierungen ablesen lässt. Zahlreiche Nominierungen beziehen sich auf Vorgänge, über die bereits ausführlich öffentlich berichtet wurde. Den Sprung zur medialen Wahrnehmung hat der Datenschutz also offensichtlich geschafft. Aber hat er ihn auch in das Verständnis der Mehrheit der Betroffenen geschafft?

Die gerade erfolgte Verleihung der diesjährigen BBA zeigt: aller medialen Aufmerksamkeit zum Trotz gerät die Verletzung von Persönlichkeitsrechten offensichtlich in manchen Lebenszusammenhängen zum Kavaliersdelikt. Gerade der Preis für die Arbeitswelt wurde für einen Trend vergeben, bei dem Unternehmen „dem Wahn erliegen, man erhielte produktive und motivierte Mitarbeiterinnen und Mitarbeiter, wenn man sie nur möglichst flächendeckend und umfassend überwachte und ihre Leistung in Zahlen vermeintlich messbar machte“. Auch ein Großteil der Schelte, die die Jury dafür einsteckte, dass sie dem in dieser Kategorie größten Kuriosum, einem per GPS permanent überwachten Mähdrescher den Preis stellvertretend zusprach, lässt Defizite im Verständnis von Datenschutz erkennen. Die Schelte gründet sich fast immer auf die Argumentation, dass es in Zeiten harter wirtschaftlicher Konkurrenz gute Gründe für die effiziente Ausnutzung teurer Landmaschinen gäbe und die Überwachung der Mähdrescherfahrer doch gar nicht beabsichtigt sei. Genau das aber ist das Missverständnis, dem nicht nur die vielen Preisträger, sondern ganz offensichtlich auch viele technikbegeisterte Landwirtschaftsfreunde aufsitzen: nämlich die Annahme, wenn man nur einen sinnvollen Zweck identifizieren könne, rechtfertige das das Ignorieren der Persönlichkeitsrechte Betroffener. „Wir wollen doch nichts Böses“ war aber zu Recht noch nie eine Zulässigkeitsgrundlage für die Verarbeitung personenbezogener Daten.

Karin Schuler

Karin Schuler ist stellvertretende Vorsitzende der Deutschen Vereinigung für Datenschutz e.V., langjähriges FIfF-Mitglied, Beraterin für Datenschutz und IT-Sicherheit und vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstei n anerkannte Sachverständige für IT-Produkte.

Kontakt: Tel. 0228-2420733 · *buero@schuler-ds.de · www.schuler-ds.de*

Flächendeckende Datenschutz-Bildung

Was kann man hieraus ablesen? Nachdem der Datenschutz es in die Medien geschafft hat, muss Wissen über seine Grundlagen und Anforderungen auch in die Breite getragen werden. Es wäre schade, wenn die öffentliche Betroffenheit, ähnlich wie nach der Bewegung gegen die Volkszählung in den 1980er Jahren, nach kurzer Zeit wieder der allgemeinen Gleichgültigkeit weichen würde. Die Bedeutung des Datenschutzes für unser demokratisches Gemeinwesen sollte allgemein verstanden werden. Dazu bedarf es insbesondere der Bildung durch alle Träger, die hierfür geeignet scheinen: Schulen, Hochschulen, Verbände und sonstige Bildungseinrichtungen müssen sich des Themas annehmen. So darf es beispielsweise nicht mehr zum guten Ton gehören, dass Lehrer damit kokettieren, sich weniger als ihre Schüler in Internet-Fragen auszukennen.

Nicht selten hört man in diesem Zusammenhang auch Diskussionen, in denen darüber gestritten wird, ob man sich als Bürger eher gegen staatliche Überwachungswünsche oder gegen die Begehrlichkeiten von Wirtschaftsunternehmen oder sonstigen Privaten zur Wehr setzen soll. Geradeso als rechtfertigte staatliche Datengier die Gleichgültigkeit gegenüber privaten Datenkraken – und umgekehrt. Die Aufstellung dieser Art von „Hitlisten" ist jedoch kontraproduktiv. Sowohl öffentliche als auch nicht-öffentliche Stellen pflegen heutzutage umfangreiche Datensammlungen und verfolgen ihre jeweiligen Interessen häufig zu einseitig. Die Aufstellung gleichermaßen demokratischer wie persönlichkeitsachtender Regeln für den Umgang mit Daten über Menschen ist für alle Bereiche – öffentliche wie nicht-öffentliche – erforderlich. Und deren Einhaltung muss in beiden Bereichen kontrolliert und Verstöße sanktioniert werden. Weder bewahren die vermeintlich wohlgeordneten Verwaltungsabläufe staatliche Stellen vor schlimmen Datenschutzverstößen noch werden nicht-öffentliche Stellen wirksam durch die hoffnungslos unterbesetzten Aufsichtsbehörden kontrolliert.

So sehr es also Aufgabe für den Gesetzgeber ist, den Ausgleich zwischen Persönlichkeitsrechten und Sicherheitsanforderungen in Zukunft nicht weiterhin ständig zuungunsten der Persönlichkeitsrechte verschieben, so sehr ist es Aufgabe für uns alle, im Interesse der Sache Abstand von Biertischparolen zu nehmen – und solche auch in Diskussionen nicht zuzulassen.

Sicher ist es für einen engagierten Datenschützer nicht immer leicht, zum x-ten Male sachlich die ignoranten Sprüche „Ich habe nichts zu verbergen", „Wer gegen Internet-Sperren ist, befördert Kinderpornografie", „Mautdaten müssen für Verbrechensbekämpfung zugänglich sein" oder „Kryptografie nutzt Terroristen" zu widerlegen. Trotzdem gibt es hierzu keine Alternative. Denn ein möglichst breites Verständnis für die Wirkungsweise demokratischer Grundprinzipien ist auch Voraussetzung für funktionierenden Datenschutz. Leider ist noch zu wenigen bewusst, dass man nicht einerseits strenge Zweckbindung für die Verwendung der eigenen Daten (sei es im Arbeitsverhältnis, sei es im Internet-Handel) verlangen und andererseits „Hurra" schreien kann, wenn die durch das Autobahnmautgesetz streng zweckgebundenen Daten bei einem Verbrechen auf einmal für eine umfassende Rasterfahndung genutzt werden sollen.

Mündige Bürger müssen begreifen, dass bestimmte demokratische Grundprinzipien nicht nach Belieben und nur für vermeintlich „rechtschaffene Bürger" gelten können, weil sie sonst sehr schnell für niemanden mehr gelten. Das ist, neben allen Forderungen an den Gesetzgeber, die Herausforderung für uns selbst.

Endnoten

1 *www.dud.de*
2 *www.secorvo.de/security-news/secorvo-ssn0910.pdf*
3 *www.lda.brandenburg.de/sixcms/media.php/2473/dsmodern.pdf*
4 *www.bmas.de/portal/37290*
5 *www.bundestag.de/bundestag/ausschuesse/a04/anhoerungen/Anhoerung_18/index.html*
6 *www.bundestag.de/bundestag/ausschuesse/a11/anhoerungen/qDatenschutz/index.html*
7 *Verein zur Förderung des bewegten und unbewegten Datenverkehrs – der Name ist eine Persiflage auf das Benennungskauderwelsch der damaligen Bundespost.*

Darüber hinaus werden wir eine Stiftung Datenschutz errichten, die den Auftrag hat, Produkte und Dienstleistungen auf Datenschutzfreundlichkeit zu prüfen, Bildung im Bereich des Datenschutzes zu stärken, den Selbstdatenschutz durch Aufklärung zu verbessern und ein Datenschutzaudit zu entwickeln. Wir sind überzeugt, dass mit dieser Lösung auch der Technologiestandort Deutschland gestärkt wird, wenn datenschutzfreundliche Technik aus Deutschland mit geprüfter Qualität weltweit vertrieben werden kann.

Wir werden beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die personelle und sächliche Ausstattung verbessern. Die Unabhängigkeit der Datenschutzaufsicht steht für uns dabei im Mittelpunkt.

Auch der Einzelne trägt Verantwortung für seine persönlichen Daten. Wir wollen deshalb die Sensibilität und Selbstverantwortung der Bürgerinnen und Bürger für ihre eigenen Daten stärken.

WACHSTUM. BILDUNG. ZUSAMMENHALT. DER KOALITIONSVERTRAG ZWISCHEN CDU, CSU UND FDP, S. 106.

Marie-Theres Tinnefeld

Freiheit für die Technik der Bürgerin und des Bürgers?

Gedanken zum technologisch geprägten Grundrechtsschutz

Einführung: Bedenklicher Prozess der Gesetzesbildung

Cato der Ältere, römischer Staatsmann im zweiten Jahrhundert vor Christus, soll jede seiner Reden im Senat mit dem Satz geschlossen haben: *„Ceterum censeo Carthaginem esse delendam"* („Im Übrigen meine ich, dass Karthago zerstört werden muss"). Diese ständige Wiederholung führte nach der Überlieferung dazu, dass der Senat schließlich Cato zustimmte und Carthago im Dritten Punischen Krieg (149-146 v. Chr.) angriff und zerstörte. Die rhetorisch geschickte, nicht immer im Sachzusammenhang motivierte *Wiederholung* war gleichsam der *Brandbeschleuniger* dieser kriegerischen Aktion.

Referat am 5. September in der Universität Bremen Festkolloquium aus Anlass des 60. Geburtstags von Prof. Dr. Hans-Jörg Kreowski

Diese Geschichte aus antiker Zeit ist Ihnen sicherlich bekannt. Vielleicht ahnen Sie auch, warum ich sie meinem Thema voranstelle. Seit den verheerenden Ereignisse von 9/11 sind in den Medien, vor allem im Fernsehen, Terrorakte immer wieder in Endlosschleifen präsentiert worden. Gleichzeitig wurde im „war on terror" gebetsmühlenartig die Forderung nach mehr Sicherheit in vorher offenen westlichen Ländern wiederholt. Die Kombination vom Endlos-Bild des Terrors mit der ständigen Forderung des Staates nach mehr Sicherheit zu Lasten klassischer Freiheitsrechte hat bislang zahlreiche Antiterrorgesetze produziert. Triumphieren diese Gesetze *„in einer - darf man sagen göttlichen, soll man sagen: teuflischen? - Freiheit"* (Peter von Matt).

Einen solchen Triumph und mithin die schleichende Erosion unseres Rechtssystems hat das Bundesverfassungsgericht häufig verhindern können, indem es Gesetze ganz oder teilweise als verfassungswidrig und für nichtig erklärte. Wesentliche Stichworte sind: der Große Lauschangriff, die Erfassung der Kontostammdaten, die vorbeugende Telekommunikations-Überwachung, das Luftsicherheitsgesetz, die präventive Rasterfahndung, die sogenannte Online-Durchsuchung und schließlich die Einstweilige Anordnung zur sogenannten Vorratsspeicherung. Das umstrittene nationale Gesetz zur Vorratsdatenspeicherung basiert auf einer ebenso umstrittenen EU-Richtlinie, die am Maßstab der Grundrechte zu messen ist.

Schon Wilhelm von Humboldt hat in seiner 1792 fertiggestellten Schrift über „Die Idee zu einem Versuch, die Grenzen der Wirksamkeit des Staates zu bestimmen" sinngemäß dargelegt, dass *Sicherheit ohne Freiheit unerträglich* ist. Die Verfassung verlangt vom Gesetzgeber, eine angemessene Balance zwischen Freiheit und Sicherheit herzustellen. Jede Freiheitseinschränkung unter der positiv klingenden Vokabel „Prävention" könnte sich andernfalls dem negativen Bild eines Überwachungsstaats annähern, in dem anlasslose und vor allem heimliche, technisch gesteuerte Eingriffe für rechtens erklärt werden.

Durch den zunehmenden Einsatz subtiler Informationstechnologien werden neue Gefährdungen grundrechtlich geschützter Freiheiten sichtbar, mit denen sich auch das Forum für Informatiker/innen für Frieden und gesellschaftliche Verantwortung mit seinem Vorsitzenden Hans-Jörg Kreowski in den letzten Jahren nachhaltig befasst hat. Die Abhängigkeit des Grundrechtsschutzes von der Technik ist kaum an anderer Stelle so deutlich formuliert worden wie im Zusammenhang mit der Kritik an der Technik auf diesem Forum. Diese führt letztlich zu der Erkenntnis, dass sich Bürger ohne *Vertrauen in eine sichere Technik* nicht mehr frei und selbstbestimmt in der vernetzten (Welt-) Risikogesellschaft bewegen können (Ulrich Beck).

Das Bundesverfassungsgericht hat sich mit dieser Entwicklung befasst und das grundrechtlich verankerte allgemeine Persönlichkeitsrecht durch neue Schutzdimensionen abgesichert. Nach dem Grundrecht auf Datenschutz hat das Gericht aus dem Persönlichkeitsrecht ein *„Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"* (im Folgenden: IT-Grundrecht) abgeleitet, das die freie Entfaltung der Persönlichkeit in Verbindung mit dem Menschenwürdeschutz gewährleistet.

Das Bundesverfassungsgericht: Bewahrer lebendiger Grundrechte

Vor mehr als 25 Jahren haben zahlreiche Bundesbürger aus Furcht vor der Undurchschaubarkeit elektronischer Datenverarbeitung, vor dem gläsernen Bürger und vor einer Volksdurchsuchung gegen ein Gesetz zur Volkszählung protestiert. Das Bundesverfassungsgericht hat in seiner Entscheidung zu diesem Gesetz am 15. Dezember 1983 nicht nur auf die Undurchsichtigkeit der technischen Vorgänge bei der personenbezogenen Datenverarbeitung reagiert, sondern es passte auch die Vorgaben des allgemeinen Persönlichkeitsrechts den Bedingungen der automatisierten Datenverarbeitung an und schuf das Grundrecht auf informationelle Selbstbestimmung bzw. auf Datenschutz, worunter auch das rechtlich geschützte Interesse des Einzelnen an Intimität und Privatheit zu verstehen ist. In neueren Entscheidungen spricht das Gericht von einem Grundrecht auf informationelle Privatheit (information privacy). Die Formulierung findet sich bereits bei Alan F. Westin in seinem Werk „Privacy and Freedom" (1967). Dem Schutz der Privatheit dienen auch spezielle Freiheitsverbürgungen wie das Grundrecht auf Unverletzlichkeit der Wohnung und das grundrechtlich verankerte Post-, Brief- und Fernmelde- bzw. Telekommunikationsgeheimnis.

Mit seiner ausdrücklichen *Forderung nach Datenvermeidung und Datensparsamkeit* hat das Bundesverfassungsgericht im Volkszählungsurteil eine Allianz von Datenschutz und Technik im Interesse der Privatheit und sicheren Kommunikation angesteuert und gleichzeitig eine zweckfreie Vorratsdatenspeicherung verboten, wie sie z. B. von der Telekom praktiziert wurde und von Sicherheitsbehörden und Geheimdiensten zu präventiven Zwecken gefordert wird.

Die Forderung nach Transparenz der Datenverarbeitung für den Betroffenen ist ein wichtiges Ziel des Datenschutzes. Sie lebt von der Voraussetzung, dass nicht beliebig viele, sondern nur die für einen bestimmten Zweck der Datenverarbeitung und Kommunikation unbedingt erforderlichen persönlichen Daten erfasst werden. Zur Ausgestaltung des Grundrechts auf Datenschutz gehört daher das Prinzip der Datensparsamkeit bzw. sogar das der Datenvermeidung, das in der Nicht-Offenlegung der Identität einer Person besteht, also ihre Anonymität sichern soll.

Dieses *Recht auf Anonymität* ist Teil des Grundrechts auf Datenschutz und somit eine Selbstverständlichkeit im täglichen Leben. Helmut Bäumler hat dies so ausgedrückt: *„Es ist fast so, wie wenn wir atmen, essen und trinken, ohne dass wir überhaupt daran denken, dass wir dabei unser Grundrecht auf Leben realisieren."* Angesichts der ständigen Beschwörung höchster Gefahren ist dieses Recht jedoch in Misskredit geraten. Wer anonym sein will, macht sich verdächtig; er hat etwas (Gefährliches, Strafbares?) zu verbergen.

Dies vermutet wohl auch der fürsorgliche Präventionsstaat, der bereits im Vorfeld von Straftaten ermitteln und vorbeugende Dateien über Personen erstellen will, von denen er annimmt, dass sie in Zukunft eine Straftat begehen wollen oder werden. Dementsprechend erodieren die Grenzen zwischen Schuldigen und Unschuldigen, und jede Person wird zum Risikofaktor. Bewegen sich die Bürger angesichts dieser Entwicklung *„schlafwandelnd in den Überwachungsstaat?"* - so die berechtigte Frage des auf der britischen Insel lebenden Rechtsinformatikers Burkhard Schäfer.

Die überwiegend von Kommunen betriebenen Kameras zur Videoüberwachung (CCTV-Systeme bzw. Closed Circuit Television) und die größte DNS Datenbank in England weisen in diese Richtung. Sie haben die Zerschlagung von kriminogenen Strukturen schon im Vorfeld eines „Anfangsverdachts" zum Ziel. Bei genauerem Hinsehen hat sich aber nicht nur die flächendekkende Videoüberwachung in Englands Städten als nutzlos erwiesen. Sie birgt auch große Gefahren für die Rechtssicherheit im Sinne verbürgter Freiheitsrechte des citizen. Gleichwohl bleibt die öffentliche Zustimmung insbesondere zur CCTV –Überwachung hoch.

Man sollte die technischen Möglichkeiten der Videoüberwachung kennen, wenn man ihr ein vernünftiges, datenschutzgerechtes Maß anlegen will. Hier sei auf geeignete Software (z.B. das Software-Modul „Privacy Protector" von KiwiSecurity) hingewiesen, mit der man die Videoüberwachung nach den Grundsätzen der Datensparsamkeit und Datenvermeidung effizient gestalten kann[1].

Der Europäische Gerichtshof für Menschenrechte: Schutzschild des Privatlebens

Eine Entwicklungslinie des Datenschutzes wurzelt in der Europäischen Menschenrechtskonvention (EMRK). Art. 8 der Konvention garantiert das Recht auf Achtung des Privatlebens, des Familienlebens, der Wohnung und des Briefverkehrs bzw. der Telekommunikation. Der Artikel gewährleistet mit seinen Teilgarantien einen *weiten Raum der freien Entfaltung der Persönlichkeit*. Er findet sich zusammen mit einer speziellen Datenschutzbestimmung in der EU- Charta der Grundrechte (Art. 7 und Art. 8 EuGRC) wieder, die erst mit der Verabschiedung des Vertrags von Lissabon rechtskräftig wird.

Im Zusammenhang mit der Speicherung von personenbezogenen Daten hat der Europäische Gerichtshof für Menschenrechte im Jahre 2000 den Schutzbereich von Art. 8 wie folgt umschrieben: „*It points out in this connection that the term «private life» must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings*." Auf diese Weise hat das Gericht den Schutzbereich des Privatlebens gegenüber neu auftretenden Gefährdungen nachhaltig erweitert, so dass der Europarechtler Rainer Schweizer Art. 8 als europäisches Auffanggrundrecht bezeichnen kann.

Vor diesem Hintergrund ist zu betonen, dass Zugriffe auf den Informations- und Kommunikationsverkehr etwa bei einem systematischen Abhören aller Telefone in einer Anwaltskanzlei, wie das in der Klage Kopp gegen die Schweiz von 1998 der Fall war, personenbezogene Daten in unzulässiger Weise erheben: Das unzulässige Abhören von Wohnungen und Telefongesprächen, die Eingriffe in die Telekommunikation und verschiedene wei-

Marie–Theres Tinnefeld

Prof. Dr. Marie-Theres Tinnefeld ist Juristin und Publizistin mit Schwerpunkt Datenschutz- und Wirtschaftsrecht. Sie ist Mitglied im wissenschaftlichen Beirat des FIfF.

tere polizeiliche Maßnahmen sind Gegenstand der Rechtsprechung des Gerichtshofes. Gleiches gilt für die Bild-Überwachung des Personenverkehrs zu Wohnungen oder das elektronische Eindringen in diese.

Der Gerichtshof schafft in seiner Einzelfall-Judikatur *Distanz zu der Maßlosigkeit der Überwachungsvorgänge in europäischen Staaten*. Auch das Bundesverfassungsgericht hat beschämende Tiefpunkte in der Sicherheitsdebatte immer wieder reflektiert. Es hat auf den Möglichkeitshorizont der modernen Technik reagiert und ein IT-Grundrecht formuliert. Mit der Schaffung des neuen Grundrechts versucht das Gericht, sich einem Modell der „Freiheit für die Technik" der Bürgerin und des Bürgers anzunähern.

Das IT-Grundrecht: Garant der Freiheit für die Technik?

Die vernetzte digitale Datenverarbeitung macht es möglich, noch mehr Informationen heimlich zu erlangen, sie beliebig zusammenzuführen, ohne dass Bürger und Bürgerinnen die Richtigkeit und Verwendung ihrer Daten kontrollieren könnten. Cyberkriminelle nutzen die Schutzlücken eigengenutzter IT-Syteme und überführen sie in ein sogenanntes Botnetz (Netz von Robotern), um sie wahlweise für das Versenden von Spam oder für gezielte Angriffe auf einzelne Dienste im Netz einzusetzen.

Sicherheitsbehörden haben ebenfalls damit begonnen, diese Einfallstore zu nutzen. Sie legen auch kein Stopp-Schild vor den Toren derjenigen ein, die aufgrund ihres Berufes zur Verschwiegenheit verpflichtet sind (z.B. Journalisten, Ärzte und Anwälte). Die Behörden durchsuchen mit technischen Hilfsmitteln, sogenannten „Trojanischen Pferden" (Online-Durchsuchung) privat genutzte Rechner, um heimlich *Informationen über die Lebensgestaltung* der jeweiligen (verdächtigen)" Zielperson" sowie ein aussagekräftiges Bild ihrer potenziellen terroristischen oder anderen kriminellen Pläne zu gewinnen.

Wer immer sich den *Zugang zu den IT-Systemen* der Bürger verschafft , erhält nach den Worten Winfried Hassemers - jedenfalls ausschnitthaft - *Zugang* zu deren *„ausgelagertem Hirn"*. Er erhält die Möglichkeit, lebensbestimmende intime und private Informationen kennen zu lernen. Beim Zugriff auf solche Systeme droht zugleich ihre irreversible Manipulation. In seinem Urteil zur Online-Durchsuchung vom 27. Februar 2008 hat das Bundesverfassungsgericht die Konsequenz aus den neuen technischen Angriffspotenzialen im Internet und deren Verlagerung auf die eigengenutzten Rechner gezogen und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geschaffen. Das Gericht hat gleichzeitig anlasslosen Eingriffsinteressen der Vertreter von Polizei und Geheimdiensten einen Riegel vorgeschoben. Ihr Traum, eher am Tatort zu sein als der Täter, dürfte damit hoffentlich ein Ende gefunden haben.

An dem neuen *IT-Grundrecht* ist zwar nicht abzulesen, wie der angemessene Schutz der Grundrechtsträgerin/des Grundrechtsträgers im Einzelnen auszusehen hat. Immerhin steht fest, dass sie die *Technik frei und selbstbestimmt* nutzen können. Ohne Vertrauen in die eigene Technik sind sie fremden Eingriffen in ihr Privatleben und ihre Kommunikation ausgeliefert. So gesehen ist das Plädoyer von Ulrich Beck *„Freiheit für die Technik"* zur Bedingung des Überlebens für den Einzelnen sowie seine Kontakt- und Begleitpersonen in einer offenen Gesellschaft geworden. Dabei trifft den Rechtsstaat zweifellos die Aufgabe, diese Freiheit zu schützen, auch wenn sie von Dritten bedroht wird.

Schlussbetrachtung: Die Menschenwürde ist nicht wegwägbar

Wilhelm von Humboldt führte einst aus, dass *Sicherheit ohne Freiheit* unerträglich wäre. Dies hat auch das Bundesverfassungsgericht immer wieder betont und darüber hinaus ausdrücklich festgestellt, dass Eingriffe in den *Kernbereich privater Lebensgestaltung*, der sich letztlich aus der *Menschenwürde* ableitet, durch staatliche Überwachungsmaßnahmen nicht erlaubt werden. Die Menschenwürde ist *nicht wegwägbar*, auch nicht mit Sicherheitspflichten des Staates. Daher stellt sich bei der Online-Durchsuchung ein gravierendes Problem. Vor einer Datenerhebung kann nicht geklärt werden, ob persönlichste Informationen (Gedanken, ungestüme Phantasien, intime Aussagen usw.) aus dem Kernbereich betroffen sind. Wird damit nicht der unendlich wertvolle Vorrat an persönlichem Gedankengut bedroht? Haben nicht totalitäre Systeme Versuche in diese Richtung unternommen?

Um solche Bedrohungen des Kernbereichs abzuwenden, hat das Bundesverfassungsgericht ein zweistufiges Schutzkonzept durch die Unterscheidung von Erhebungs- und Auswertungsphase entwickelt. Dies hindert zwar die Sicherheitsbehörden, nicht aber einen kontrollierenden Richter, Kenntnis von Informationen aus dem Kernbereich zu erhalten. Damit aber wird nun der Kernbereich für die Abwägung durch den Richter offen und so auch antastbar oder sogar relativierbar.

Durch ständige Wiederholung einer Aussage im Sinne Catos wird schließlich Wahrheit vorgetäuscht. Ständige Hinweise auf die bedrohte Sicherheit lassen Anti-Terror-Gesetze ausufern. Dass sie ihre Grenze in der Unabdingbarkeit der Menschwürde finden, ist ein Postulat, das wir alle zu verteidigen haben.

Endnote

1 *Das Modul wurde im August 2009 mit dem EuroPriSe-Siegel (www.european-privacy-seal.eu) ausgezeichnet. Es ermöglicht im Einzelfall etwa die datenschutzgemäße Verschleierung von Video-Klardaten in Echtzeit. Bewegte Personen oder personenbeziehbare Objekte (z.B. Kfz-Kennzeichen) in digitalen Videobildern, die nicht erforderlich sind, können unkenntlich gemacht werden.*

Alex Klein

DIGITAL IST BESSER? – IKT IN DER ARMUTSBEKÄMPFUNG

Eine der wohl größten Herausforderungen der Menschheit ist die globale Bekämpfung von Armut. Welchen Beitrag können moderne Informations- und Kommunikationstechnologien leisten, wo und wie finden sie schon heute Einsatz und welche Resultate einer IKT-gestützten Armutsbekämpfungsstrategie zeichnen sich ab? Alex Klein beschreibt im Folgenden das Potenzial von IKTs als Werkzeug zur Armutsbekämpfung und schildert beispielhaft den Fortschritt von entsprechenden Projekten in Äthiopien.

Als die Vereinten Nationen zusammen mit der Weltbank, der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) und einigen Nichtregierungsorganisationen im Jahr 2000 die globalen Millenniumsziele formulierten, stellten sie sich einer großen Herausforderung. Die acht formulierten Zielsätze, die bis 2015 umgesetzt werden sollen, gelten seither als Messlatte für die Anstrengungen der internationalen Gemeinschaft bei der weltweiten Bekämpfung von Armut. Von Informations- und Kommunikationstechnologie ist in diesen Zielen nicht die Rede. Das ist jedoch auch nicht weiter verwunderlich. Schließlich wurden Ziele formuliert und keine Strategien. Doch können Informations- und Kommunikationstechnologien einen Beitrag zur Armutsbekämpfung leisten? Und wenn ja, wie kann dieser aussehen?

Gewöhnlich denken wir, wenn von Armut die Rede ist, an Hunger, Durst oder medizinische Unterversorgung. Nach diesem Verständnis kann moderne Informationstechnologie die Armutsbekämpfung nur mittelbar unterstützen. Beispielsweise bei der Koordinierung der humanitären Hilfsmaßnahmen. Wird jedoch ein Armutsverständnis zugrunde gelegt, wie es der indische Ökonom und Nobelpreisträger Amartya Sen formulierte, wird das Potenzial von IKT durchaus deutlicher. Demnach ist Armut nicht nur ein Zustand, sondern wird vielmehr als ein Prozess verstanden, der Verfügungsrechte, Chancen und Fähigkeiten (*entitlements, opportunities* und *capabilities*) in den Mittelpunkt der Betrachtung rückt. Armut besteht, verkürzt ausgedrückt, nach dieser Definition dann, wenn Menschen aufgrund struktureller Einschränkungen nicht in der Lage sind, ein selbstbestimmtes Leben zu führen und somit ihrer individuellen Entwicklungschancen beraubt werden. Dieser erweiterte Armutsbegriff umfasst somit beispielsweise auch die Zugangseinschränkung zu Bildung, Information und politischer Teilhabe.

Liegt diese Definition von Armut zugrunde, eröffnet sich ein weites Feld an Möglichkeiten, wie moderne Informations- und Kommunikationstechnologien zur Armutsbekämpfung und Entwicklung beitragen können. Darüber hinaus hat dieses Verständnis von Armut Auswirkungen auf die Problematik des globalen *Digital Divide*, jener Unterscheidung von Personen bzw. Personengruppen, die über Zugang zu modernen Informations- und Kommunikationstechnologien verfügen und damit effektiv umgehen können und solchen, die davon ausgeschlossen sind. Die Bekämpfung dieser weltweiten digitalen Kluft ist somit nicht nur eine Wunschvorstellung einer verblendeten digitalen Bohème oder gar ein Luxusproblem. Der Zugang zu Informationen und die Möglichkeiten der Präsentation, wie sie moderne IKTs zur Verfügung stellen können, sind grundlegende Bedürfnisse und Rechte aller Menschen dieser Erde und somit auch ein Bestandteil der Armutsbekämpfung. Es soll dabei nicht in Abrede gestellt werden, dass in einer Situation größten Mangels ein Sack Reis viel wichtiger ist, als eine Laptopbatterie. Um jedoch eine nachhaltige und vor allem selbstbestimmte Entwicklung zu ermöglichen, und somit den Teufelskreis der Armut und Fremdbestimmtheit zu durchbrechen, sind IKTs ein wichtiger Baustein.

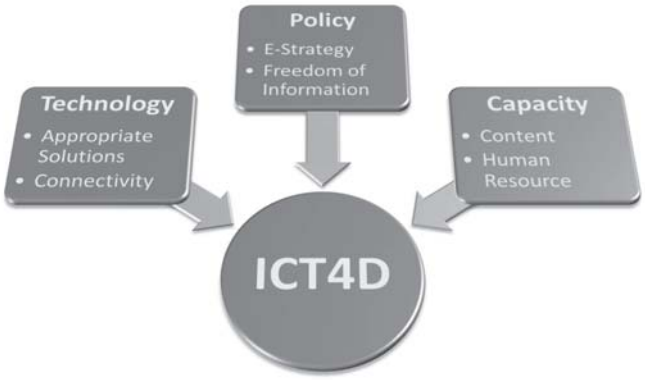
Dieser Gedanke ist nicht neu und auch der Einsatz von Kommunikations- und Informationstechnologie in der Armutsbekämpfung und Entwicklungszusammenarbeit ist nichts Außergewöhnliches mehr. Bereits Ende der 90er Jahre wurde mit Nachdruck das Potential von IKTs in diesen Bereichen diskutiert. Entstanden ist die Abkürzung ICT4D, welche für *„Information and Communication Technology for Development"* steht und seither eine Art Sammelbegriff für alle Bemühungen darstellt, die mit Hilfe moderner IKTs Armut bekämpfen und Entwicklung fördern wollen. So allgemein, wie dieser Überbegriff gehalten ist, so ungleich sind die Strategien und Vorgehen in der Umsetzung. Wichtig ist es jedoch, ICT4D nicht als ein rein technisches Konzept misszuverstehen. Computer, Mobiltelefone oder Internetzugänge für sich genommen, schaffen noch keine Entwicklung oder bekämpfen Armut. Sie sind lediglich ein Werkzeug in einem Konzept, dass, soll es erfolgreich sein, noch weitere wichtige Aspekte umfassen muss. Um IKTs für die Armutsbekämpfung und für eine nachhaltige Entwicklung nutzbar zu machen,

Alex Klein

Alex Klein studierte Friedens- und Konfliktforschung an der Otto-von-Guericke Universität in Magdeburg und hat zuvor ein Studium der Wirtschaftsinformatik an der Fachhochschule für Wirtschaft in Berlin abgeschlossen. Im Rahmen der Erstellung seiner Masterarbeit reiste er nach Äthiopien, um vor Ort einen Einblick in die ICT4D Strategie der äthiopischen Regierung zu erhalten.

müssen darüber hinaus entsprechende politischen Rahmenbedingungen gegeben sein und hinreichende Kapazitäten zur Verfügung stehen. Die politischen Rahmenbedingungen sind notwendig, um den Auf- und Ausbau der technischen Infrastruktur zu ermöglichen und gegebenenfalls zu koordinieren. Ferner sollten Sachverhalte wie der grundsätzliche Umgang mit IKTs, Informationen oder geistigem Eigentum politisch und juristisch definiert sein. Ganz klar ist dabei auch die unzensierte Informations- und Ausdrucksfreiheit ein elementarer Bestandteil. Das Entwickeln von Kapazitäten bezieht sich zum einen auf die Aus- und Weiterbildung der Menschen, um sie zu befähigen, IKTs nutzen zu können. Zum anderen ist die Erstellung und Zurverfügungstellung von Inhalten, die relevant, verständlich und leicht zugänglich sein müssen, von erheblicher Bedeutung. Dies gilt umso mehr für die Möglichkeit, eigene Inhalte zu publizieren und somit einen tatsächlichen Informations*austausch* zu ermöglichen.

Aus dieser Beschreibung ergibt sich folgendes Schema, welches zusammenfassend die wichtigsten Bestandteile einer umfassenden ICT4D Strategie darstellt:



ICT4D als Dreiklang aus Technology, Policy und Capacity. Klein 2009

Das bekannteste und vermutlich umfangreichste derzeitige ICT4D Projekt ist die populäre *One Laptop Per Child* (OLPC) Initiative, welches am *Massachusetts Institute of Technology* (MIT) von dem Internet-Vordenker Nicholas Negroponte initiiert wurde. Im Mittelpunkt dieser Initiative steht ein kleiner grüner, XO-1 genannter, Laptop. In den Medien wurde der Computer häufig als 100-Dollar-Laptop beschrieben, da das Ziel der Entwickler darin bestand, die Produktionskosten bei der Massenfertigung auf 100 US-Dollar pro Einheit zu begrenzen. Dieses speziell für Kinder konzipierte Gerät ist äußerst robust gebaut und für den Einsatz auch unter widrigen Bedingungen geeignet. Als Betriebssystem kommt Linux mit der kindergerechten GNOME-Oberfläche Sugar zum Einsatz. Der Computer soll in erster Linie im Schulunterricht in Entwicklungs- und Schwellenländern eingesetzt werden. Die Initiative verfolgt bei der Konzeption des Projektes und auch bei der eingesetzten Software den Ansatz der konstruktivistischen Didaktik. Dies bedeutet, dass Lernen als ein selbstbestimmter und selbsterfahrender Prozess verstanden wird, der individuell erfolgt. Dieser Ansatz könnte vereinfacht auch mit Lernen durch Ausprobieren beschrieben werden.

Der XO-1. laptop.org.

Auch wenn das Ziel der Produktionskostenreduzierung bisher nicht erreicht wurde (derzeit liegt der Produktionspreis bei ca. 188 USD), findet der XO-1 heute in vielen Ländern rund um den Globus zahlreich Anwendung. Neben der Software wurde auch bei der Projektumsetzung sehr viel Wert auf Open Source gelegt, so dass es mittlerweile eine weltweite Community gibt, die das OLPC Projekt aktiv unterstützt. Allerdings wird bei näherer Betrachtung dieses UnterstützerInnenkreises etwas deutlich, was sehr typisch zu sein scheint, wenn es um ICT4D geht: Die Foren, Wikis und Mailinglisten sind voll von technischen Debatten. Dort geht es häufig darum, das Gerät zu übertackten, andere Betriebssysteme zu installieren oder anderweitige Hacks durchzuführen. Diskussionen um Probleme bei den Projektumsetzungen oder die Unterstützung von Forschungsprojekten finden in sehr viel geringerem Umfang statt. Dieser technische Fokus ist auch in der allgemeinen medialen Berichterstattung erkennbar. Auch dort steht der günstig-praktische und irgendwie drollig ausschauende Laptop mit seinen technischen Raffinessen im Vordergrund.

Das dieses kleine grüne Ding aber nur ein Werkzeug ist, welches in eine den jeweiligen Umständen entsprechende Projektkonzeption eingebettet werden muss, um erfolgreich zu sein, findet wenig Beachtung. Es ist häufig ein einseitiger, technikeuphorischer Diskurs der weit entfernt ist von den Problemen einer konkreten Umsetzung. So beispielsweise in Äthiopien, wo in einer ersten Phase im November 2008 insgesamt 5000 der kleinen grünen Geräte an vier Pilotschulen verteilt wurden. Bislang stehen dort keine technischen Problemstellungen im Vordergrund, die Akzeptanz der Geräte im Unterricht gehört zu den größten Herausforderungen. Die Vorbehalte haben mehrere Gründe. Zum einen fürchten die LehrerInnen, durch die Computer ersetzt zu werden. Zum anderen kollidiert die traditionelle lehrerInnenzentrierte Lehrmethode Äthiopiens mit dem didaktischen Konzept der OLPC Initiative, welches das selbstbestimmte Lernen in den Mittelpunkt rückt. Diese Hindernisse lassen sich jedoch nicht durch den Einsatz von Technik lösen. Die Bearbei-

tung der Probleme setzt eine eingehende Auseinandersetzung und ein grundlegendes Verständnis der jeweiligen Lebensweisen und lokalen Gegebenheiten voraus.

Die äthiopische OLPC Initiative ist nur eines von vielen ICT4D Projekten in Äthiopien. Die Regierung des ostafrikanischen Landes hat ICT4D seit dem Jahr 2002 zu einer der tragenden Säulen der nationalen Entwicklungsstrategie gemacht und hat seither viele Fördermittel der internationalen Gemeinschaft für die Projektumsetzung erhalten. Es wurden umfangreiche Aktionspläne und Strategiepapiere verfasst sowie Behörden geschaffen, welche die IKT-gestützte Bekämpfung von Armut sowie die allgemeine Entwicklung des Landes koordinieren sollen. Dennoch lässt sich weder bei den gängigen IKT-Entwicklungsindizes, noch bei den allgemeinen Entwicklungskennzahlen des Human Development Indexes (HDI) der UN eine signifikante Verbesserung nachvollziehen, die auf den Einsatz von Informations- und Kommunikationstechnologien zurückzuführen wäre. Ganz offensichtlich reicht der Wille, mit IKT Fortschritte zu erreichen, allein nicht aus. Auch wenn dies freilich keine Überraschung ist, stellt sich doch die Frage, was aus den Vorhaben wurde und welche Probleme auftraten. Es soll im Folgenden nicht begründet werden, warum die Bemühungen der Regierung weitgehend erfolglos blieben. Vielmehr steht die Darstellung der Hindernisse und Herausforderung bei ICT4D Projekten an einem praktischen Beispiel im Vordergrund.

Auf den ersten Blick, sehen die Anstrengungen der äthiopischen Regierung beeindruckend aus. Eines der ärmsten Länder der Welt arbeitet bereits seit 2002 an einer umfassenden, nationalen Strategie zur Bekämpfung der Armut mit Hilfe von modernen Informations- und Kommunikationstechnologien. Erste Überlegungen zu dieser Thematik fanden sogar bereits fünf Jahre zuvor statt. 2004 wurde ein annähernd 600 Seiten starker Aktionsplan veröffentlicht, der insgesamt über 280 ICT4D Projekte aufzählte, die in den darauffolgenden Jahren realisiert werden sollten. Zwei Jahre später erschien ein 34 Seiten umfassendes Dokument, welches die Strategie der äthiopischen Regierung umfassend darstellte und die Ziele ausformulierte. Bei genauer Betrachtung wird jedoch sichtbar, dass die aufgezählten Projekte nur sehr ungenau beschrieben sind und eine Analyse der überhaupt zur Verfügung stehenden Ressourcen vollständig fehlt. Das Strategiepapier hinterlässt zwar einen durchdachten Eindruck, kommt aber ohne die Nennung von konkreten, messbaren Zielen aus. So wird als Zielstellung die Transformation Äthiopiens in eine Informations- und wissensbasierten Wirtschaft und Gesellschaft innerhalb der kommenden 20 Jahre beschrieben, nicht hingegen, was darunter überhaupt zu verstehen ist. Allerdings sollte hinzugefügt werden, dass europäische PolitikerInnen vermutlich ebenfalls erhebliche Schwierigkeiten hätten, das in der westlichen Politik ebenso häufig verwendete Begriffspaar Informations- und Wissensgesellschaft gegenständlich zu erklären.

Neben den Dokumenten wurde eine Behörde ins Leben gerufen, welche die ICT4D Projekte der Regierung zentral koordinieren sollte. Die *Ethiopian Information and Communication Technology Development Agency* (EICTDA), welche dem äthiopischen Entwicklungsministerium unterstellt ist, hat jedoch nur bedingt eine koordinierende Funktion. Praktisch sind sehr viele verschiedene Institutionen und Behörden mit der Durchführung von ICT4D Projekten in Äthiopien betreut, die häufig nur mangelhaft miteinander kommunizieren und kooperieren. Internes Kompetenzgerangel oder die Bedingungen der geldgebenden Institutionen und Länder sind nur zwei der Gründe, die zu dieser organisatorischen Inhomogenität führen.

Ein weiteres, viel grundsätzlicheres Problem bei der Umsetzung der nationalen IKT-Strategie besteht jedoch in der Politik der autokratisch agierenden äthiopischen Regierung, die einer Informations- und Wissensgesellschaft diametral gegenübersteht. In einem Land, in dem Oppositionsparteien kriminalisiert werden, die mediale Berichterstattung durch scharfe Repressionen stark eingeschränkt wird und zahlreiche Webseiten nicht zugänglich sind, ist von einer ernst gemeinten IKT-orientierten Entwicklungsstrategie nur wenig zu spüren. Dies wird auch bei einem der Prestigeprojekte der Regierung, dem Woreda-Net Projekt, deutlich. Ziel des Projektes ist die Einbindung aller Regierungs- und Verwaltungsebenen (über 600), sowohl landesweite, als auch regionale und lokale, in ein zentrales Netzwerk. Diese Vernetzung dient in erster Linie der administrativen Informationsübermittlung und wird hauptsächlich durch Satellitenverbindungen (V-SAT) realisiert. Ein wichtiger Bestandteil des Projektes ist außerdem die Möglichkeit, Videokonferenzen durchzuführen, mit deren Hilfe Gerichtsverhandlungen dezentral abgehalten werden können, um so lange und teure Reisen der Beteiligten zu vermeiden.

Was in der Theorie gut klingt, hat in der Praxis zahlreiche Hindernisse. Viele der eigens für dieses Projekt ausgebildeten Fachkräfte verlassen die ländlichen Gebiete, um in der äthiopischen Hauptstadt Addis Abeba oder im Ausland mehr Geld zu verdienen, als es für sie im äthiopischen Staatsdienst möglich ist. Zudem entspricht die installierte Technik häufig nicht den Anforderungen in warmen, staubigen bzw. feuchten oder kalten Umgebungen und ist somit sehr störanfällig. In einigen Gebieten kann zudem die notwendige Stromversorgung zum Betrieb der teuren Hardware nicht gewährleistet werden. Offiziellen Angaben der

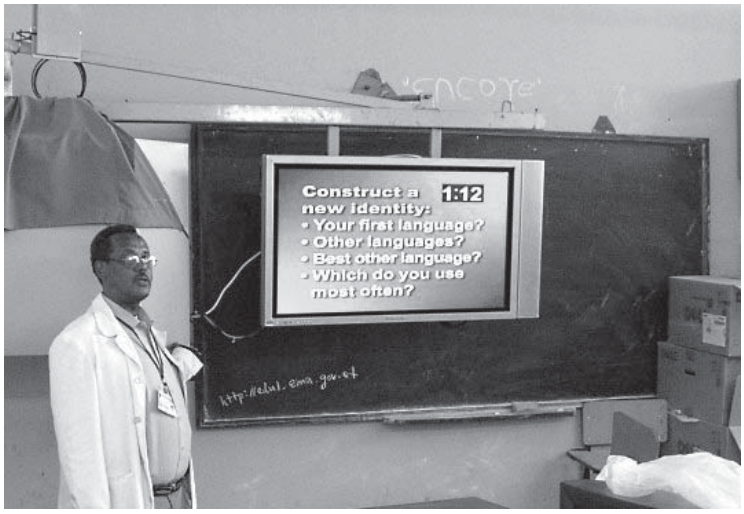
WoredaNet VSAT-Anlage in Mida, Äthiopien.
Karl Södersen 2009

zuständigen Behörde zufolge, sind derzeit ca. 60-70% der Woredas funktionstüchtig an das Netzwerk angeschlossen. Doch auch die zur Verfügung stehenden Datendienste, ursprünglich Videokonferenz, Voice over IP, E-Mail, Internet (WWW) und Datenbankzugriffe, funktionieren nur eingeschränkt. So können Videokonferenzen aufgrund falscher Hardwareinstallationen, schlechter Wartung oder zu geringer Bandbreiten nur selten genutzt werden. Die Telefoniefunktion wurde in weiten Teilen kurz nach Inbetriebnahme deaktiviert, da Mitarbeiter in den ländlichen Gebieten Telefongespräche an die Bevölkerung verkauften. Ebenso die Internetkonnektivität, die nach offiziellen Angaben eingeschränkt wurde, um die Übertragungsbandbreite für die anderen Dienste zu optimieren. Neben diesen praktischen Hindernissen und Problemen muss auch die Motivation der Regierung zur Durchführung dieses Projektes kritisch hinterfragt werden. So ermöglicht dieses System den Zugriff auf Gebiete des Landes, die zuvor für staatliche Stellen kaum erreichbar waren, weil sie beispielsweise weit abgelegen von befahrbaren Gebieten lagen. Darüber hinaus dient es, nach Angaben von BeoachterInnen, der Zentralregierung in Addis Abeba insbesondere dazu, um direkt mit den Woredas, den kleinsten Verwaltungseinheiten, zu kommunizieren und somit die mittleren Verwaltungsebenen (die *Regional Offices)*, welche teils von oppositionellen Kräften geführt werden, zu umgehen.

Ein weiteres prestigeträchtiges Projekt der äthiopischen Regierung, welches hier nur kurz beschrieben werden soll, ist das SchoolNet Projekt. Im Rahmen dieser Initiative sollen über 700 Sekundarschulen in Äthiopien ebenfalls mit einer V-SAT-Verbindung vernetzt werden. Diese, in diesem Falle nur unidirektionale, Verbindung soll dazu genutzt werden, um Bildungsinhalte auf einen in den Schulen installierten großen Plasmabildschirm zu übertragen. Neben den technischen Schwierigkeiten, die ähnlich wie bei dem Woreda-Net Projekt, auf die unzureichende Verfügbarkeit von ausgebildeten Fachkräften zurückzuführen sind, sind es vor allem konzeptionelle Hindernisse, die den Erfolg des Projektes einschränken. So sind die Bildungsprogramme in der Regel in englischer Sprache, welche von den Kindern oft nicht im ausreichenden Maße beherrscht wird. Zudem haben die Schulen und LehrerInnen keinen Einfluss auf die Programmgestaltung und -durchführung. Häufig sind sie ebenso überfordert, wie die SchülerInnen. Aufgrund der Einweg-Verbindung sind auch interaktive Inhalte oder andere Funktionalitäten wie der Zugang zum Internet nicht nutzbar. Die Kosten dieses Mamutprojektes sind enorm und stehen in keinem Verhältnis zum recht zweifelhaften Nutzen. Dieser Umstand wird besonders dadurch deutlich, dass ein vergleichbarer Nutzen mit deutlich höherer Flexibilität in der Unterrichtsgestaltung durch sehr einfache Mittel hätte erreicht werden können: Ein Fernseher, zusammen mit einem DVD Abspielgerät und einer entsprechenden Bibliothek an Datenträgern, hätte eine vergleichbare Funktionalität zu einem Bruchteil der Kosten gehabt. Offensichtlich steht bei diesem Projekt nicht die Lösung eines Problems als vielmehr der Einsatz von modernen IKTs im Mittelpunkt des Interesses. Der Bildungsforscher David Hollow, bezeichnete die SchoolNet Initiative im April 2009 auf der *Africa Gathering* Konferenz in London entsprechend als ein ICT4**P** Projekt – *Information and Communication Technology for Politics*.

Diese praktischen Beispiele machen deutlich, dass moderne Informations- und Kommunikationstechnologien keine Wunderwaffen im Kampf gegen Armut und für die Unterstützung von Entwicklungsbemühungen sind. Sie sind lediglich hilfreiche und immer mehr auch notwendige Hilfsmittel, die nur dann ihre Potenziale entfalten können, wenn sie entsprechend angepasst an die gegebenen Umständen und im Rahmen einer nachhaltig angelegten Projektkonzeption nutzenorientiert eingesetzt werden. Dies ist allerdings ein grundsätzliches Problem der Armutsbekämpfung und Entwicklungszusammenarbeit, welches auch im Zusammenhang mit IKTs bestehen bleibt und weiterhin die größte Herausforderung darstellt.

Die vollständige Masterarbeit mit den entsprechenden Quellenangaben und ausführlicheren Analysen kann unter http://www.alex-klein.net abgerufen werden.



Plasmabildschirm in einer Schule in Bahir Dar, Äthiopien.
Karl Södersen 2007

H.-Peter Neitzke, Dieter Behrendt, Silke Kleinhückelkotten, Eckhard Steinmüller & Dagny Vedder
ECOLOG-Institut für sozial-ökologische Forschung und Bildung, Hannover

Risiken allgegenwärtiger Informations- und Kommunikationstechnik

Die Informations- und Kommunikationstechnik (IKT) hat sich zu einer wirtschaftlichen Schlüsseltechnik entwickelt. Die Möglichkeiten, die immer leistungsfähigere Computer, das Internet als Zugang zu einer unfassbaren Vielfalt und Menge an Informationen, die Mobiltelefonie und viele andere IKT-Anwendungen bieten, haben darüber hinaus weitreichende Änderungen der Arbeits- und Lebenswelt herbeigeführt. Möglich wurde dies durch die rasanten Fortschritte in der Mikroelektronik und Kommunikationstechnik. Die Leistungsfähigkeit von Mikroprozessoren hat sich z.B. in den zurückliegenden 30 Jahren etwa alle 18 Monate verdoppelt. Beim UMTS-Mobilfunk, der in Deutschland im Jahr 2003 mit Probeläufen startete, sind Datenübertragungsraten möglich, die 1500-mal so hoch sind wie im analogen C-Mobilfunknetz, das seinen Betrieb im Jahr 1986 aufnahm.

Es wird allgemein davon ausgegangen, dass diese technischen Trends anhalten und dass künftig noch weitaus größere Datenmengen erfasst, übertragen und verarbeitet werden können. Die Prozessoren und andere Komponenten werden nicht nur immer leistungsfähiger, sondern auch immer kleiner und billiger. Damit wird möglich, was Anfang der 1990er Jahre noch als Vision formuliert wurde: »intelligente« Gegenstände mit eingebetteten IKT-Komponenten und eine allgegenwärtige IKT-Infrastruktur, die nicht nur die Erfassung von Daten, den Zugriff auf Informationen und eine technisch vermittelte Kommunikation zu jeder Zeit und an jedem Ort erlaubt, sondern die weitgehend selbständig Prozesse durchführt und kontextsensitiv auf Benutzerbedürfnisse1 reagiert. Hierfür wird im Folgenden das Akronym AACC (Anytime, Anywhere Communication and Computing) benutzt.

AACC ist durch die folgenden Merkmale gekennzeichnet:

- Miniaturisierung: Die IKT-Komponenten werden immer kleiner und mobiler.
- Einbettung: IKT-Komponenten sind in Geräte und Gegenstände des täglichen Gebrauchs integriert (»Smart Objects«).
- Vernetzung: Die IKT-Komponenten sind meist drahtlos miteinander vernetzt. Die Vernetzung erfolgt spontan je nach den technisch, örtlich und zeitlich gegebenen Möglichkeiten.
- Allgegenwart: Eingebettete IKT-Komponenten sind allgegenwärtig, sie versehen ihre Dienste unauffällig und weitgehend unsichtbar.
- Kontextsensitivität: Die IKT-Komponenten beschaffen sich durch drahtlosen Datenaustausch und mittels Sensoren Informationen über ihren Nutzer und ihre Umgebung und richten ihr Verhalten danach aus.

Es wird davon ausgegangen, dass AACC alle Gesellschafts- und Wirtschaftsbereiche durchdringen wird. Die folgenden kurzen Beschreibungen ausgewählter Anwendungsfelder verdeutlichen die Potentiale von AACC:

- Information und Kommunikation: AACC soll den jederzeitigen und allgegenwärtigen Zugang zu Informationen ermöglichen, Informationsangebote werden auf die spezifischen Merkmale einer Person und den situativen Kontext abgestimmt. Mit AACC soll eine technisch vermittelte Kommunikation an jedem Ort zu jeder Zeit möglich werden.
- Medizin und Gesundheitswesen: Am Körper getragene Sensoren, die medizinische Daten erfassen und an den Arzt übertragen, werden eine umfassende Überwachung des Gesundheitszustandes von Patienten erlauben. Das Monitoring gesundheitsrelevanter Aktivitäten (Bewegung, Ernährung, Genussmittelkonsum) soll neue Formen der Prävention und eine risikogerechte Beteiligung an den Krankheitskosten ermöglichen.
- Unternehmen und Arbeitswelt: Die Arbeitswelt wird sich durch AACC stark wandeln, weil viele Kontroll- und Überwachungsfunktionen von technischen Systemen übernommen und viele betriebliche Abläufe automatisiert werden können. Die jederzeitige und allgegenwärtige Verfügbarkeit von Daten, Informationen und Computerleistungen ermöglicht neue Formen der Arbeitsorganisation ohne feste Arbeitsplätze und -zeiten.
- Handel und Dienstleistungen: Durch die Kennzeichnung von Produkten mit kontaktlos elektronisch auslesbaren Etiketten (z.B. RFID-Chips) wird eine weitgehende Automatisierung in der Logistik möglich. Die Zusammenführung der Produktdaten mit allgemeinen Kundendaten, die z.B. über eine elektronische Kundenkarte oder die bargeldlose Bezahlung verfügbar sind, wird die weitgehende Erfassung von Konsumaktivitäten und damit die Erstellung umfassender Konsumentenprofile ermöglichen. Diese können von den Anbietern unter anderem für die Erstellung personen- oder kontextbezogener Angebote genutzt werden. Auch für andere Bereiche können Persönlichkeitsprofile erstellt werden, die eine gezielte Bewerbung von Kunden oder die Anpassung von Versicherungsprämien an das Risikoverhalten erlauben. Viele Bezahlvorgänge insbesondere bei kleineren Beträgen, z.B. Öffentlicher Nahverkehr und Eintrittspreise, können automatisiert werden.
- Sicherheit: Mit AACC wird es nicht nur möglich festzustellen, wo sich eine Person gerade aufhält, auch ein umfassendes Monitoring von Verhaltensweisen und eine situationsbezo-

gene Kontrolle von Aktivitäten werden möglich. Dies kann z.B. zur Verbrechensprävention und zur Fahndung genutzt werden, aber auch, um Fehlverhalten in Risikosituationen im Alltag, z.B. beim Autofahren, zu erkennen und die Betroffenen zu warnen bzw. durch technische Gegenmaßnahmen vor Schäden zu bewahren (»Elektronische Schutzengel«).

- Wohnen: AACC-Techniken können in Häusern und Wohnungen zur weitgehenden Automatisierung der Versorgungsfunktionen (z.B. Wärme, Lüftung) eingesetzt werden, aber auch um z.B. die Atmosphäre eines Raums (Beleuchtung, Musikhintergrund) oder das Fernsehprogramm an die Präferenzen des jeweiligen Nutzers anzupassen. Sensoren werden in Verbindung mit einem Haushaltsführun gscomputer automatisch erfassen, wenn Produkte des täglichen Bedarfs zur Neige gehen, und diese automatisch nachbestellen. Oder sie helfen bei der richtigen Sortierung von Abfall oder Schmutzwäsche.

Der wichtigste Treiber dieser Entwicklung sind die ökonomischen Potentiale von AACC, aber es werden auch erhebliche soziale und ökologische Chancen in dieser technologischen Entwicklung gesehen. Welchen Nutzen AACC tatsächlich entfalten wird, hängt nicht zuletzt davon ab, ob es gelingt, Risiken, die mit dieser technologischen Entwicklung verbunden sind, rechtzeitig zu erkennen und ihnen zu begegnen. In der Literatur werden bereits seit einigen Jahren einzelne Risikoaspekte von AACC diskutiert (u.a. die Abfall- und Energieproblematik, die Vulnerabilität komplexer technischer Systeme und mögliche Auswirkungen auf die Privatsphäre). Den bereits vorliegenden Untersuchungen zu den Risiken künftiger IKT ist gemein, dass nur ausgewählte Risiken betrachtet wurden und dass die Risikoanalysen überwiegend durch vergleichsweise kleine Expertengruppen mit einem recht engen fachlichen Hintergrund erfolgten. Die Diskussion über mögliche Risiken von AACC wurde zudem bisher nur in kleinen Expertenkreisen geführt. In der Öffentlichkeit wurden die Auswirkungen, die AACC in praktisch allen Lebensbereichen haben dürfte, abgesehen von einzelnen Presseberichten, bisher kaum thematisiert.

Im Rahmen des vom BMBF geförderten Programms »Sozialökologische Forschung« führt der Forschungsverbund AACC-risk im Themenschwerpunkt »Systemische Risiken« ein Projekt mit einer breiteren Zielsetzung durch. Das Projekt soll dazu beitragen,

- die mit AACC möglicherweise verbundenen ökologischen, sozialen und ökonomischen Risiken sowie insbesondere mögliche systemische Risiken unter Beteiligung von Experten unterschiedlichster Fachrichtungen aber auch von Laien zu identifizieren und zu analysieren und

- eine gesellschaftliche Auseinandersetzung mit der technologischen Entwicklung im Bereich IKT und ihren Risiken anzuregen und zu unterstützen.

Das Projekt begann im Oktober 2005 und endet im März 2010. Über einige der bereits vorliegenden Befunde wird im Folgenden berichtet.

Soziale, ökologische und ökonomische Risiken durch AACC

Ausgangspunkte der Analyse möglicher Risiken von AACC waren

- eine umfassende Literaturrecherche verbunden mit einer Befragung von Experten, um die Sicht von Wissenschaftlern und anderen Experten abzudecken, und

- Interviews mit 80 Bürgern aus unterschiedlichen sozialen Milieus (s.u.) zu ihren Einstellungen zu modernen IKT, ihren Erwartungen an zukünftige IKT und ihrer Wahrnehmung der Risiken von IKT und AACC.

Die Ergebnisse der Recherche und der Interviews flossen in die Erstellung einer Liste von 108 potentiellen Risiken durch AACC ein. Diese Liste wurde 61 Experten und Laien mit einem überdurchschnittlichen Bildungsstand zur Bewertung vorgelegt. Die Aufgabe bestand darin, für die Risiken unabhängig voneinander die Eintrittswahrscheinlichkeit des angenommenen Schadensfalls und die Höhe des im Schadensfall eintretenden Schadens einzuschätzen. Bei der Auswertung wurde die Risikobewertung dann als Produkt dieser beiden Faktoren berechnet.

In Tabelle 1 sind die Risiken aufgeführt, die von Seiten der Experten am höchsten eingeschätzt wurden. Zum Vergleich sind auch die Bewertungen durch alle Befragten und die durch die Informierten Laien aufgeführt. Hoch bewertetet wurden von den Experten vor allem Risiken, die die Privatsphäre und die Sicherheit persönlicher Daten betreffen. Hohe Bewertungen gab es auch bei Fragen der Gerechtigkeit und für die Gefahr, Opfer krimineller Aktivitäten zu werden. Bei der überwiegenden Zahl der Risiken fielen die Risikoeinschätzungen durch die Experten höher aus als die durch die informierten Laien. Nur bei zwei Risikothemen lagen die Bewertungen durch die informierten Laien deutlich höher, nämlich bei dem Risiko, dass die beim Mobilfunk verwendete elektromagnetische Hochfrequenzstrahlung Gesundheitsschäden verursacht, und bei den Risiken für Unternehmen, Regierungsstellen und Behörden, dass Unbefugte die drahtlose Datenübertragung nutzen, um sich Zugang zu deren Daten verschaffen.

Die größten Unterschiede zwischen den Risikobewertungen durch Experten und informierte Laien gab es bei dem von den Experten sehr hoch eingeschätzten Verschuldungsrisiko durch personalisierte oder auf die jeweilige Situation bezogene Konsumreize sowie bei der Einschätzung der Wirkung »Elektronischer Schutzengel«, des Monitorings gesundheitsrelevanter Aktivitäten und der permanenten Überwachung des Gesundheitszustandes von Patienten. Das Risiko, dass dies als Überwachung und/oder Entmündigung empfunden werden könnte, wurde von den Experten sehr viel höher eingeschätzt als von den informierten Laien. Weitere Risiken, bei denen die Einschätzungen durch die Experten deutlich über denen der informierten Laien lagen, beziehen sich auf die Überwachungsmöglichkeiten durch eine AACC-Infrastruktur im öffentlichen Bereich bzw. in Unternehmen.

Die größten Streuungen in den Risikoeinschätzungen durch Experten gab es bei zwei Gesundheitsrisiken, nämlich bei den

	Risiko-Einschätzung		
	Alle	**Experten**	**Inform. Laien**
Die Erfassung der Aktivitäten von Personen verletzt die Privatsphäre	16,1	19,3	15,0
Die Vernetzung ermöglicht neue Formen der Computerkriminalität im wirtschaftlichen Bereich	18,2	19,1	17,8
Die Ortung von Personen verletzt die Privatsphäre	15,2	19,1	13,4
Personalisierte oder auf die jeweilige Situation bezogene Konsumreize führen zu Ausgaben, die dem Einkommen nicht angemessen sind (Verschuldung)	13,0	18,0	11,1
Bei Stromausfällen werden weite Bereiche der Wirtschaft beeinträchtigt	15,8	17,8	14,9
Die Verfügbarkeit umfassender Konsumentenprofile führt zu Benachteiligungen von Menschen durch Banken (z.B. Kreditkonditionen)	16,7	17,6	16,3
Verlust der informationellen Selbstbestimmung: Andere können auf persönliche Daten zugreifen und sie verwenden, ohne dass die Betroffenen davon wissen	16,4	17,6	15,6
Verlust der informationellen Selbstbestimmung: Andere können auf persönliche Daten zugreifen und sie verwenden, ohne dass die Betroffenen dies beeinflussen können	15,6	17,0	14,7
Die Verfügbarkeit umfassender Konsumentenprofile führt zu Benachteiligungen von Menschen durch Versicherungen (z.B. Vertragsbedingungen und Prämien)	15,9	16,9	15,5
Die Vernetzung ermöglicht neue Formen der Computerkriminalität im Privatbereich	16,4	16,7	16,2

Tabelle 1: **Risiken mit den höchsten Einschätzungen durch Experten (90 %-Quantil)**
(möglicher Wertebereich der Risikoeinschätzungen: 1 [niedriges Risiko] bis 25 [hohes Risiko])

Schutzgüter	**Risikoeinschätzungen**	
	Experten	**Inform. Laien**
Datensicherheit	16,1	15,3
Technische Funktionssicherheit	15,6	13,4
Persönlichkeitsrechte	15,3	11,5
Gerechtigkeit	14,7	11,5
Materieller Wohlstand	14,1	11,6
Umwelt	13,4	11,0
Wirtschaftliche Leistungsfähigkeit	13,3	12,2
Kontrollierbarkeit technischer Systeme	13,1	11,7
Psychische Gesundheit	13,0	9,4
Individuelle Autonomie	12,7	8,9
Soziale Einbindung	12,1	9,5
Menschliche Fähigkeiten	10,7	8,3
Physische Gesundheit	10,1	9,5

Tabelle 2: **Einschätzung der Risiken für Schutzgüter durch Experten und informierte Laien**
(Mittelwerte der Einschätzungen aller Risiken, die das jeweilige Schutzgut betreffen)

Folgen der Exposition gegenüber der Hochfrequenzstrahlung (Funkwellen), die zur Datenübertragung sowie zur Steuerung und Vernetzung der AACC-Komponenten eingesetzt wird, und denen des körperlichen Kontakts mit AACC-Komponenten, z.B. mit implantierten Sensoren oder Chips zur Personenidentifizierung. Auch bei der Frage, ob AACC als Gesamtsystem zu einem Verlust der Kontrolle über die eigene Lebenswelt führt oder entsprechende Ängste verursacht, lagen die Experteneinschätzungen recht weit auseinander. Konkrete AACC-Anwendungen oder Anwendungsbereiche, bei denen die Risikoeinschätzungen durch die Experten stark streuten, sind der Einsatz »Elektronischer Schutzengel« und der AACC-Einsatz in Unternehmen bzw. neue Formen der Gestaltung von Arbeitsverhältnissen und -abläufen, die durch AACC möglich werden.

Die 108 in die Bewertung aufgenommenen Risiken wurden 13 Schutzgütern zugeordnet. In Tabelle 2 sind die Risikoeinschätzungen zum einen von Seiten der Experten und zum anderen von Seiten der informierten Laien für diese Schutzgüter aufgeführt. Die Schutzgüter, für die durch AACC aus Sicht der Experten die höchsten Risiken entstehen sind: Datensicherheit, technische Funktionssicherheit und Persönlichkeitsrechte. Relativ hoch fiel auch die Expertenbewertung der zum Schutzgut Gerechtigkeit formulierten Risiken aus. Die Risikobewertung durch informierte Laien ergab ebenfalls die höchsten Werte für Datensicherheit und technische Funktionssicherheit, dann folgten jedoch die Schutzgüter wirtschaftliche Leistungsfähigkeit und materieller Wohlstand. Vergleichsweise niedrig fielen in beiden Gruppen die Bewertungen bei Risiken aus, die sich auf Gefahren für die physische Gesundheit, die Entwertung menschlicher Fähigkeiten und die Schwächung sozialer Bindungen beziehen. Gesundheitsrisiken durch die bei der AACC-Vernetzung eingesetzten hochfrequenten elektromagnetischen Felder und durch den körperliche Kontakt mit AACC-Komponenten (z.B. in Form von Implantaten) waren allerdings die unter den Experten am stärksten umstrittenen Risiken (s.o.). Die Risiken für die Umwelt erreichten in beiden Gruppen mittlere Bewertungen.

Wahrnehmung der Risiken von IKT und AACC in der Bevölkerung

Parallel zu Risikoanalyse, an der Experten und informierte Laien beteiligt waren, wurde eine Repräsentativbefragung in der Bevölkerung durchgeführt. Befragt wurden 5030 Personen der deutschsprachigen Wohnbevölkerung im Alter ab 14 Jahre zu in den folgenden Bereichen:

- Besitz und Nutzung von sowie Umgang mit IKT, Bonus-Programmen und Kundenkarten
- Entwicklung/Zukunft, Chancen und Risiken von AACC
- Nutzung von und Risiken durch AACC-Einstiegstechnologien (Mobilfunk, Gesundheitskarte, RFID)
- Vertrauen in Informationen unterschiedlicher Institutionen und Informationsmedien
- Persönliche Handlungsintentionen in einer von moderner IKT durchdrungenen Welt

Das Besondere an dieser Repräsentativbefragung war die Möglichkeit, die Daten nicht nur für die Gesamtbevölkerung und, wie üblich, nach sozio-demographischen Merkmalen der Befragten, wie Alter, Geschlecht, Bildung und Einkommen, auszuwerten, sondern auch eine Differenzierung nach der Zugehörigkeit zu bestimmten sozialen Milieus vorzunehmen. Soziale Milieus sind Gruppen von Menschen, die sich in ihrer Lebensauffassung, ihren Wertprioritäten, ihren Verhaltensweisen sowie ihren alltagsästhetischen Stilen und Präferenzen ähneln. In dieser Untersuchung wurde mit den Sinus-Milieus gearbeitet. Die Sinus-Milieulandschaft wird in Westdeutschland seit 1979 kontinuierlich beobachtet, in Ostdeutschland seit Anfang der 1990er Jahre. Seit 2001 gibt es ein gesamtdeutsches Milieumodell, das aktuell zehn Milieus umfasst. Die Sinus-Milieus, die sich vier größeren Lebenswelt-Segmenten zuordnen lassen, werden anhand ihrer Wertebezogenen Grundorientierungen und ihrer sozialen Lage unterschieden (der prozentuale Anteil an der Bevölkerung ist in der Tabelle 3 jeweils angegeben):

Die Befragung ergab eine hohe Technikaffinität in den gesellschaftlichen Leitmilieus. In den Milieus der Etablierten, Postmateriellen und insbesondere dem jungen Leitmilieu der modernen Performer liegt der Ausstattungsgrad der privaten Haushalte mit moderner IKT deutlich über dem Durchschnitt. Gleiches gilt für das Lifestyle-Avantgarde-Milieu der Experimentalisten. Die mit Abstand prozentual höchsten Anteile an Intensivnutzern von Mobiltelefon und Internet finden sich in den vergleichsweise jungen Milieus der modernen Performer und Experimentalisten. Den Gegenpol bilden die traditionellen Milieus (Konservative, Traditionsverwurzelte, DDR-Nostalgische), in denen die Verfügbarkeit moderner IKT und die Intensität der Nutzung von Internet und Mobiltelefon deutlich unter dem gesellschaftlichen Durchschnitt liegen.

Die Antworten auf die Fragen zu den Risiken des Mobilfunks scheinen die Hypothese zu bestätigen, dass Technikaffinität einher geht mit einer Negierung technogener Risiken, und Technikskepsis bzw. -aversität mit einer Überbetonung der Risiken. In den Milieus der Etablierten, der modernen Performer und der Experimentalisten hält weniger als die Hälfte, bei den modernen Performern sogar deutlich weniger als die Hälfte, die dauernde Exposition gegenüber elektromagnetischer Strahlung für bedenklich. Auch bei den Hedonisten sind die, die in dieser Hinsicht Bedenken haben, in der Minderheit. In den Milieus der modernen Performer und der Experimentalisten würden, sogar wenn bewiesen wäre, dass mobiles Telefonieren gesundheitlich bedenklich ist, drei Viertel bzw. zwei Drittel der Befragten nicht auf das Mobiltelefon verzichten. Auf der anderen Seite stehen, im Einklang mit der Hypothese, die technikfernen traditionellen Milieus, in denen jeweils eine deutliche Mehrheit Bedenken wegen der dauernden Exposition gegenüber elektromagnetischer Strahlung hat. Ein zweiter Blick zeigt aber, dass der Zusammenhang zwischen Technikaffinität bzw. -aversität und der Wahrnehmung technogener Risiken nicht so einfach ist: Im Milieu der Postmateriellen sind die neuen Technologien weiter verbreitet als im Bevölkerungsdurchschnitt (s.o.), zugleich ist aber auch das Bewusstsein für mögliche Risiken überdurchschnittlich ausgeprägt. Mehr als zwei Drittel der Befragten aus diesem Milieu hält die allgegenwärtige Exposition gegenüber elektromagnetischer Strahlung für bedenklich. Noch höher als bei den Postmateriellen ist der Anteil der Besorgten in der bürgerlichen Mitte, die ebenfalls nicht zu den technikskeptischen Milieus zu rechnen ist. Hier würde aber, selbst wenn es gesundheitlich riskant wäre, eine deutliche Mehrheit nicht auf die Nutzung eines Mobiltelefons verzichten.

Gesellschaftliche Leitmilieus	
Etablierte ETA (10 %)	Grundorientierung: Das selbstbewusste Establishment: Erfolgs-Ethik, Machbarkeitsdenken und ausgeprägte Exklusivitätsansprüche Soziale Lage: überdurchschnittlich hohes Bildungsniveau; hohe und höchste Einkommen; hoher beruflicher Status
Postmaterielle PMA (10 %)	Grundorientierung: Das aufgeklärte Nach-68er-Milieu: Liberale Grundhaltung, postmaterielle Werte und intellektuelle Interessen Soziale Lage: hohe bis höchste Bildungsabschlüsse; hohe und höchste Einkommen; höhere Angestellte, Beamte, Freiberufler, Studenten
Moderne Performer PER (10 %)	Grundorientierung: Die junge, unkonventionelle Leistungselite: Intensives Leben – beruflich und privat, Multi-Optionalität, Flexibilität und Multimedia-Begeisterung Soziale Lage: hohes Bildungsniveau; z. T. noch bei den Eltern lebend oder gehobenes eigenes Einkommen; Schüler / Studenten, Selbständige, Freiberufler
Traditionelle Milieus	
Konservative KON (5 %)	Grundorientierung: Das alte deutsche Bildungsbürgertum: Konservative Kulturkritik, humanistisch geprägte Pflichtauffassung und gepflegte Umgangsformen Soziale Lage: hohes Bildungsniveau; mittlere bis gehobene Einkommen, teilweise hohes Vermögen; hoher beruflicher Status (vor dem Ruhestand)
Traditionsverwurzelte TRA (14 %)	Grundorientierung: Die Sicherheit und Ordnung liebende Kriegs- / Nachkriegsgeneration: Verwurzelt in der kleinbürgerlichen Welt bzw. in der traditionellen Arbeiterkultur Soziale Lage: eher niedriges Bildungsniveau: überwiegend Haupt- bzw. Volksschulabschlüsse; kleine bis mittlere Einkommen; hoher Anteil von Rentnern und Pensionären
DDR-Nostalgische DDR (5 %)	Grundorientierung: Die resignierten Wende-Verlierer: Festhalten an preußischen Tugenden und altsozialistischen Vorstellungen von Gerechtigkeit und Solidarität Soziale Lage: einfache bis mittlere Bildungsabschlüsse, auch Hochschulabschlüsse; kleine bis mittlere Einkommen; einfache Angestellte, (Fach-)Arbeiter und Arbeitslose
Mainstream-Milieus	
Bürgerliche Mitte BÜM (15 %)	Grundorientierung: Der statusorientierte moderne Mainstream: Streben nach beruflicher und sozialer Etablierung, nach gesicherten und harmonischen Verhältnissen Soziale Lage: qualifizierte mittlere Bildungsabschlüsse; mittlere Einkommen; einfache und mittlere Angestellte und Beamte, Facharbeiter
Konsum-Materialisten MAT (12 %)	Grundorientierung: Die stark materialistisch geprägte Unterschicht: Anschluss halten an die Konsumstandards der breiten Mitte als Kompensationsversuch sozialer Benachteiligungen Soziale Lage: niedrige Bildungsabschlüsse; niedrige und mittlere Einkommen; überdurchschnittliche viele Arbeiter, Facharbeiter, Arbeitslose
Hedonistische Milieus	
Experimentalisten EXP (8%)	Grundorientierung: Die extrem individualistische neue Bohème: Ungehinderte Spontaneität, Leben in Widersprüchen, Selbstverständnis als Lifestyle-Avantgarde Soziale Lage: gehobene Bildungsabschlüsse; viele noch ohne eigenes Einkommen; Angestellte, Selbständige, Freiberufler, Jobber, Schüler, Studenten, Auszubildende
Hedonisten HED (11%)	Grundorientierung: Die spaßorientierte moderne Unterschicht / untere Mittelschicht: Verweigerung von Konventionen und Verhaltenserwartungen der Leistungsgesellschaft Soziale Lage: einfache und mittlere Bildungsgrade, viele noch ohne eigenes Einkommen; einfache Angestellte, Arbeiter, Schüler, Auszubildende

Tabelle 3: **Die Sinus-Milieulandschaft** *(prozentualer Anteil an der Bevölkerung)*

Der auffälligste Befund in den Befragungsergebnissen zur Wahrnehmung der Chancen bzw. der Risiken zukünftiger Entwicklungen in Richtung allgegenwärtiger Informations- und Kommunikationstechnologien ist, dass Mehrheiten in der Bevölkerung Vorteile von AACC erwarten, dass es zugleich aber eine weit verbreitete Skepsis oder sogar Angst vor den Möglichkeiten gibt, die mit AACC kommen werden. Jeweils mehr als zwei Drittel der Bevölkerung erwarten, dass AACC zu einer höheren Informiertheit und einer größeren Vielfalt menschlicher Kontakte führen wird. Auch in der Vermeidung menschlicher Fehler durch Technik und die Beschleunigung demokratischer Verfahren werden von deutlichen Mehrheiten Chancen gesehen. Auf der anderen Seite teilen jeweils mehr als drei Viertel der Befragten die Befürchtungen, dass das Alltagsleben immer anfälliger für technische Störungen wird, dass die Bürger immer stärker kontrolliert werden und Personengruppen, die mit der technischen Entwicklung nicht mithalten können, benachteiligt werden (s. Tabelle 4). Diese Risiken wurden auch von den Experten hoch eingeschätzt (s.o.). Von deutlichen Mehrheiten werden zudem eine Entmündigung des Menschen und negative kulturelle Auswirkungen erwartet. Auch dass der Umwelt von AACC erhebliche Gefahren drohen, wird von einer deutlichen Mehrheit in der Bevölkerung gesehen.

Bei der Wahrnehmung der Chancen und der Risiken von AACC zeigen sich hinsichtlich der Ausprägung in den sozialen Milieus die bereits bei den modernen IKT beobachteten Pole: Auf der einen Seite gibt es hohe positive Erwartungen bei gleichzeitig unterdurchschnittlichem Risikobewusstsein in den Milieus der Etablierten und der modernen Performer. Dieses Einstellungsmuster ist auch, wenngleich nicht so stark ausgeprägt, bei den Experimentalisten festzustellen. Auf der anderen Seite sind in den traditionellen Milieus eine deutlich geringere Wahrnehmung der Chancen und eine starke Betonung der Risiken zu beobachten. Postmaterielle und Bürgerliche Mitte liegen hinsichtlich der Wahrnehmung der Chancen meist über dem Durchschnitt, weisen zugleich aber auch ein stärker ausgeprägtes Risikobewusstsein auf. Bei den Hedonisten fällt auf, dass der Anteil derer, die an AACC positive Erwartungen knüpfen, weitgehend im Durchschnitt liegt, dass sie mögliche Risiken aber überdurchschnittlich häufig ausblenden.

Die Ambivalenz der Einschätzungen der mit AACC zu erwartenden Entwicklungen belegen auch die in Tabelle 5 wiedergegebenen Haltungen zu AACC: Für zwei Drittel der Befragten überwiegen die Vorteile, die AACC bieten wird. Nahezu genauso viele geben aber auch an, dass sie ein ungutes Gefühl haben bei dem, was sie auf sich zukommen sehen.

	Bev.	ETA	PMA	PER	KON	TRA	DDR	BÜM	MAT	EXP	HED
	%	%	%	%	%	%	%	%	%	%	%
Gesamt	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0
Unser Leben wird immer anfälliger sein für technische Störungen	81,3	71,3	86,8	59,7	90,2	93,5	93,8	86,1	84,6	82,1	68,5
Das Verhalten der Menschen wird immer mehr kontrolliert	80,5	71,3	87,0	59,9	90,3	93,8	96,6	90,6	83,7	79,5	55,4
Personen, die mit Technik nicht umgehen können, werden ausgegrenzt	78,4	70,9	82,8	73,1	81,3	83,1	88,8	89,6	80,1	71,5	60,9
Die Menschen werden sich so sehr auf die Technik verlassen, dass sie die Fähigkeit zur eigenen Entscheidung verlieren	66,9	53,7	62,6	43,4	78,3	80,5	87,0	77,0	73,6	67,8	50,3
Herstellung, Transport und Betrieb der IKT-Geräte werden bleibende Schäden an der Umwelt verursachen	59,2	48,5	51,8	39,5	65,0	74,8	72,3	67,6	59,2	59,4	53,6
Ich befürchte, dass eine vernetzte IKT sehr viel Energie verbraucht	57,0	46,8	45,3	40,6	68,3	73,0	70,4	67,0	58,4	54,6	46,7
Die zunehmende Technisierung des Alltags bedroht unsere Kultur	54,5	43,5	54,8	26,4	67,8	75,4	74,3	58,5	54,4	54,1	42,8

Tabelle 4: **Wahrnehmung der Risiken allgegenwärtiger IKT (AACC)**
(Antwortvarianten »stimmt ganz genau« und »stimmt eher«)

	Bev.	ETA	PMA	PER	KON	TRA	DDR	BÜM	MAT	EXP	HED
	%	%	%	%	%	%	%	%	%	%	%
Gesamt	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0
Alles in allem bringt uns die weltweite Vernetzung mehr Vorteile als Nachteile	67,6	84,7	68,1	92,4	58,2	41,5	61,1	75,1	62,2	69,9	62,8
Ein durch Technik perfekt funktionierender Alltag wäre mir unheimlich	65,2	52,6	71,1	28,1	78,7	87,6	83,5	73,4	72,2	54,6	50,1
Ich habe ein ungutes Gefühl, was da auf uns zukommt	59,9	45,8	56,3	29,1	76,9	81,7	80,7	67,0	63,5	51,6	51,8

Tabelle 5: **Haltung gegenüber AACC**
(Antwortvarianten »stimmt ganz genau« und »stimmt eher«)

Ausblick

Die bisher aus dem Forschungsprojekt vorliegenden Befunde zeigen, dass mit der Realisierung von AACC erhebliche Risiken verbunden sein können, insbesondere im Hinblick auf

- die Sicherheit der Daten von Privatpersonen, öffentlichen Stellen und Unternehmen
- die Funktionssicherheit immer komplexer werdender technischer Systeme
- den Erhalt der Privatsphäre und die Wahrung von Persönlichkeitsrechten
- die gleichberechtigte Teilhabe aller Bürgerinnen und Bürger am gesellschaftlichen Leben und dem materiellen Wohlstand
- die Verfügbarkeit von Ressourcen und den Erhalt der Umwelt.

Aus den Ergebnissen der Repräsentativbefragung in Verbindung mit psychologischen Analysen ist zudem zu schließen, dass gut zwei Drittel der Bevölkerung den sich durch AACC abzeichnenden Entwicklungen skeptisch oder sogar mehr oder weniger hilflos gegenüber stehen. Vor diesem Hintergrund erscheint ein breiter gesellschaftlicher Dialog darüber notwendig, welche Entwicklungen, die AACC möglich macht, tatsächlich angestrebt werden sollen, wie die dazu erforderlichen Techniken zu gestalten sind, welche rechtlichen Rahmensetzungen notwendig sind und wie Bürgerinnen und Bürger zu einem kompetenten Umgang mit den neuen Techniken befähigt werden können. Der Schwerpunkt der Arbeiten in der zweiten Phase des Projekts lag und liegt deshalb auf

- der Erarbeitung von Empfehlungen für Vorsorgestrategien im Zusammenhang mit AACC in ausgewählten Anwen–dungsbereichen unter Beteiligung von Bürgern und Exper–ten sowie ihrer Vermittlung an Politik, Wissenschaft und IKT-Wirtschaft
- die Entwicklung eines Konzepts für eine zielgruppengerechte Risikokommunikation im Zusammenhang mit AACC
- der Unterstützung eines öffentlichen Dialogs über die Perspektiven von AACC und die damit verbundenen Risiken.

Autoren

Alle Autorinnen und Autoren sind Mitarbeiterinnen und Mitarbeiter des ECOLOG-Institut für sozial-ökologische Forschung und Bildung in Hannover (*mailbox@ecolog-institut.de*). H.-Peter Neitzke ist promovierter Physiker und Wissenschaftlicher Leiter des Instituts und Geschäftsführer seit 1991, Dieter Behrendt ist Diplom-Geograph (Wirtschaftsgeographie) und Wissenschaftlicher Mitarbeiter seit 1998, Silke Kleinhückelkotten ist promovierte Kulturwissenschaftlerin, wissenschaftliche Mitarbeiterin seit 1998 und stellvertretende Geschäftsführerin seit 2005, Ekhard Steinmüller ist Diplom-Soziologe und Wissenschaftlicher Mitarbeiter seit 2008 und Dagny Vedder ist Diplom-Soziologin (Techniksoziologie) und Wissenschaftliche Mitarbeiterin seit 2008.

Literatur

Ausführliche Beschreibungen der Vorgehensweise, Darstellungen der Ergebnisse sowie Hinweise auf die einschlägige Literatur finden sich in den folgenden Arbeiten:

Behrendt D., Kleinhückelkotten S., Neitzke H.-P. & Wegner E. 2007: Identifizierung und Bewertung der Risiken ubiquitärer Informations- und Kommunikationstechnologien (AACC) durch Experten und informierte Laien. AACCrisk Report 1/2007

Moser S. & Bruppacher S. 2008: Menschliches Handeln als Ursache von und Bewältigungsmöglichkeit der Risiken ubiquitärer Informations- und Kommunikationstechnologien. Arbeitsbericht, IKAÖ, Universität Bern

Plöger W. 2008: Anytime, Anywhere Communication and Computing (AACC): Wahrnehmung von Risiken und Ansprüche an die Risikokommunikation in strategischen Zielgruppen. Befunde der qualitativen Untersuchung (Fokusgruppen). Arbeitsbericht, Sinus Sociovision Heidelberg

Wippermann C., Calmbach M. & Wippermann K. 2008: Anytime, Anywhere Communication and Computing (AACC). Eine bevölkerungsrepräsentative Untersuchung zur Wahrnehmung von Chancen und Risiken allgegenwärtiger und alltagsdurchdringender ICT vor dem Hintergrund der Sinus-Milieus. Arbeitsbericht, Sinus Sociovision, Heidelberg

Wippermann C., Calmbach M., Wippermann K., Bruppacher S., Moser S., Kleinhückelkotten S. & Neitzke H.-P. 2008: Wahrnehmung der Chancen und Risiken allgegenwärtiger Informations- und Kommunikationstechnologien in der Bevölkerung. AACCrisk Report 1/2008

Neitzke H.-P., Calmbach M., Behrendt D., Kleinhückelkotten S., Wegner E. & Wippermann C. 2008: Risks of Ubiquitous Information and Communication Technologies. GAIA 17(4): 362–369

Dank

Die Autoren danken den Kollegen im Forschungsverbund AACCrisk für die Zusammenarbeit und spannende Diskussionen: Dr. Susanne Bruppacher und Stephanie Moser von der Interfakultären Koordinationsstelle für Allgemeine Ökologie IKAÖ der Universität Bern, die im Rahmen des Vorhabens psychologische Fragestellungen bearbeiteten, Marc Calmbach, Wolfgang Plöger, Dr. Carsten Wippermann und Katja Wippermann, die qualitative sozial-wissenschaftliche Untersuchungen und die Repräsentativbefragung durchführt haben, sowie den Kollegen im ECOLOG-Institut Dr. Julia Osterhoff, Dr. Hartmut Voigt und Elisabeth Wegner für ihre Unterstützung bei den Risikoanalysen. Ein besonderer Dank gilt auch den Mitgliedern des Beirats, der das Vorhaben begleitete, und dem BMBF für die finanzielle Förderung.

Endnotes

1 *In diesem Text werden, wo immer es möglich ist, geschlechtsneutrale Formulierungen verwendet. Wo es von der Sache her geboten ist, wird explizit die weibliche oder männliche Form benutzt. An anderen Stellen folgt die Wortwahl um der besseren Lesbarkeit willen den allgemeinen sprachlichen Konventionen. Aus Sicht der Autoren bedeutet dies keine Geringschätzung der Rolle von Frauen in Gesellschaft und Wissenschaft.*

Viola Bräuer

Kritischer Wissensaufbau oder Wissen als Entity-Relation zwischen Infohäppchen

„Wissen ist Macht und nichts Wissen macht nichts" alter Spruch aus der Schule, gebraucht vor Prüfungen. Wir wandeln uns von einer Informationsgesellschaft zu einer Wissensgesellschaft und wir wissen nicht, was das ist. Hat das was mit Computern zu tun und mit Internet und mit viel Wissen? Oder mit immer genau das wissen, was gerade gefragt ist: Wikipedia und Google hilf!
Dieser Artikel will dem Begriff Wissen auf die Spur kommen, ihn in Relation setzen zu den Begriffen Nachricht, Information, Weisheit und Vernunft und so einen zugegebenermaßen subjektiven Sinn schaffen.

Informationsquellen

Neben Wikipedia und Google, kann mensch auch seinen Mitmenschen fragen, in Büchern lesen, Vorträgen zuhören, selbst Beobachtungen anstellen, eigene Erfahrungen ernst nehmen und selbst Schlüsse daraus ziehen.

Abhängig von der Informationsquelle variiert die Zuverlässigkeit der Information – es ist eben nicht alles richtig, was mensch bei Google findet. Die Medien zeigen, was sie zeigen sollen und wollen, nicht was mensch hofft, darin zu finden. Nicht ohne werden Medien auch als vierte Macht im Staat bezeichnet und auch manche Mitmenschen besitzen die Gabe, Informationen so zu verpacken, das damit bestimmte Gedanken, Vorstellungen, Wünsche und Handlungen beim Empfänger ausgelöst werden. Kritische Informationsaufnahme ist jedoch nicht immer möglich. In einem Trancezustand, wie er leicht beim Fernsehschauen oder bei einer Meditation eintritt, wird das kritische Bewusstsein geschwächt und empfangene Informationen können ungehindert das Gehirn passieren.

Nachricht, Information, Wissen

Bevor eine Information zu uns kommt, liegt sie als Nachricht vor. Irgendeine Folge von Bits, eine Menge von Ereignissen, was auch immer, das an einer Person oder an einen Prozess gesendet wird. Eine Nachricht ist ein Datenstrom, der an eine bestimmte Entität, an einen bestimmten Empfänger gerichtet wird.

Ob diese Nachricht verstanden wird, hängt von der Entität ab. Ich will eine Nachricht, die für den Empfänger deutbar ist als Information bezeichnen. Als Beispiel ist eine verschlüsselte Email eine Nachricht, aber im verschlüsselten Zustand stellt sie für den Empfänger keine Information dar. Das sagt ihm schlicht nichts.

Kommt die Nachricht inhaltlich an, wird also bei Empfänger zu Information, so obliegt der Empfänger mitunter der Versuchung, die neuen Nachricht mit bereits Bekanntem zu verknüpfen.

Passiert das öfters mit ähnlichen Informationen, so häufen sich die Informationen zu einem bestimmten Themengebiet und mit der Anzahl der Verknüpfung der einzelnen Informationshäppchen entsteht Wissen zu dem bestimmten Thema.

Wissen um etwas

Das Wissen sich um eine Themengebiet herum ansammelt, hängt mit der Wichtigkeit der Verknüpfung der Informationen zusammen. Zusammenhänge zwischen den einzelnen Informationen herstellen, Ursachen, Wirkungen, Wechselwirkungen und Widersprüche aufdecken, gehört zum Verknüpfen der Informationen, die dann in einem Beziehungskontext zueinander stehen.

Besonders die Widersprüche. Nichts ist für einen menschlichen Geist spannender als Widersprüche. Er will sie lösen. Widersprüche sind für den Geist wie Konflikte für eine Gesellschaft – unvermeidbar, störend und Triebfeder zugleich. Dadurch werden, wenn das Wissensgebiet für den Geist interessant ist, mit der Zeit immer mehr Informationen gesammelt und sie werden immer mehr verknüpft und strukturiert.

Viola Bräuer

Viola Bräuer, CISSP, CISA, CISM, ist seit 2001 selbständige Beraterin für IT-Security Management. Ihr Schwerpunkt liegt im Spannungsfeld zwischen Verfügbarkeit, Vertraulichkeit, Integrität und Nicht-Abstreitbarkeit von Informationen und deren organisatorische und technische Realisierung in Großunternehmen.

Zudem ist sie im Prüfungsausschuss der IHK München und Oberbayern u.a. für die Berufe Fachinformatikerin und Fachinformatiker.

Ist ein Wissensgebiet erst einmal ansatzweise erfasst, das bedeutet, es sind innerhalb einer hinreichenden Menge von Informationen genügend Verknüpfungen erstellt worden, so können weitere Informationen durch logisches Schließen gewonnen werden. Das logische Schließen ist das bewusst machen der Informationen, die „zwischen den Zeilen" des bereits Vorhanden liegen. Diese Informationen stecken in den Relationen der Informationen, ihren Abhängigkeiten und Wechselwirkungen.

Aus dem logischen Schließen innerhalb eines Wissensgebiets kann Abstraktion erfolgen, die wiederum in ähnlichen Wissensgebieten angewandt werden kann. Durch Abstraktion und Deduktion können Schlussfolgerungen, die auf einem Gebiet gezogen werden, in ein anderes Gebiet übertragen werden. Das Gebiet, auf das sich Wissen bezieht ist somit sehr weit gefasst.

Das ist so wie Go-Spielen; aus der eigenen Mitte heraus in neue Gebiete vordringen. Beides setzt voraus, zumindest etwas richtig verstanden zu haben, zumindest ein Gebiet wirklich erobert und sich angeeignet zu haben – halt das Gegenteil von Oberflächlichkeit.

Neuronen und Beziehungen

Der Aufbau von Wissen im menschlichen Gehirn lässt sich schön mittels Neuronen beschreiben. Das Gehirn besteht aus einer Vielzahl von Neuronen. Jedes Neuron ist Träger kleinster Informationseinheiten und ist mit anderen Neuronen verbunden. Neuronen können gleichzeitig agieren, das Gehirn ist also ein massiver Parallelrechner. Jeder Gedanke hangelt sich durch unzählige Neuronen hindurch um von einer staubigen Wolke zu einem ausgesprochen Satz zu werden. Und wie bei einem Strassen- oder Eisenbahnnetz besteht die Stärke eines neuronalen Netzes in der Menge , der Qualität und der Sinnhaftigkeit der Verknüpfung.

Das menschliche neuronale Netz kann vereinfacht durch maschinelle neuronale Netze siwerden, die Entscheidungen aufgrund von Gelerntem treffen können.

Schlussfolgerungen aus mehreren Datenquellen ziehen... ... können Computer auch

Entscheidungen können Computer auch aufgrund von Datenbanken treffen, in denen Daten strukturiert abgelegt sind. Auch hier ist die Art der Verknüpfung entscheidend für die Möglichkeit der späteren Nutzung. Man erinnere sich an Datenbankmodellierung und das Aufdröseln von n:m-Beziehungen. Und wehe, wenn sich später herausstellte, dass das Design Mist war.

Die Daten einer Datenbank können miteinander korreliert werden, die gefundenen Beziehungen der Daten untereinander stellen weitere Informationen dar; ähnlich wie dem menschlichen Korrelieren von Informationen. Bei Datenbanken heißt das Data mining; oder, weitergehend, das Data warehouse, das Informationen von mehrere Datenbanken sammelt und diese wiederum korrelliert in einem Data mart ablegt. Das Data mart ist somit eine Informationssammlung aus mehreren Datenbanken die mittels Relationen verknüpft sind.

Ein menschliches Data mart entsteht wenn ein Mensch Informationen aus unterschiedlichen Quellen miteinander verknüpft. Mein Großvater schaute in den Zeiten des kalten Krieges immer zwei Nachrichten: „Aktuelle Kamera", die Nachrichtensendung aus dem DDR-Fernsehen und anschließend „Heute" im ZDF. Wie bereits oben im Abschnitt Datenquellen erwähnt, sind Widersprüche normal und kritisches Bewusstsein gefragt.

Ressourcenverbrauch: Energie und Zeit

Der Begriff Wissen geht wie hier beschrieben über das reiner Faktenwissen hinaus. Reines Faktenwissen stellt ausschließlich eine Sammlung von Informationen dar. Wissen setzt das Vorhandensein von Zugriffsmöglichkeiten auf entsprechende Informationen voraus, beinhaltet aber zusätzlich die Fähigkeit zur Verknüpfung derselben. Also eins und eins zusammen zu zählen. Die Anzahl möglicher Schlussfolgerungen wächst expotentiell mit der zur Verfügung stehenden Informationsmenge.

Andere nötige Ressourcen sind Energie und Zeit; das gilt sowohl für das Data mart als auch für den Kopf; Denken nimmt viel Energie in Anspruch – nicht zu Unrecht gilt Schach spielen als Sportart-. Allein der „Betrieb" eines menschlichen neuronalen Netzes ist energetisch aufwendig.

Das logische Schließen benötigt Zeit, da die sinnvollen Relationen zu einer Menge von Informationen „abgegrast" werden müssen. Wie effizient dabei eine Datenbank oder ein menschliches Gehirn ist hängt unter anderem von der Anordnung der Informationen ab; also welche Information mit welcher verknüpft ist / welches Neuron mit welchen anderen beziehungsweise wie das Datenschemata der Datenbank aussieht/ welche Relationen zwischen den Tabellen definiert sind. Und wie bei der Datenbank fließt in das Design der Relationen die am weitesten reichende Arbeit. Das anschließende Füttern mit Datensätzen ist eher stupide. Dagegen braucht das Finden eines „roten Fadens" aus einem Wust von gelesenem Material seine Zeit. Das diese Zeit dann nicht mit stupidem Auswendiglernen vertan werden kann, liegt auf der Hand. Der Umkehrschluss gilt genauso: Wenn keine Zeit zum Nachdenken vorhanden ist, nützt das ganze schöne „data mart" nix.

Versuch einer Definition: Wissen

Wissen ist die Fähigkeit aus einer Menge von Informationen durch Bildung geeigneter Relationen im Vorfeld unbekannte Fragestellungen zu beantworten. Also ungefähr das, was einem in einer Prüfung abverlangt wird.

Wissen ist gefährlich

In der Prüfung kommt die Fragestellung von außen. Die Fragestellung kann bei Menschen auch von innen kommen. In dem Moment, wo ein Mensch selbständig entscheidet, worüber sie nachdenkt und welche Informationen sie sich dafür verschafft, ist das Ergebnis nicht mehr vorhersagbar.

Wissen und Vernunft

Der Sinn des Wissens ist die Beantwortung von Fragestellungen. Dazu hilft eine schnelle Auffassungsgabe, die eine in die Lage versetzt, rasch praktischen Gebrauch von Dingen zu machen- zum Beispiel ein technisches Gerät oder eine Software nach dem benötigten Feature abzuscannen oder herauszubekommen wo das Gesuchte in der neuen Word-Version steckt. Wissen ist auf praktische Ziele hin orientiert.

Hingegen ist Vernunft umfassender (ich benutze den Begriff Vernunft von Erich Fromm („Den Menschen Verstehen, Psychoanalyse und Ethik", Deutscher Taschenbuchverlag, 7. Auflage Januar 2005, Seite 86). Vernunft will zum Wesen der Dinge vordringen, „ihre verdeckten Zusammenhänge, ihren tieferen Sinn" ergründen. Die Zusammenhänge erkennt ein Data mart, den Sinn nicht.

Weiter bei Fromm: „ Sie (die Vernunft Anm. d. A.) hat die Aufgabe, etwas zu wissen, zu verstehen, zu erfassen und den Menschen durch dieses Begreifen zu den Dingen in Beziehung zu setzen." Der letzte Aspekt, das In-Beziehung-Setzen zwischen Mensch und dem Objekt des Interesses ist meiner Meinung nach der wesentliche Unterschied zwischen einem Data mart und einem Menschen. Ein Data mart kann kein Verhältnis aufbauen zwischen sich und den gespeicherten Daten; es kann keine Nächte durchdiskutieren, kann nicht leidenschaftlich studieren und sich selbst immer wieder zu fragen – es kann sich nicht einer Sache hingeben und es kann dem Wissen keinen Sinn geben. Und vor allem kann das Data mart das Objekt seines Wissen nicht selbst bestimmen. Die Unterschied zwischen Wissen und Vernunft liegt demnach in der Vergabe von Sinn, der abhängig ist von der Beziehung Wissender und Wissensgebiet. Mit allen Sinnen bei der Sache sein, erleichtert den Erwerb von Wissen ungemein (und mensch bekommt die damit verbrachte Zeit nicht mehr mit).

Wissen und Weisheit

Wenn Wissen, wie oben dargestellt, das Schlussfolgern von bereits bestehenden Fakten beinhaltet, so ist Weisheit mehr das Vorhersagen von Unbekanntem auf Basis von Erfahrung. Die Erfahrung ist im Prinzip auch Wissen, das vielleicht auf anderen Gebieten gesammelt wurde und durch Abstraktion und Deduktion auf die scheinbar völlig andere Situation angewandt wird. Erfahrungswissen verfügt im Gegensatz zu Auswendiggelerntem über eine subjektiv vertrauenswürdige Quelle. Und es umfasst im Gegensatz zu logisch Geschlussfolgertem auch die Prämissen, die in die theoretische Betrachtung nicht einflossen.

Die Begriffe Vernunft (das Wesen einer Sache erfassen) und Weisheit bedingen sich. Ich muss das Wesen einer Sache erfassen um Aussagen über deren zukünftiges Verhalten machen zu können.

Zusammenfassung und Fazit

Die Verknüpfung von Fakten zu Wissen über ein Gebiet braucht Zeit und Energie. Ein über Relationen verknüpftes Informationsnetz lässt Schlussfolgerungen und damit die Beantwortung konkreter Fragen zu dem Wissensgebiet zu. Bei Computern heißt das Data mining oder auch Data mart, je nach Menge der Informationsquellen.

Verschiedene Informationsquellen miteinander verknüpfen und Korrelationen zwischen den Informationen erstellen können Mensch und Maschine. Sich seinen eigenen Senf dazu zu denken, das Objekt des Interesses selbst auszusuchen, das Wesen einer Sache zu erkennen, zu ihr eine Beziehung aufzubauen und Sinn zu stiften ist eine rein menschliche Angelegenheit.

Wolfgang Coy

Rechnen, Denken, lebenslange Bildung

Am Ende von Wittgensteins Tractatus logico-philosophicus, nachdem er das menschliche Erkenntnisvermögen vom Reich der Objekte auf sprachliche Aussagen über die Welt und das Räsonnement über diese Aussagen zurückführt hat, steht unter 6.52 die gern überlesene Bemerkung ›Wir fühlen, dass selbst, wenn alle möglichen wissenschaftlichen Fragen beantwortet sind, unsere Lebensprobleme noch gar nicht berührt sind. Freilich bleibt dann eben keine Frage mehr; und eben dies ist die Antwort.‹

*

Alan Mathison Turing steht nicht nur als Cambridge-Absolvent der sprachlichen Wende Wittgensteins sehr nahe. Er nähert sich dem Denken von der Seite der Berechenbarkeit und verschiebt den linguististic turn zum Begriff der Berechenbarkeit hin. Rechnen wird bei Turing anders als bei anderen gleichzeitig formulierten formalen Kalkülen der Berechenbarkeit durch die Tätigkeit eines menschlichen Rechners mit Bleistift, Radiergummi und Karopapier beschrieben. Wir können uns ein Schulkind bei seinen Rechenaufgaben vorstellen. Zu jedem Zeitpunkt ist dieser menschliche Rechner in einem von einigen möglichen ›Arbeitszuständen‹. Betrachtet wird nur ein einziges Karokästchen, in dem ein wohlvertrautes Zeichen aus einem endlichen Vorrat steht. Im Kopf ist eine algorithmische Anweisung, eine von ein paar Anweisungen, was jetzt zu tun sei: Ob das Zeichen durch ein anderes ersetzt wird oder ob das rechts oder das links anschließende Kästchen zu bearbeiten sei, oder ob die Rechnung zu Ende gekommen ist. Eine schlichte Vorstellung, die gleichwohl alles ›Rechnen‹ vollständig beschreiben soll. ›It is my con-

tention that these operations include all those which are used in the computation of a number.‹ Turing nennt dieses wohlerzogene rechnende Schulkind paper machine.

Turings Weltbild war vom allgemeinen Stand der Wissenschaften geprägt, soweit sie Mathematikern vertraut war, in den engen Ansätzen der formalen Logik, die sich zu dieser Zeit sehr stark auf das Hilbertsche Grundlagenforschungsprogramm konzentrierten, also die Forderung nach Vollständigkeit, Widerspruchsfreiheit und Entscheidbarkeit axiomatischer Kalküle. Sein Biograf Andrew Hodges hat dies sehr schön auf den Punkt gebracht, als er darauf hinwies, für den ganz jungen Alan sei ›Natural Wonders every Child Should Know‹, das wichtigste Buch gewesen, eine schlichte Popularisierung und Reduktion aller Naturwissenschaften auf die Mechanik.1

Vor diesem Hintergrund wird deutlich, dass Turing zwei Vorstellungen pflegt:

- Alles Denken ist formal und symbolisch als Schlussfolgern beschreibbar (was mit geeignetem Programm von seiner paper machine als Rechnung ausführbar wäre).

- Aus Gründen der endlichen molekularen Struktur der Gehirns lässt sich alles Schlußfolgern in finiten Kalkülen beschreiben. Bei Turing heißt es dazu knapp: ›For the present I shall only say that the justification lies in the fact that the human memory is necessarily limited.‹2 Turings Überlegungen bleiben dabei etwas vage. Roger Penrose spitzt dies m.E. angemessen zu: ›It seems likely that he [Turing] viewed physical action in general — which would include the action of a human brain — to be always reducible to some kind of Turing-machine action.‹3 Andrew Hodges nennt die die Turing-These (im Unterschied zur Church-Turing These).

Er folgt damit dem Wittgensteinschen Programm des Tractatus, ohne sich explizit darauf zu beziehen – und ohne die kritischen Zweifel, die Wittgenstein in den Jahrzehnten nach der Erstveröffentlichung quälten. Turing interessiert sich mehr für die Frage, wie weit seine paper machines gehen können. In seinem 1950 für ein philosophisch interessiertes Publikum geschriebenen Aufsatz ›Computing machinery and intelligence‹ schlägt er einen Wettbewerb zwischen Mensch und Maschine vor, um die Leistungsfähigkeit ›Intelligenter Programme‹ zu testen. Der Aufsatz endet mit: ›We may hope that machines will eventually compete with men in all purely intellectual fields. But which are the best ones to start with? Even this is a difficult decision. Many people think that a very abstract activity, like the playing of chess would be best. It can also be maintained that it is best to provide the machine with the best sense organs that money can buy, and then teach it to understand and speak English. This process could follow the normal teaching of a child. Things would be pointed out and named, etc. Again I do not know what the right answer is, but I think both approaches should be tried.‹

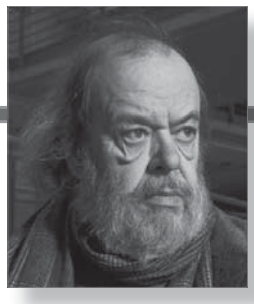
Mit ähnlicher Unbekümmertheit haben John McCarthy und Marvin Minsky diese Vorgehensweise fortgeführt, als sie 1956 auf der berühmten Dartmouth-Conference ein Forschungsprogramm zur künstlichen Intelligenz verkündeten, dessen philosophische Höhenflüge bis heute wenig ergiebig sind, wobei die vorherrschenden Denkfiguren sich von Dekade zu Dekade wandeln - vom Turingtest zum Schachspiel, vom Schachspiel zum Sprachverstehen, vom Sprachverstehen zur Robotik, von Robotern zur Schwarmintelligenz - ohne das sie der Turingschen Frage ›Can a machine think?‹ wirklich näher gekommen sind.

*

Kant wären solch rein computationale Bestimmungen des Denkens wohl fremd geblieben. ›So kann sich niemand bloß mit der Logik wagen, über Gegenstände zu urteilen.‹ heißt es in der Kritik der reinen Vernunft. Kant hat Denken nicht nur als Logik begriffen, sondern im Kontext von Erkenntnis, moralischer und ästhetischer Bewertung und zum Zwecke des Entscheidens und Handelns gesehen. Drei Fragen sind laut Kant zu beantworten:

- Was kann ich wissen?
- Was soll ich tun?
- Was kann ich hoffen?

Zur Beantwortung der Frage, was wir sicher wissen können, wie also menschliche Erkenntnis möglich sei, führte Kant drei Schichten des Denkens ein: die Vernunft, die das logische Denken reguliert, den Verstand, der das analytische Denken konstituiert und die Urteilskraft, die nach Erkenntnis des Sachverhaltes und der Handlungsmöglichkeiten die Abwägung zum Bewerten und Handeln erlaubt. Menschliches Handeln überwindet damit die Zwänge der Natur und erlaubt es, freie Entscheidungen zu treffen.[4] Ein gutes Urteil gründet notgedrungen auf Sinneseindrücken, auf dem, was der Fall zu sein scheint – also auf den Phänomenen, die nach bester Einsicht für wahr gehalten werden. Urteilskraft muss freilich entwickelt werden. Sie ist Ergebnis einer lebenslangen Bildung, Erfahrung und Übung, ein Ergebnis, das freilich nicht immer erreichbar ist: ›Der Mangel an Urteilskraft ist



Wolfgang Coy

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

eigentlich das, was man Dummheit nennt, und einem solchen Gebrechen ist gar nicht abzuhelfen.‹ heißt es ohne große Hoffnung in der Kritik der reinen Vernunft.

Was bedeutet dies nun nach dem Eintritt der ›Denkmaschinen‹ in unsere Alltagswelt? Computer sollen die Frage ›Was kann ich wissen?‹ zu beantworten helfen, so dass die Antwort auf die Frage ›Was soll ich tun?‹ leichter fällt. Die Frage ›Was kann ich hoffen?‹ bleibt davon unberührt. Diese wird weder bei Wittgenstein noch bei Turing als wissenschaftliche Frage gesehen – und auch bei Kant bleibt sie zwischen den Zeilen offen. So offen, das der preußische König Friedrich Wilhelm II ihm in einer privat versendeten Kabinettsordre verbot, öffentlich darüber zu räsonnieren (Was der Königsberger Rektor bis zum Tod des Königs auch beachtete). Kants Reflexion Nr. 177 ›Was wir denken, können wir nicht immer sagen‹ aus den ›Reflexionen zur Anthropologie‹ klingt unter diesen Umständen wie Resignation vor der Zensur; es ist aber eine Bemerkung über das Denken, das die Grenze zum Hoffen überschreitet. Damit geht Kant über eine alleinige Bestimmung des Menschen als „denkendem Wesen" hinaus. Den drei Leitfragen lässt er deshalb eine vierte Frage folgen: ›Was ist der Mensch?‹[5] Diese kann weder von der Formalen Logik noch von der Informatik beantwortet werden. Jeder Vergleich mit dem Computer führt nur in die Irre.

*

Wittgensteins Neffe Heinz v. Foerster greift die Schlussbemerkung im Tractatus auf seine Weise auf. Wie Turing geht er zum Beispiel der Machine zurück, wobei er triviale und nichttriviale Maschinen unterscheidet. Ein funktionierender Automat ist trivial, weil er genau das tut, was er tun soll. Heinz v. Foerster führte als Beispiel gern Rolls-Royce-Motoren an, bei denen er unterstellte, die sie genau so funktionierten, wie die Ingenieure sich das vorstellten. Auch eine deterministische Turingmaschine ist in Bezug auf den nächsten Arbeitsschritt trivial (so wie auch das Programm einer nicht-deterministischen Turingmachine eine nicht genauer diskriminierte Menge möglicher Nachfolgezustände festlegt). Die Frage, ob so eine paper machine jemals mit dem Rechnen zu Ende kommt, ist freilich, wie wir dank Alan Turing wissen, nicht entscheidbar. Foersters Dreh ist nun, dass er alle ›interessanten‹ Fragen als nicht entscheidbar einstuft, wobei er von der logischen Unentscheidbarkeit zur Unentscheidbarkeit des richtigen Handelns übergeht. Ob das Weltall unendlich alt oder groß ist oder ob ein Big Bang die Erklärung ist, ob wir jemals Zeitreisen unternehmen können, ob unsere Galaxis in einem schwarzen Loch verschwinden wird, ob Götter oder Dämonen existieren, ob der Mensch seinem Wesen nach gut oder böse ist, all dies sind unentscheidbare Fragen. Das wäre als solches eine billige Beobachtung. Spannend wird sie bei Fragen, die ein Handeln verlangen. Bei der Frage, ob wir diesen Partner oder jenen heiraten sollen oder besser ledig bleiben, ob wir eine Krankheit durch eine Operation bekämpfen lassen wollen, ob wir auswandern sollen oder im Lande bleiben, ob wir diesen Beruf ergreifen oder jenen, ob wir aus dem Haus gehen oder ein Buch lesen, müssen wir uns entscheiden und es gibt keine eindeutige Handlungsanweisung. ›Das ist das Amüsante an den prinzipiell unentscheidbaren Fragen; dass es eben keinen Formalismus, keinen Zwang gibt, der mich zwingt, diese Fragen in dieser oder jener Form zu beantworten. Mit dieser prinzipiellen Unentscheidbarkeit ist ein Raum der Freiheit geöffnet, in dem du jetzt entscheiden kannst. Das heisst, prinzipiell unentscheidbare Fragen können nur wir entscheiden, indem wir sagen: Ich möchte diese Entscheidung wählen, denn ich habe die Freiheit, hier zu wählen, was ich will. Die Idee, die Freiheit mit der prinzipiellen Unentscheidbarkeit zu kombinieren, bringt jetzt die Idee der Verantwortung mit sich, denn wenn ich eine prinzipiell unentscheidbare Frage entscheide, habe ich mit dieser Entscheidung die Verantwortung für diese Entscheidung übernommen.‹[6] An der logischen Kategorie der ›nicht entscheidbaren Fragen‹ spiegelt sich so die ethische Kategorie der ›Zu entscheidenden Fragen.‹ Turings These und mit ihr manche Hoffnungen der Künstlichen Intelligenz lösen sich im Ethischen Imperativ Foersters auf. Noch einmal Heinz v. Foerster: ›Unentscheidbarkeit ist die Einladung, sich zu entscheiden. Für diese Entscheidung trägt man dann die Verantwortung.‹ Das heißt also, selbst wenn alle logisch entscheidbaren Fragen geklärt wären, alles Berechenbare berechnet wäre, bliebe das Ethische unbearbeitet. Dafür brauchen wir Urteilskraft. Das ist das lebenslange Ziel von Erziehung und Bildung.

Literaturhinweise

Lena Bonsiepen, Folgen des Marginalen, in G. Cyranek und W. Coy (Hrsg): Die maschinelle Kunst des Denkens – Perspektiven und Grenzen der KI. Braunschweig/Wiesbaden: Vieweg,1994

Monika Bröcker & Heinz v. Foerster, Teil der Welt – Fraktale einer Ethik. Ein Drama in drei Akten. Carl Auer Systeme Verlag, Heidelberg 2002

Wolfgang Coy: Reduziertes Denken. Informatik in der Tradition des formalistischen Forschungsprogramms, in P. Schefe, H. Hastedt, Y. Dittrich und G. Keil (Hrsg.): Informatik und Philosophie. 31-52. Mannheim–Leipzig–Wien–Zürich: BI Wissenschaftsverlag, 1993

Bernhard Dotzler und Friedrich Kittler (Hrsg.), Alan Turing – Intelligence Service, Berlin: Brinkmann & Bose, 1987.

Heinz v. Foerster, Wissen und Gewissen, Frankfurt/Main: Suhrkamp, 1993.

Andrew Hodges, Alan Turing – Enigma, Berlin: Kammerer und Unverzagt, 1990

Roger Penrose, Shadows of the Mind: A Search for the Missing Science of Consciousness, Oxford: Oxford University Press, 1994

Alan M. Turing, On Computable Numbers, with an Application to the Entscheidungsproblem, Proc. London Math. Soc. (2), 42 (1937), 230-265.

Alan M. Turing, Computing machinery and intelligence, Mind, Vol. LIX. No.236., Oktober 1950, S.433-460

Ludwig Wittgenstein, Logisch-philosophische Abhandlung. Tractatus logico-philosophicus, Frankfurt/Main: Suhrkamp, 1969.

Endnoten

1 Vgl. A. Hodges, Alan Turing – Enigma, a.a.O.

2 In "On Computable Numbers with an Application to the Entscheidungsproblem." a.a.O.

3 Roger Penrose, Shadows of the Mind a.a.O., S. 21

4 Die aktuelle Debatte, ob dieser freie Wille dabei vollständig bewusst verläuft oder auch in tieferen Schichten unseres Gehirns verankert ist, wird davon gar nicht berührt - so wie wir nicht freiwillig für immer aufhören können zu atmen, wohl aber für eine gewisse Dauer.

5 …und er fügt in Klammern hinzu ›Anthropologie; über die ich schon seit mehr als 20 Jahren jährlich ein Kollegium gelesen habe.‹ Vgl. Hamburg: Meiner, Briefwechsel, 1989, S.634

6 M. Bröcker & H. V. Foerster, Teil der Welt, a.a.O. S.178

Jürgen Altmann

Nanotechnik, Singularität und Transhumanismus

Herausforderungen für Wissenschaft und Moral

Künstliche Intelligenz (KI) und Robotik sind beide zunächst mit hoch fliegenden Versprechungen angetreten. Viele Leistungen, die dem Menschen einfach erscheinen – Objekte in komplexer Umgebung visuell erkennen, Sprache verstehen, Probleme lösen usw. – haben sich dann aber als extrem schwierig zu programmieren herausgestellt. Noch heute sind Menschen bei solchen Aufgaben Rechnern überlegen, auch wenn Rechner in anderen Bereichen (z.B. Schach Spielen) den Menschen übertroffen haben.

Seit Mitte der 1980er Jahre wird nun das Konzept der Nanotechnik propagiert, das die Rechnerleistungen immer weiter steigern und unvermeidlich zu künstlicher Intelligenz auf menschlichem Niveau oder darüber führen soll. Dabei spielten die Visionen von K. Eric Drexler eine zentrale Rolle, die auch von einigen führenden, wenn auch nicht unumstrittenen Software-, KI- und Robotikexperten – vor allem Ray Kurzweil, Marvin Minsky und Hans Moravec - positiv aufgenommen wurden. Drexlers Hauptidee ist der universelle molekulare Montageautomat (sog. „Assembler“).[1] Durch ein Programm gesteuert synthetisiert er beliebige Moleküle und größere Einheiten, indem er die entsprechenden Bausteine der Umgebung entnimmt und mechanisch an die richtige Stelle setzt, wo sie eine Bindung eingehen. Insbesondere kann er eine Kopie von sich selbst erzeugen. Um makroskopische Produkte herzustellen, würde man die Assembler sich z.B. 30 Generationen lang verdoppeln lassen und dann bei den nunmehr 1 Milliarde Assemblern das Programm auf das gewünschte Produkt umschalten. Dieses Konzept – von den Befürwortern inzwischen „molekulare Nanotechnik“ genannt – ist wissenschaftlich umstritten, aber nicht widerlegt.

Eine zweite Grundidee ist die des Nanoroboters – eines Systems von einigen hundert Nanometer bis einigen Mikrometer Größe, das eine Energieversorgung, ein Kommunikationssystem und einen Steuerrechner hat, sich fortbewegen kann, Eigenschaften seiner Umgebung feststellen und aktiv auf letztere einwirken kann, sich ggf. auch vermehren kann. Um Wirkungen in größerem Maßstab zu erzielen, würden Nanoroboter in der Regel in Schwärmen auftreten. Nanoroboter könnten z.B. in lebenden Zellen als Sonden wirken und somit die biochemischen Prozesse vollständig aufklären helfen. Sie würden defektes Erbgut (DNS) in Zellen reparieren, Alterungsprozesse aufhalten oder zurück drehen. Die Vorgänge in Zellen könnten gestoppt und wieder in Gang gesetzt werden. Knochen würden mit Diamant verstärkt, Organe leistungsfähiger gemacht oder durch bessere ersetzt.

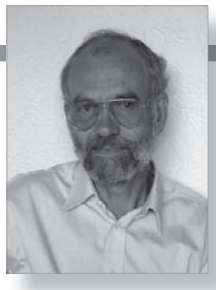
Eine Reihe weiterer Konzepte sind mit molekularer Nanotechnik verbunden, darunter das Auslagern des Gehirninhalts in einen Rechner, wo die Person dann als Software weiter lebt, und die Ausbreitung in den Weltraum.

Würden Nanoroboter in allen Nervenzellen sitzen, könnte man damit von außen messen, was alle Neurone im Gehirn gerade tun (feuern oder nicht feuern), ggf. auch die Zustände an den einzelnen Synapsen feststellen und melden. So könnte ein vollständiges Bild des Gehirns erstellt werden, in einen Rechner heruntergeladen werden und dort als Simulation weiter laufen. Umgekehrt könnten die Nanoroboter die Neurone steuern und so Sinneseindrücke erzeugen oder Gedanken hervorrufen. Auch könnten so Verbindungen zu künstlichen Informationsverarbeitungssystemen und -speichern hergestellt werden, die sich im Körper oder außerhalb befinden, oder zu den Gehirnen anderer Menschen.

Molekulare Nanotechnik würde den Transport in den Weltraum radikal verbilligen. Die durch Wachstum der Menschheit (wenn niemand mehr stirbt) oder den Aufwuchs nanotechnischer Systeme auf der Erde zu erwartenden Ressourcenprobleme ließen sich überwinden, indem man Rohstoffe auf dem Mond, Planeten und Asteroiden abbaut und große Teile der Menschheit in Weltraumkolonien auslagert. Das würde auch Probleme lösen wie Umweltverschmutzung, Atomkrieg oder Zusammenstoß der Erde mit einem Asteroiden.

Andere empfehlen aber auch, Nanoroboter für die Reinigung der Umwelt auf der Erde von Schadstoffen zu verwenden; wei-

Jürgen Altmann



PD Dr. Jürgen Altmann ist Physiker und Friedensforscher. Er hat Rechner betreut und Computer-Mustererkennung (an Bildern, an akustischen und seismischen Signalen) betrieben. Seit 1985 macht er Abrüstungs-orientierte Forschung. Schwerpunkte sind kooperative Verifikation von Abrüstungs- und Friedensabkommen mit akustischen, seismischen und magnetischen Sensoren sowie Militär-Technikfolgenabschätzung und präventive Rüstungskontrolle. Im letzteren Bereich hat er u.a. geforscht über „nicht tödliche“ Waffen, Nanotechnik und besatzungslose militärische Systeme. Er ist Mitgründer des Forschungsverbundes Naturwissenschaft, Abrüstung und internationale Sicherheit FONAS und ein stellvertretender Sprecher des Arbeitskreises Physik und Abrüstung der Deutschen Physikalischen Gesellschaft DPG. *(altmann@e3.physik.tu-dortmund.de)*

ter gehende Vorstellungen sehen die Umgestaltung der Erde vor, das sog. Terraforming.

Eine ausführliche jüngere Darstellung vieler der mit molekularer Nanotechnik verbundenen Konzepte ist Ray Kurzweils Buch „The Singularity is Near" (2005).[2] In Bezug auf Computer stellt Kurzweil ein Modell des Wachstums der Rechenleistung auf, bei dem die Verdopplungszeit des „Moore'schen Gesetzes" sich im Laufe der Zeit immer weiter verringert, so dass die Rechenleistung, die man für 1000 $ kaufen kann, mit der Zeit gemäß einer doppelt-exponentiellen Funktion ansteigt. Das passt auf die Entwicklung von 1900 bis heute, wird dann aber bis 2100 extrapoliert. Demnach wird die Rohrechenleistung eines menschlichen Gehirns (10^{16} Rechnungen pro Sekunde) um 2023 erreicht, die von 10 Milliarden menschlicher Gehirne, 10^{26} R/s) um 2049. Grenzen gibt es nur für spezifische Technologien, dann kommt nach Kurzweil jeweils eine neue Technik, die das weitere Wachstum ermöglicht. Die Silizium-Lithografie reicht etwa noch für zehn Jahre, in den Folgejahrzehnten werden dreidimensionale Strukturen das weitere Wachstum sicherstellen. Um 2080 werde man 10^{42} R/s für 1000 $ erreichen, in dem jedes der in 1 kg Materie enthaltenen 10^{25} Atome 100 bits speichert und 10^{15} Rechenschritte pro Sekunde durchführt. Später werde die (dann hauptsächlich nicht-biologische) Intelligenz die Masse des Sonnensystems zum Rechnen nutzen (10^{70}-10^{80} R./s im frühen 22. Jahrhundert), und schließlich werde sie sich mit Lichtgeschwindigkeit (oder schneller) das Universum vornehmen, das dann „aufwacht".

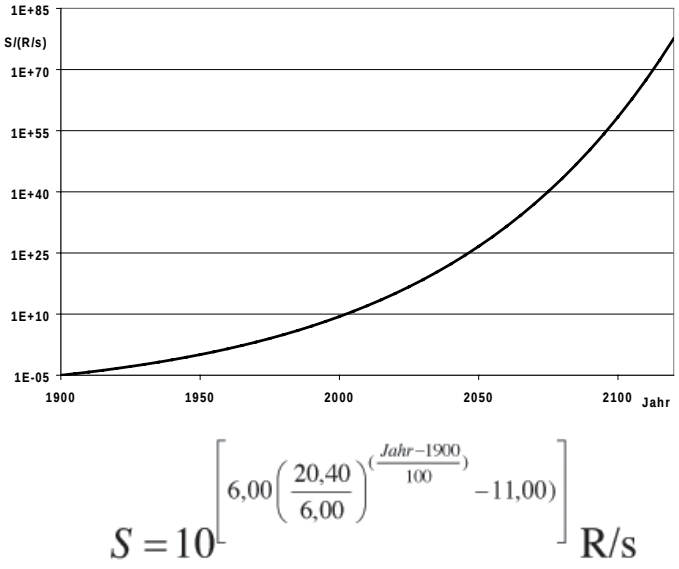


Abbildung 1:
Rechenleistung, die man nach Kurzweils Modell für 1000 $ kaufen kann (in Rechnungen pro Sekunde über der Zeit). Im logarithmischen Maßstab wird die Doppel-Exponentialfuntion sichtbar.

Wenn die Roh-Rechenleistung eines Computers in anderthalb Jahrzehnten die des menschlichen Gehirns erreichen wird, dann – so Kurzweil – wird auch die entsprechende „starke" KI damit verbunden sein. Das könne durch Nachbau des Gehirns erreicht werden, das man durch immer bessere Untersuchungstechniken vollständig verstehen werde. Anschließend werden die Computerfähigkeiten aber beschleunigt weiter gesteigert werden und die Intelligenz des Menschen schnell hinter sich lassen. Diese super-intelligenten Systeme werden dann Wissenschaft viel schneller betreiben und die Technik (einschließlich sich selbst) immer schneller weiter entwickeln, bis zu den durch die Naturgesetze gegebenen Grenzen. Dies ist dann die sogenannte Singularität, von Kurzweil auf 2045 datiert – bei der man so radikale Veränderungen erwarten muss, dass Vorhersagen kaum möglich sind. Jedoch schreibt Kurzweil meist im Indikativ Futur[3] – diese Intelligenzen werden mit den Menschen verschmelzen bzw. die Menschen werden sich in sie verwandeln und in Software weiter leben. Dies ist eine freundliche Version des Transhumanismus, der davon ausgeht, die Hauptaufgabe der Menschheit sei es, die nächste Stufe der Evolution möglichst zügig herbeizuführen. Es gibt aber auch die Warnungen, „Gentechnik, Nanotechnik und Robotik, die mächtigen Techniken des 21. Jahrhunderts, werden Menschen überflüssig machen und wissensbasierte Massenvernichtung mit sich bringen."[4]

Das Denksystem der Befürworter von molekularer Nanotechnik, Singularität und Transhumanismus ist eine seltsame Mischung von alten Menschheitsmythen und Technikeuphorie, von wissenschaftlich belegten Aussagen, einigermaßen begründeten Extrapolationen und dogmatisch anmutenden Erwartungen.[5] Man könnte diese Ideen ignorieren, aber sie werden zunehmend in der „normalen" Wissenschaft, Wissenschaftsförderung und Technikplanung aufgenommen, vor allem in den USA. So gab es dort ab 2001 eine Reihe regierungsfinanzierter Tagungen zu den sogenannten „konvergierenden Techniken". Nano-, Bio-, und Informationstechnik sowie Kognitionswissenschaft (englisch NBIC) würden zusammenwachsen und ganz neue Möglichkeiten für die Verbesserung der menschlichen Leistungsfähigkeit bringen. Neben Stärkung des US-Militärs und wolkigen Versprechungen wie der, die Menschheit könne zu einem einzigen, verteilten und vernetzten „Gehirn" werden, wurden eine Reihe von in 20 Jahren erreichbaren Visionen formuliert, darunter schnelle Schnittstellen zwischen dem menschlichen Gehirn und Maschinen sowie den Menschen angepasste Roboter und Software-Agenten. Der menschliche Körper werde dauerhafter und leich-

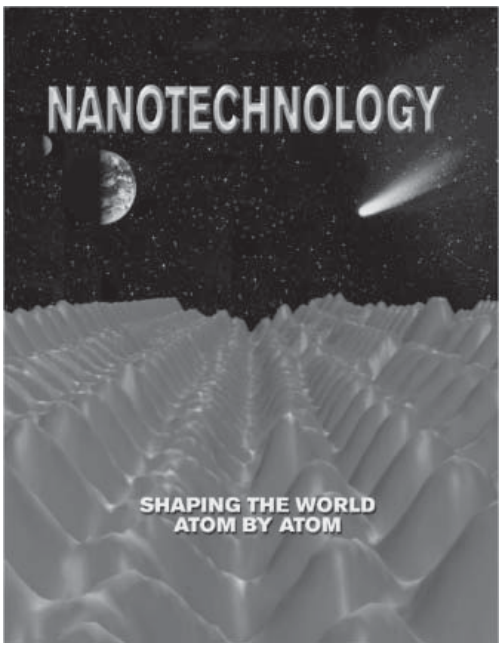


Abbildung 2:
Titelbild einer Broschüre der US-National Nanotechnology Initiative von 1999

ter zu reparieren sein. Nicht nur Pflanzen und Tiere, sondern auch Menschen werde man gentechnisch verändern – Konsens in ethischen Fragen werde sich im Prozess bilden. Mittels Weltraumbasen werde man die Ressourcen von Mond, Mars und nahen Asteroiden ausbeuten.[6] Die National Nanotechnology Initiative verspricht, die Welt „Atom für Atom zu gestalten".

In Europa wurde 2005 an der Oxford University ein Future of Humanity Institute eingerichtet. Direktor wurde Nick Bostrom, der 1998 die World Transhumanist Association mit gegründet hatte. Mit Hauptbeteiligung von Google wurde 2008 auf dem Gelände des NASA Ames Center in Kalifornien die „Singularity University" gegründet; Ray Kurzweil war führend dabei.

Die „normale" Wissenschaft hat sich um dieses Ideengebäude nicht wirklich gekümmert – auf Nanotechnik-Konferenzen hörte man ab und zu abfällige Bemerkungen, und es gab eine Handvoll kritischer Artikel in populärwissenschaftlichen Zeitschriften – bis heute gibt es aber keine begutachteten Arbeiten, die sich auf naturwissenschaftlich-technischer Basis gründlich mit diesen Konzepten auseinandersetzen. Sie entfalten aber in Teilen der Öffentlichkeit und bei Entscheidungsträgern eine gewisse Wirkung – in den USA mehr als in Europa, aber auch hier.

Von daher ist es wichtig, dass sich die an verantwortlicher Nutzung von Wissenschaft und Technik Interessierten diesen Themen zuwenden und sie sowohl unter Gesichtspunkten der Wissenschaft wie der Moral kritisch untersuchen. Dabei haben die wissenschaftlichen Aspekte eine gewisse Vorrangstellung – schließlich hängt die Relevanz der moralischen Beurteilung der Abschaffung des Todes, der Gehirnsteuerung durch Nanoroboter, des Übergangs vom Menschen zu einer neuen Techno-Spezies davon ab, ob diese Ideen realisierbar sein werden und wenn ja, wann. Auch haben sozial- und geisteswissenschaftliche Untersuchungen zu moralischen Fragen schon einige Vorarbeit geleistet.[7]

Für die wissenschaftliche Beschäftigung stellen sich Herausforderungen wie:

- Wo liegen Grenzen für die Verkleinerung von Rechnerstrukturen bzw. die Erhöhung der Rechenleistung? Kann man für die weitere Zukunft davon ausgehen, dass immer dann, wenn eine Technologie an ihr Ende kommt, die nächste bereit stehen wird?

- Wie realistisch ist die Erwartung, Schwärme von Nanorobotern im Körper könnten die Zellprozesse überwachen und verändern oder gar flexibel auf eindringende zerstörerische Nanotechnik reagieren?

- Wie genau kann die Detailanalyse des lebenden menschlichen Gehirns werden (räumliche und zeitliche Auflösung, Größe des untersuchten Teils)?

Zur Bearbeitung muss man tief einsteigen, Kurzweil gibt hunderte von Zitaten an – z.T. von Befürwortern der molekularen Nanotechnik, aber auch aus der „normalen" Wissenschaft.

Bei den moralischen Herausforderungen geht es unter anderem um folgende Bereiche:

- In Gedankenexperimenten sollten alle möglichen Konsequenzen propagierter Entwicklungen erkundet werden.

- Wenn dystopische Szenarien nicht ausgeschlossen werden können – was ist dann die angemessene Anwendung des Vorsorgeprinzips?

- Sollen Entwicklungen in Richtung auf Verschmelzung von Rechner und Mensch schnell vorangetrieben oder eher gebremst werden? Wenn letzteres, wo und wie sollte das geschehen?

- Wie angemessen ist die Aussage, die zukünftigen Cyborgs oder Software-Entitäten würden als menschlich gelten?

- Wenn der Öffentlichkeit unfundierte Heilsversprechen gemacht werden: Wie kann man sie wirksam kritisieren?

- Ist neue Technik das vorrangige Mittel zur Überwindung von Menschheitsübeln wie Hunger, Unterentwicklung, Ungerechtigkeit, oder geht es eher um gesellschaftliche/soziale/politische Veränderungen?

Hier ist interdisziplinäre Arbeit gefordert, wofür das Verständnis der Informatik als komplexe Wissenschaft, die sich auch mit der Einbettung von Agenten und Akteuren in die menschliche Zivilisation befasst, eine gute Voraussetzung bildet.

Endnoten

1 *K. Eric Drexler, Engines of Creation – The Coming Era of Nanotechnology, New York: Anchor/ Doubleday 1986/1990. S. auch die Informationen des Foresight Institute, http://www.foresight.org.*

2 *R. Kurzweil, The Singularity is Near – When Humans Transcend Biology, New York etc.: Penguin 2005. S. auch http://singularity.com/, http://www.kurzweilai.net.*

3 *Man muss R. Kurzweil zugute halten, dass er einige seiner Annahmen als Spekulation bezeichnet, etwa die Auffassung, mit Piko- oder Femtotechnik werde man in Atomkernen und Elementarteilchen Rechnerstrukturen unterbringen können.*

4 *Bill Joy, Why the future doesn't need us – Our most powerful 21st-century technologies – robotics, genetic engineering, and nanotech – are threatening to make humans an endangered species, Wired 8.04 (April 2000), http://www.wired.com/wired/archive/8.04/joy_pr.html.*

5 *Für genauere Analysen s. C. Coenen, M. Schuijff, M. Smits, P. Klaassen, L. Hennen, M. Rader, G. Wolbring, Human enhancement. Brüssel: European Parliament 2009 (IP/A/STOA/FWC/2005-28/SC32 & 39), http://www.europarl.europa.eu/stoa/publications/studies/stoa2007-13_en.pdf (Section 2.8) und die dort zitierte Literatur sowie C. Coenen, Entgrenzung und Tradition: Zur politisch-historischen Einordnung des visionären Diskurses über Nanotechnologie, in: A. Ferrari, S. Gammel (Hg.): Visionen der Nanotechnologie, Heidelberg: AKA 2009.*

6 *M. C. Roco, W. S. Bainbridge (eds.), Converging Technologies for Improving Human Performance – Nanotechnology, Biotechnology, Information Technology and Cognitive Science, Boston etc.: Kluwer, 2003 (auch http://www.wtec.org/ConvergingTechnologies/Report/NBIC_Report.pdf).*

7 *Z.B. Coenen et al. (Fn. 5), A. Nordmann: If and Then – A Critique of Speculative Nano-Ethics, Nanoethics 1 (1), 31-46, 2007, Symposium Untangling the Debate: The Ethics of Human Enhancement, Nanoethics 2(3), 2008.*

Lesen –
Neues für den Bücherwurm

Stefan Hügel

Kontrollverluste
Interventionen gegen Überwachung

Das Thema Überwachung ist stärker denn je in der Diskussion. Nicht überraschend also, dass eine Reihe von Büchern zu diesem Thema in den vergangenen Wochen und Monaten veröffentlicht wurde. Dabei decken die Autoren zumeist ein breites politisches Spektrum ab – in der Ablehnung zunehmender staatlicher Kontrolle gibt es in der politischen Opposition – ob Linke, ob Grüne, ob FDP – einen breiten Konsens.

Die Initiative Leipziger Kamera entstand in der Stadt des Pilotprojekts zur Videoüberwachung öffentlicher Plätze und besteht dort seit 2003. Sie hat nun einen Sammelband herausgegeben, in dem eine dezidiert linke Position in der Überwachungskritik vertreten wird. Neben Autoren aus dem Umfeld des CCC, von Attac und aus der Linkspartei geht das Spektrum bis hin zu einem Beitrag des Schwarzen Blocks.

Positionen

Damit verschiebt sich die politische Perspektive gegenüber der Hauptströmung der Überwachungskritik deutlich. Zu erkennen ist das sofort an den Positionen zum Bundesverfassungsgericht und seinen Entscheidungen der letzen Monate: Während diese von einer breiten Mehrheit begrüßt werden, schreibt Elke Steven vom Komitee für Grundrechte und Demokratie in ihrem Beitrag „Die Gerichte werden uns nicht befreien!“ skeptisch:

> *Von manchen Bürger_innen werden diese Entscheidungen gefeiert, als würde damit dem Staat in seiner Entwicklung hin zu einem präventiven Sicherheitsstaat tatsächlich die Grundlage entzogen. Aufgrund bisheriger Erfahrungen lässt sich jedoch voraussagen, dass lediglich weitere Gesetze folgen werden, die sukzessive die Grenzen weiter verschieben. … Kaum hat das Gericht festgestellt, dass ein Gesetz (teilweise) rechtswidrig ist, sucht der Gesetzgeber nach neuen Anlässen und Wegen, seine Eingriffsrechte auszudehnen. Und das Gericht vollzieht diese Entwicklung nach.*

Und Ron Steinke, Autor u.a. bei Jungle World und Konkret kritisiert im Beitrag „Radikal wie Karlsruhe“ die Verschiebung des Diskurses vom politischen ins juristische und schreibt:

> *Die öffentliche Diskussion über staatliche Überwachung hat sich … durch die ‚Verrechtlichung‘ des Themas merklich verschoben, weg von der ursprünglichen Frage „Ist eine bestimmte Überwachungsmaßnahme politisch kritikwürdig?“ hin zur wesentlich unkritischeren Frage „Gibt es rechtliche Einwände?“*

Inhalt

Der Band ist in sechs Abschnitte gegliedert, die jeweils mehrere Beiträge versammeln. Der erste Abschnitt „Was geht?“ behandelt Entwicklungen im Bereich der Überwachung und ihre politischen und gesellschaftlichen Aspekte. Hier wird auch der Bezug der Überwachungskultur zum Neoliberalismus hergestellt.

Der zweite Abschnitt „Was geht nicht?“ setzt sich mit der überwachungskritischen Bürgerrechtsbewegung auseinander – ihm entstammen die Zitate oben. Insbesondere nimmt er kritisch Stellung zum Vertrauen der Bürgerrechtsbewegung in staatliche Institutionen – in erster Linie das Bundesverfassungsgericht und den Bundesdatenschutzbeauftragten. Kritisiert werden auch aus Sicht eines Autors verbreitete Reaktionsmuster selbst innerhalb der Bürgerrechtsbewegung auf Überwachung: Ignoranz, d.h. den Hang zum „Wer nichts zu befürchten hat, hat auch nichts zu verbergen.“, Hypersensible Paranoia, d.h. die Überzeugung, dass die Lage ohnehin hoffnungslos sei und zuletzt die Erwartung, dass Aufklärung und Appelle das wirksame Gegenmittel gegen Überwachung sind.

Der dritte Abschnitt „Sind wir alle 129a?“ behandelt die Auswirkungen des Terrorismusparagraphen und hat als zentrale Autoren Andrej Holm, der vor rund zwei Jahren aufgrund des §129a – rechtswidrig, wie der BGH später feststellte – verhaftet wurde, und Anne Roth. Sie berichten von der Öffentlichkeitsarbeit während der Inhaftierung und über den Blog zu Überwachung, den Anne Roth seither betreibt.

Hauptthema des vierten Abschnitts „Was noch?“ ist das Leben abseits des Mainstreams. Er behandelt die besonderen Aspekte der Überwachung bei Flüchtlingen und Migranten, im Arbeitsleben, und im Sicherheitsbereich. Außerdem geht er auf die besonderen Aspekte der Überwachung bei Jugendlichen und das Thema Überwachung vs. Sicherheit aus der Perspektive von Frauen ein.

Die letzten beiden Abschnitte „Was sagen?“ und „Was tun?“ behandeln Argumentations- und Aktionsstrategien gegen Überwachung – von der „Rhetorik und Realität der Überwachung“ über „Schritte zu einem sicher(er)en Computersystem“ bis zu den Surveillance Camera Players.

Fazit

Der Band behandelt ein breites Spektrum von Themen: neben der allgegenwärtigen Vorratsdatenspeicherung und der Online-Durchsuchung – und den Positionen des Bundesverfassungsgerichts dazu – auch Aspekte wie den Zusammenhang der Überwachung mit dem Neoliberalismus, die Überwachung benachteiligter Gruppen und den „Kampf gegen den Terror" mit seinen Auswirkungen. Er setzt sich dabei teilweise deutlich vom bürgerrechtlichen Mainstream-Diskurs ab; viele Positionen sind bei der breiten Mehrheit sicherlich nicht anschlussfähig.

Aber auch, wenn man nicht alle Positionen teilt, die in dem Buch vertreten werden: Es lenkt den Blick auf eine Reihe von Aspekten von Kontrolle und Überwachung, die bei der Diskussion nicht übersehen werden dürfen.

Leipziger Kamera (Hg.): Kontrollverluste. Interventionen gegen Überwachung, Münster: Unrast-Verlag, 2009. Preis: €18.00

Ralf E. Streibl

Kinderpornographie und Internet

Endlich! – ist man versucht zu sagen, wenn man sich das Buch von Korinna Kuhnen genauer ansieht, eine medienwissenschaftliche Dissertation an der Universität Paderborn, die beim Hogrefe Verlag in der Reihe »Internet und Psychologie« publiziert wurde. Betrachtet man die in diesem Jahr geführte Debatte über die Sperrung von Internetseiten mit kinderpornographischen Inhalten, so zeichneten sich die Protagonisten dieser Forderungen zumeist durch profunde Unkenntnis der technischen Hintergründe aus. Von Seiten der Gegner wurden neben technischen vor allem grundsätzliche politische Bedenken (Schaffung einer Zensur-Infrastuktur etc.) ins Feld geführt. Differenzierte Töne haben es bei diesem Thema schwer, in der aufgeheizten Debatte zu Kenntnis genommen zu werden.

Es wäre fatal, die Debatte um Kinderpornographie im Internet alleine auf die technische oder politische Diskussion zu reduzieren. Korinna Kuhnen kommt das Verdienst zu, in ihrer Arbeit, die vor der jüngsten Debatte entstand, in fundierter und sorgfältiger Weise das Thema von verschiedenen Seiten anzugehen und zu diskutieren. Sie beginnt mit dem Versuch einer Klärung des Begriffs Kinderpornographie. Schon hier zeigt sich, dass es zu diesem in der politischen Debatte meist plakativ gebrauchten Begriff keine klare juristische, gesellschaftliche und kulturell übergreifende Definition gibt. Diese differenzierte und vorsichtige Betrachtung führt jedoch im weiteren Verlauf nicht zu einer unangemessenen Relativierung der Problematik. Weitere Kapitel beschäftigen sich mit der Sicht der Strafverfolgung sowie Nutzungsaspekten des Internets, insb. hinsichtlich der Frage der Zugänglichkeit kinderpornographischer Materialien. Ein großes Kapitel widmet sich den Tätern und thematisiert ausführlich mögliche Ursachen, Motive und Wirkungen, ohne hierbei die Spezifika des Mediums Internet dabei aus den Augen zu verlieren. Ein kürzeres aber umso wichtigeres Kapitel thematisiert die Opferseite und macht überaus deutlich, dass nicht nur bei der Produktion kinderpornographischer Materialien zum Teil massiver Missbrauch an Kindern getrieben wird, sondern dass durch die Verbreitung und den Warencharakter dieser Missbrauch dauerhaft perpetuiert wird. Das abschließende Kapitel über die politische Debatte, welches den provokativen Untertitel »Kinderschutz versus Datenschutz« trägt, enthält zwar nicht die Diskussionen der letzten Monate, ist aber ungeachtet dessen in seiner Analyse auch heute lesenswert. Insofern überrascht es nicht, dass die Autorin in ihrem Resümee, betitelt »Die Ablenkung vom Wesentlichen«, deutlich Stellung bezieht. Sie stellt heraus, dass Kinderpornographie im Internet kein herbei geredetes, sondern ein real existentes Problem ist, dessen grundlegende Ursache jedoch nicht im Internet zu suchen sei. Sie analysiert sorgfältig die Wirkungen des Mediums, bleibt dabei jedoch nicht in einer rein medienwissenschaftlichen Betrachtung stecken. Vielmehr äußert sie Besorgnis, dass durch den intensiven Fokus auf das globale Medium Internet „der eigentliche Kern der Kinderpornographie, nämlich der ganz alltägliche, sexuelle Missbrauch von Kindern womöglich aus dem Blickfeld" (S.298) geraten könnte. So befürchtet sie, dass die skandalisierende und pauschalisierende Diskussion für die Schärfung der gesellschaftlichen Wahrnehmung eher kontraproduktiv wirksam wird.

Fazit: Endlich eine differenzierte Annäherung an ein stark durch Tabus und vorgefasste Meinungen geprägtes Thema, welches in der politisch aufgeladenen Diskussion immer wieder instrumentalisiert zu werden droht. Schade, dass offenkundig viele an der aktuellen politischen Diskussion Beteiligte dieses Buch (noch?) nicht gelesen haben.

Korinna Kuhnen: Kinderpornographie und Internet, Medium als Wegbereiter für das (pädo-)sexuelle Interesse am Kind? Göttingen: Hogrefe, 2007.

Ralf E. Streibl

Gewissensbisse

Recht druckfrisch ist das von einem fünfköpfigen Autorinnen- und Autorenteam verfasste Büchlein, welches den Untertitel *Ethische Probleme der Informatik* trägt. Der Ausgangspunkt lag in Diskussionen in der Fachgruppe *Informatik und Ethik* der Gesellschaft für Informatik (GI). In den *Ethischen Leitlinien* der GI (1994/2003) wird u.a. gefordert, dass die GI interdisziplinäre Diskurse zu ethischen und sozialen Problemen der Informatik initiiert und fördert. Dies sei – so das Autorenkollektiv in seinen Vorbemerkungen – ein Ziel des vorliegenden Buches.

Das Buch enthält eine ganze Reihe von Fallbeispielen zu ethischen Fragen im Kontext von Informatik, „die genutzt werden können, eine Diskussion zu stimulieren und voranzutreiben“ (S.12). Vorangestellt ist ein kurzes Kapitel über Verantwortung in der Informatik. Knapp die Hälfte der Fallbeispiele im Buch ist nach der szenisch gehaltenen Darstellung eines Dilemmas mit einer »Diskussion« versehen, bei den anderen sind noch einige »Fragen« am Ende des Szenarios aufgelistet. Ein Abschlusskapitel über konkrete Erfahrungen mit derartigen Fallbeispielen in Seminaren sowie ein Anhang, in dem die Ethischen Leitlinien der GI, ein Diskussionsschema sowie drei exemplarische studentische Ausarbeitungen enthalten sind, beschließen das Buch. Wesentlicher Gedanke bei der Gestaltung des Buches war offenkundig der modulare Aufbau – es ist möglich einzelne Fallbeispiele unabhängig voneinander zu lesen und zu bearbeiten. Das Autorenkollektiv hat sich nach eigenem Bekunden bewusst dafür entschieden, dem Buch kein Kapitel über allgemeine Ethik beizufügen. Es ist gut möglich, dass die Hauptzielgruppe des Buches dies auch nicht vermisst. Doch wäre es möglicherweise hilfreich gewesen, das Kapitel über »Verantwortung in der Informatik« vor diesem Hintergrund ausführlicher zu gestalten und mit mehr konkreten und kommentierten Verweisen auf einschlägige Literatur zu versehen – als Möglichkeit und Anregung zu einer weitergehenden eigenen Auseinandersetzung mit unterschiedlichen für die Informatik möglicherweise relevanten ethischen Ansätzen. Der Zwiespalt hinsichtlich der Frage, wie viel an Vorgabe bzw. Unterstützung für die inhaltliche Auseinandersetzung mit ethischen Fragen sinnvoll, nützlich oder gar notwendig ist, mag auch die Beurteilung der Fallbeispiel-Kapitel beeinflussen. Das Autorenkollektiv hält die Diskussion hier bewusst knapp oder wirft in der Mehrzahl der Fallbeispiele nur Fragen auf – mit Verweis darauf, dass Fallbeispiele keine eindeutigen Lösungen vorgeben. So richtig dies ist, vermisste ich bei der Lektüre doch systematische Hinweise auf hilfreiche Literatur zur weiteren Vertiefung (findet sich nur vereinzelt) der den Fallbeispielen zugrunde liegender, für eine ethische Debatte wesentlichen Parameter oder (auch kontroverser) Positionen. Natürlich kann man die Ansicht vertreten, dass das Heraussuchen entsprechender Quellen Aufgabe der jeweiligen Lehrenden oder Studierenden bzw. Schüler sei. Jedoch besteht ohne geeignete Einstiegspunkte – insbesondere bei manchen Themen, die stärker an der Lebenswelt der Teilnehmerinnen und Teilnehmer sind – leicht die Gefahr einer zu stark nach »Bauchgefühl« geführten Diskussion. Ungeachtet dieser kritischen Anmerkungen, die vor allem die Hoffnung auf eine in dieser Hinsicht erweiterte zweite Auflage ausdrücken, ist das vorliegende Buch sicherlich eine hilfreiche Anregung und »Steinbruch« für die Gestaltung kommunikativer Lernsituationen im Bereich *Informatik und Gesellschaft*.

Fazit: Ein nützliches und gut zu lesendes Buch, welches hilfreiche Anregungen für Szenarien und Fragenansätze liefert, die konkrete Diskussion und Auseinandersetzung damit dabei weitgehend den Leserinnen und Lesern überlässt.

Debora Weber-Wulff, Christina Class, Wolfgang Coy, Constanze Kurz, David Zellhöfer: Gewissensbisse. Ethische Probleme der Informatik. Bielefeld: transkript, 2009.

Ralf E. Streibl

Beitragen statt tauschen

Auf den ersten Blick erschließt sich nicht, warum ein Buch mit diesem Titel in der FIfF-Kommunikation angekündigt werden sollte. Der Untertitel verrät mehr: *Materielle Produktion nach dem Modell Freier Software*.

Der Autor – an der FU Berlin in Informatik promoviert und als Software-Entwickler und Textmining-Experte tätig – setzt sich in dem Buch mit der Möglichkeit einer anderen Ökonomie und damit einer anderen Gesellschaftform konkret auseinander und bezieht sich dabei auf die Idee der *Peer-Produktion* ein von Yochai Benkler geprägter Begriff, der die gemeinschaftliche und offene Produktionsweise bezeichnet, die beispielsweise der Entwicklung Freier Software und der „Freie Kultur“-Bewegung zugrunde liegt. Peer-Produktion beruht auf Beiträgen anstelle von Verdienstmöglichkeiten oder Planwirtschaft. Der Autor erörtert im Verlauf des Buches, ob diese Grundidee auch jenseits von Informationsgütern in kleineren Peer-Projekten sowie in einer größeren Gesellschaft möglich sein könnte. Die Abschlusskapitel beschreiben darauf aufbauend das Leben in einer umfassenden Peer-Ökonomie und setzen sich mit Einwänden und Fragen diesbezüglich auseinander. Anders als manch andere Veröffentlichung zu Wirtschaftsthemen zeichnet sich dieses Buch durch eine erfrischend klare Sprache und hohe Verständlichkeit aus. Der klare Aufbau lädt ein, sich dem Autor folgend auf eine gedankliche Reise in eine andere Gesellschaftsform zu begeben,

Fazit: Eine spannende und anregende Lektüre, die in der Beschreibung einer anderen Ökonomie ganz nebenbei auch die Auen öffnen mag bezüglich einiger Aspekte derzeit verbreiteter Gesellschaftsformen.

Christian Siefkes: Beitragen statt tauschen. Materielle Produktion nach dem Modell Freier Software. Neu Ulm: AG SPAK, 2007.

Ralf E. Streibl

Computerspiele und Politik

Zur Konstruktion von Politik und Gesellschaft in Computerspielen ist dieser Sammelband untertitelt. Dahiner verbirgt sich ein interessanter Ansatz und eine spannende Grundfragestellung. Anstatt – wie leider immer noch oft üblich – Einflüsse von Computerspielen auf die Spielerinnen und Spieler vor dem Hinter-

grund einfach gestrickter Wirkungstheorien zu behaupten, nähern sich die aus verschiedenen geisteswissenschaftlichen Disziplinen stammenden Autorinnen und Autoren in ihren Beiträgen von einer andern methodischen Seite und versuchen eine Rekonstruktion der Darstellungen von Politik und Gesellschaft in Computerspielen. Zugrunde liegt die (nicht neue) Idee, dass in nahezu allen Computerspielen politisch-gesellschaftliche Aussagen enthalten sind.

Tobias Bevc vertritt die These, dass „diese Aussagen in den gängigen und erfolgreichen Computerspielen durchweg eine Ideologie des Bestehenden transportieren" (S.50) und somit die Realgesellschaft stark vereinfacht darstellt, nicht hinterfragt, sondern kritik- und alternativlos anerkannt wird. *Julian Kücklich* betrachtet in seinem Beitrag Online-Rollenspiele, die er als „virtuelle Zivilgesellschaften" ansieht. Er kritisiert jedoch, dass durch die Vorgaben und Möglichkeiten der Spiele-Anbieter „die Spieler in einer Art und Weise ihrer Rechte beraubt werden, die in der realen Welt niemals toleriert würde" (S.71). Er vergleicht die Entmündigung von Online-Rollenspielern mit neoliberalen Einflüssen in der realen Gesellschaft und stellt eine interessante These auf: „In einer Welt, in der der öffentliche Raum zunehmend kleiner wird, mögen Online-Rollenspiele als Rückzugsräume erscheinen, aber tatsächlich werden sie der realen Welt immer ähnlicher" (ebd.). Neben eher theoretisch-methodischen Reflexionen enthält der Band auch konkrete Analysen, so z.B. von Spielen mit historischem Inhalt, sowie einen Beitrag über die „Veränderung des traditionellen Sportbildes in Gesellschaft und Politik durch eSport".

Fazit: Die Beiträge des Bandes mögen für die einzelne Leserin bzw. den einzelnen Leser je nach konkretem Interesse unterschiedlich interessant sein, wie dies ja oft bei Tagungsbänden der Fall ist. Insgesamt ist der Band ein erfreulicher Versuch, die gesellschaftliche Diskussion über Computerspiele auf andere Fragestellungen zu bringen und die in Computerspielen transportierten Weltbilder expliziter zu machen.

Tobias Bevc (Hrsg.): Computerspiele und Politik. Zur Konstruktion von Politik und Gesellschaft in Computerspielen. Münster: Lit, 2007.

Ralf E. Streibl

Beiträge zu Datenschutz, Sicherheit und Überwachung ...

Das FIfF kooperiert ja seit langem mit anderen Bürgerrechtsorganisationen (vgl. FIfF-Kommunikation 2/2009). Es bietet sich daher an, an dieser Stelle auf einige interessante Publikationen aus diesem Kreise hinzuweisen.

Beginnen möchte ich mit einer bereits vor einem Jahr erschienen Ausgabe der *Vorgänge* (Nr. 184). Das Heft trägt den Titel *Der gläserne Mensch* und brachte – vor dem Hintergrund 25 Jahre Recht auf informationelle Selbstbestimmung – eine hochspannende Zusammenstellung von Beiträgen renommierter Autorinnen und Autoren, darunter z.B. der derzeitige BfD Peter Schaar, Hans Peter Bull (BfD von 1978-1983), Sarah Spiekermann. Das Inhaltsverzeichnis ist unter *http://www.humanistische-union.de/publikationen/vorgaenge/* einsehbar.

Ferner sei an dieser Stelle auf den *Grundrechte-Report 2009* verwiesen. Nicht überraschend ist, dass Beiträge zu Datenschutz und Privatheit auch in diesem Jahr einen großen Stellenwert einnehmen. Diese jährlich in Taschenbuchformat erscheinende Publikation wird als Projekt gemeinsam von folgenden Bürger- und Menschenrechtsorganisationen getragen: Humanistische Union, Gustav-Heinemann-Initiative, Komitee für Grundrechte und Demokratie, Bundesarbeitskreis kritischer Juragruppen, Pro Asyl, Republikanische Anwältinnen- und Anwälteverein, Vereinigung demokratischer Juristinnen und Juristen, Internationale Liga für Menschenrechte, Neue Richtervereinigung. Das Inhaltsverzeichnis des Grundrechte-Reports finden Interessierte unter sich unter: http://www.grundrechte-report.de

Das ebenfalls dieses Jahr herausgegebene *Graubuch Innere Sicherheit* ist ein hochwichtiges Buch über die Folgen des 11. September 2001 hinsichtlich der Sicherheitspolitik in Deutschland. Systematisch, kenntnisreich, dicht und in der Konsequenz erschreckend werden in 21 Kapiteln die Anti-Terror-Pakete und viele weitere Teile einer wachsenden Sicherheitarchitektur und des damit einher gehenden Freiheitsverlustes in unserer Gesellschaft dargestellt, analysiert und kommentiert. Das Graubuch ist eine Pflichtlektüre für alle, die sich mit den in den letzten Jahren veränderten Überwachungsmethoden und deren Auswirkungen kritisch auseinander setzen wollen. Den Herausgebern gebührt großer Dank für diese Zusammenstellung, die in ihrer Gesamtheit die Entwicklungen und Tendenzen staatlicher Überwachung in unserer Gesellschaft schonungslos offenlegt.

Fazit: Alle genannten Publikationen enthalten jeweils sehr interessante Beiträge zu den aktuellen gesellschaftlichen Entwick-

lungen in diesem Bereich. Neben den bekannten, regelmäßigen Publikationen *Vorgänge* und *Grundrechte-Report* sei insbesondere das *Graubuch Innere Sicherheit* als reich mit Quellenbezügen versehenes Referenzwerk hervorgehoben und dringend zur Lektüre empfohlen.

Vorgänge, 47 (4). Nr. 184: Der gläserne Mensch. (2008)

Till Müller-Heidelberg, Ulrich Finckh, Elke Steven, Moritz Assall, Marei Pelzer, Andrea Würdinger, Martin Kutscha, Rolf Gössner, Ulrich Engelfried (Hrsg.): Grundrechte-Report 2009. Zur Lage der Bürger- und Menschenrechte in Deutschland, Frankfurt: Fischer, 2009.

Gustav Heinemann-Initiative & Humanistische Union (Hrsg.): Graubuch Innere Sicherheit. Die schleichende Demontage des Rechtsstaates nach dem 11. September 2001. Norderstedt: Books on Demand, 2009.

Ralf E. Streibl

Von Pfeil und Bogen zum »Digitalen Bogen«

Informatik und „Dritte Welt" ist ein Thema, welches eher selten im Informatik-Kontext angesprochen wird. Auf einer technisch-statistischen Ebene kann man Host-Rechner zählen oder fragen, ob es noch Länder auf der Erde gibt, die keinen Internet-Zugang haben. Das mögen Fakten sein. Die Frage, ob das hinsichtlich des Themas weiterhilft, mag hier unbeantwortet bleiben.

Einen ganz anderen Weg geht Eliane Fernandes Ferreira. Die Ethnologin hat sich in ihrer Dissertation in überaus spannender und beeindruckender Weise in konkrete Situationen hineinbegeben und mehrfach – teilweise in mehrjährigem Abstand – die sich entwickelnde Internetnutzung bei einigen indigenen Gemeinschaften in Brasilien beobachtet und vorsichtig begleitet. In ihrer Beschreibung sind die Menschen und Gemeinschaften nicht Forschungsobjekt, sondern sie werden als aktiv handelnde Gestalter ihrer eigenen technologischen Entwicklung erkennbar. Leserinnen und Leser, die wenig über Brasilien und die dortigen Indigenen wissen, lädt das Buch zunächst kompetent und verständlich, deren Geschichte und aktuelle Lebenssituation zu verstehen. Eine Analyse der Bedeutung von Medien für Indigene weltweit und in Brasilien schließt sich an und bildet die Brücke zu einer genauen Betrachtung spezifischer Internetprojekte für und mit Indigenen in Brasilien. Die Autorin schildert gleichermaßen sorgfältig wie einfühlsam ihre Beobachtungen und Feldforschungen an verschiedenen Orten. Sie hinterfragt die Motivation der Projekte, beschreibt technische Schwierigkeiten und gibt Einblick in die Nutzung so geschaffener Internetzugänge. Dabei reproduziert sie jedoch nicht eine distanzierte Außensicht einer technologisch geprägten Welt, sondern geht mit ihrem ethnographischen Ansatz auf indigene Identität und die daraus resultierende Aneignung der neuen Technologie ein. Wünsche und Schwierigkeiten werden sichtbar und kulturelle Prozesse werden nicht isoliert, sondern deutlich eingebettet in gesamtgesellschaftliche Entwicklungen dargestellt und diskutiert.

Fazit: Die aus Brasilien stammende und seit vielen Jahren in Deutschland lebende Wissenschaftlerin hat ein außergewöhnliches Werk vorgelegt, welches gleichermaßen in seinem wissenschaftlichen Ansatz als auch durch seine einfühlsame, reflektierte Herangehensweise und Schilderung beeindruckt.

Eliane Fernandes Ferreira: Von Pfeil und Bogen zum »Digitalen Bogen«. Die Indigenen Brasiliens und das Internet. Bielefeld: transkript, 2009.

Ralf E. Streibl

Soft Skills für Softwareentwickler

Der Ruf der Praxis beeinflusst offenkundig nicht nur die Ausgestaltung von Bachelor-Studiengängen im sogenannten Bologna-Prozess, wo laut Plan ein gewisses Maß an fachunabhängigen »Schlüsselqualifikationen« in die berufsqualifizierenden Bachelor-Studiengänge integriert werden soll. Ein Indiz, dass es für entsprechende Kompetenzen einen Bedarf gibt, ist auch das Erscheinen eines Buches, das sich schon im Titel explizit an die Zielgruppe »Software-Entwickler« richtet.

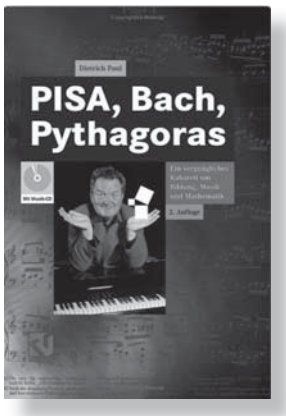
Anlass für die Entstehung des über 300 Seiten starken Bands war – wie die Autoren Uwe Vigenschow und Björn Schneider (beide lt. Selbstbeschreibung mit Hintergrund in der Software-Entwicklung und Beratung) in ihrem Vorwort schreiben – ihre Beobachtung, dass Softwareprojekte nur selten aufgrund technischer Probleme scheitern würden, sondern die Ursachen dafür meist in mangelhafter Kommunikation zu suchen seien. In fünf Teilen nähert sich das Buch dann den sogenannten *Soft Skills*, angefangen von einer Beschreibung der »Kommunikationsschnittstellen« über »Fragetechniken«, »Kommunikationsmodelle«, »Kommunikationstypen« bis »Konfliktmanagement«. Die Kapitel bereiten bekannte kommunikationstheoretische Grundlagen und bereiten diese zumeist in übersichtlicher Weise auf. Die gewählten Beispiele werden dabei auf die Zielgruppe bezogen. Ein Anhang beinhaltet sowohl Ausblicke in die zugrundeliegenden Kommunikationstheorien als auch einige einfache Übungsvorschläge. Bei der Lektüre drängt sich den Lesern vermutlich die grundsätzliche Frage auf, ob sich »Soft Skills« aus Büchern lernen lassen. Angemessene praktische und Übungen im Rahmen der Ausbildung sowie stetige Reflexion und Feedback zur eigenen Kommunikationspraxis dürften wohl für ein handlungsorientiertes Lernen wirkungsvoller sein. Dennoch stellt das Buch einen guten Versuch dar, das Thema für die Zielgruppe in systematischer und verständlicher Weise aufzubereiten.

Fazit: Als Einstieg ins Thema, aber auch als Ergänzung zu praktischen Bildungsveranstaltungen und Eigenreflexion ein hilfreiches Buch.

Uwe Vigenschow & Björn Schneider: Soft Skills für Softwareentwickler. Heidelberg: dpunkt, 2007.

Ralf E. Streibl

PISA, Bach, Pythagoras



Schon etwas älter – aber unverändert lesenswert – ist das Buch *PISA, Bach, Pythagoras* von Dietrich Paul, manchen vielleicht eher bekannt unter seinem Alter Ego »Piano Paul« unter er dem seit 1988 verschiedene Kabarett-Programme mit Musik gestaltet hat (Auftritte im gesamten deutschsprachigen Raum, u.a. in der Münchner Lach- und Schießgesellschaft und im Scheibenwischer). Der promovierte Autor war viele Jahre in Forschung und Lehre in Mathematik tätig. Und hier ergibt sich die Brücke für die hier empfohlene Veröffentlichung.

2005 erstmalig und 2008 (im Jahr der Mathematik) in einer verbesserten zweiten Auflage erschienen legt der Autor ein verschriftliches Kabarettprogramm vor, das in hohem Maße für alle unterhaltsam ist, die eine gewisse Affinität zu Mathematik und Musik aufweisen – allzu große Vorkenntnisse sind für die Lektüre aber nicht erforderlich. Schritt für Schritt führt »Piano Paul« kurzweilig und kenntnisreich von einfachen Melodien zur komplexen Polyphonie, nicht ohne unterhaltsame Besuche bei Kombinatorik und Mengenlehre. Nebenbei erfährt man auch noch, warum es im Sommer warm und im Winter kalt ist sowie über die Kunst der Fuge. Reizvoll wird dieser Spaziergang durch zahlreiche Fußnoten, die reflexiv bis rekursiv das dokumentierte Kabarettprogramm kommentieren sowie durch die vielen eingestreuten, zwischen feiner Ironie und herber Polemik angesiedelten Seitenbemerkungen zu PISA, Bildung und dem ganzen Rest.

Fazit: Eine unterhaltsame Lektüre für alle, die Lust haben, bei Kabarett noch mit- und um die Ecke zu denken. Durch geschickte Wahl der Kapitel und Fußnoten kann die Leserin bzw. der Leser selbst entscheiden, wie tief sie oder er in Mathematik oder Musik einsteigen möchte.

Dietrich Paul: PISA, Bach, Pythagoras. Ein vergnügliches Kabarett um Bildung, Musik und Mathematik. 2. Auflage. Wiesbaden: vieweg, 2008 (incl. Musik-CD).

Meldungen: Kooperation für den Frieden / Friedensbewegung

FIfF Mitglied im Kooperationsrat

Seit 2009 ist das FIfF Mitglied der *Kooperation für den Frieden*. Die darin zusammengeschlossenen Gruppen und Organisationen haben das Ziel, in einem gleichberechtigten Dialog politische Stellungnahmen zu entwickeln und auf deren Grundlage gemeinsame Aktionen und Kampagnen ins Leben zu rufen. Sie setzen sich ein für eine aktive Friedensbewegung, die langfristig und strategisch denkt, aber auch schnell und dabei demokratisch abgestimmt handelt. In dem Ende Oktober neu gewählten Kooperationsrat – dieser koordiniert die kontinuierliche Arbeit – ist das FIfF seitdem gemeinsam durch Dietrich Meier-Ebrecht und Ralf E. Streibl vertreten.

www.koop-frieden.de

Friedenskultur.2010

2010 ist ...

- 65 Jahre nach dem 8. Mai 1945
- 65 Jahre nach den Atombomben-Abwürfen auf Hiroshima und Nagasaki
- 60 Jahre nach dem Stockholmer Appell zum Verbot von Atomwaffen
- 55 Jahre nach dem Russel-Einstein-Manifest „Eine Welt ohne Krieg“ (vgl. Kasten)
- 50 Jahre nach dem ersten deutschen Ostermarsch
- Ende der von der UN-Generalversammlung erklärten »Internationalen Dekade für eine Kultur des Friedens und der Gewaltfreiheit für die Kinder dieser Welt« (2001-2010)

Vom 3. bis 28. Mai 2010 ist New York Ort der Überprüfungskonferenz zum Atomwaffensperrvertrag (Nuclear Non-Proliferation Treaty - NPT). Bereits am 19.-21. März 2010 findet vor diesem Hintergrund in Essen ein internationaler Kongress *Friedenskultur.2010 – Unseren Zukunft atomwaffenfrei* statt (Programm und weitere Informationen unter *www.friedenskultur2010.de*). Und noch vorher, am 12. und 13. Februar 2010, lädt die *Kooperation für den Frieden* zu ihrer *Strategiekonferenz 2010* nach Heidelberg ein.

FIfF e.V.

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

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

Das FIfF-Büro

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

Die aktuellen Bürozeiten entnehmen Sie bitte unseren Webseiten.

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

FIfF im Netz

Das ganze FIfF:
www.fiff.de

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

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

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

Beirat

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

FIfF-Vorstand

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

Impressum

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

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

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

Aktuelle Ankündigungen

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

CCC: 26C3: Here Be Dragons
26th Chaos Communication Congress
27. - 30.12.2009 in Berlin
https://events.ccc.de/congress/2009/

Big Brother Award 2010
Nominierung bis 15.7.2010
www.bigbrotherawards.de

26. FIfF-Jahrestagung
»Arbeitnehmerdatenschutz«
5. - 7.11.2010 in Köln

KIF 38: Konferenz der Informatikfachschaften
26. - 30.05.2010 in Dresden

FIfF-Kommunikation

1/2010 – »Verantwortung 2.0«
H.-J. Kreowski, R.E. Streibl u.a. (Redaktionsschluss: 2.2.2010)

2/2010 – »Netzpolitik«
Stefan Hügel u.a.
(Redaktionsschluss: 4.5.2010)

3/2010 – »Arbeit und EDV«
Peter Bittner, Klaus Hess, Katharina Just-Hahn
(Redaktionsschluss: 4.8.2010)

4/2010 – »Verkehr«
Wolfgang Hesse u.a.
(Redaktionsschluss: 4.11.2010)

W&F – Wissenschaft & Frieden:

1/10 – Intellektuelle und Krieg
2/10 – Ambivalenzen des Islam

DANA – Datenschutz-Nachrichten:

4/09 – BigBrotherAwards 2009

Das FIfF-Büro

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

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

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

Schluss FIfF

»Herausforderungen«: Angesichts der Tatsache, dass der bisherige Bundesinnenminister, geehrt mit dem BigBrotherAward 2009 für sein Lebenswerk, sein Amt verlassen hat, wird händeringend jemand benötigt, der sich ebenso passioniert für die Sicherheit in Deutschland einsetzt. Die FIfF-Kommunikation ist froh und stolz, für die Suche das passende Instrument (entwickelt und gestaltet 2008 von Sebastian Rave) präsentieren zu können.

Aus der Spielanleitung:

Deutschland im Jahre 2008: Terroristen, Raubkopierer, Extremisten und Verbrecher gefährden unbescholtene Bürger. Es gibt nur eine Möglichkeit, sie zu stoppen: Rechte müssen beschnitten, Freiheiten beschränkt und Geheimnisse vor dem Staat gelüftet werden. Helfen Sie mit, Deutschland zu retten und toben Sie sich richtig aus! Aber nehmen Sie sich in Acht: Bringen Sie nicht das fragile Konstrukt aus Grundrechten zum Einsturz Chaos und Anarchie wären die Folge!

Zunächst muss das Kartenhaus der Grundrechte aber noch aufgebaut werden. Dies fordert ein wenig Geduld, immerhin haben ganze Generationen ein Leben lang dafür gekämpft.

(...)

Suchen Sie sich ein Grundrecht aus, das Ihnen besonders gefährlich vorkommt. Welches Recht könnten Feinde der Freiheit und der Demokratie für ihre Zwecke missbrauchen? Sobald Sie die potentielle Gefährdung ausgemacht haben, versuchen Sie ganz vorsichtig, die Karte aus dem Haus zu ziehen. Keine Sorge, Sie tun nichts Verbotenes, das Grundgesetz sieht die Einschränkung der Grundrechte im Notfall vor und um den handelt es sich ja zweifelsfrei.

Haben Sie es geschafft? Herzlichen Glückwunsch Ihr erster Eingriff in die Grundrechte! Suchen Sie sich gleich das nächste Recht und versuchen Sie vorsichtig, es aus dem Haus zu entfernen.

Sollte das Haus zusammenbrechen ist der nächste Spieler am Zug – oder, wenn Sie alleine sind, versuchen Sie es einfach nochmals. Bauen Sie die Grundrechte mühsam wieder auf und greifen Sie erneut ins Grundrecht ein. Oder, wenn Ihnen danach ist, versuchen Sie einfach mal andere Spielmodi, zum Beispiel »1933«: Statt vorsichtig und einzeln Grundrechte einzuschränken, werfen Sie einfach direkt das Kartenhaus um! Ihrer Phantasie sind keine Grenzen gesetzt.

Sebastian Rave *ist ein 27-jähriger Mediengestalter, der zur Zeit in Japan lebt. Neben seiner Begeisterung für alles Multimediale und Interaktive ist er außerdem damit beschäftigt, den Kapitalismus abzuschaffen und ihn durch eine menschenwürdige Gesellschaft zu ersetzen. Bisher vergeblich.*

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