H 7625

# FIfF-Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

30. Jahrgang 2013 Einzelpreis: 7 EUR

3/2013 – September 2013

# Weltweite Datenausspähung

# Informatik und Bildung

ISSN 0938-3476

• Biometrie • Panic Button • FIfF-Jahrestagung •

FIfF-Kommunikation

Titelbild: Bad Aibling Station, Dr. Johannes W. Dietrich
Wikimedia Commons, CC-BY-2.0

*Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.*

# Inhalt

Ausgabe 3/2013

inhaltt

# Editorial

*Wissen ist Macht!* Mit diesem alten Spruch wird gerne die Notwendigkeit umfassender Bildung begründet. Doch neben dem bereits lange geplanten Schwerpunkt dieses Hefts zu *Informatik und Bildung* können wir ihn auch auf unseren ungeplanten zweiten Schwerpunkt beziehen, mit dem wir die aktuellen – erschreckenden – Nachrichten der vergangenen Wochen verarbeiten: Der Skandal um die allem Anschein nach *weltweite Ausspähung* der Bevölkerung, der Wirtschaft und der politischen Entscheidungsträger durch Geheimdienste. Auch hier geht es letztlich darum, Macht auszuüben – dass das gelingt, zeigt vielleicht auch die zurückhaltende Reaktion der deutschen Bundesregierung.

Den Anstoß zu den Nachrichten geben die Enthüllungen des ehemaligen NSA-Mitarbeiters Edward Snowden. Mittlerweile verliert man leicht den Überblick über die in steter Folge veröffentlichten Berichte zur Überwachung. Gleichzeitig bleibt so das Thema in der öffentlichen Debatte – sicherlich auch dank einer geschickten Publikationsstrategie. *Sara Stadler* hat die *Ereignisse der letzten Wochen* nochmals chronologisch zusammengestellt.

Viele Statements unterschiedlicher bürgerrechtlicher Organisationen wurden in diesem Zeitraum veröffentlicht. Auch das zeigt die Bedeutung des Themas für die Bürgerrechte – und auch hier verliert man mittlerweile leicht den Überblick. Für dieses Heft haben wir zwei Statements ausgewählt, die auch vom FIfF unterstützt werden: Das *Washington Statement*, in dem Datenschutzaktivisten aus den USA, aus Kanada und aus Europa die EU-Politiker auffordern, durch hohe Datenschutzstandards die Privatsphäre der Menschen zu sichern. US-Präsident Obama wird in einem Brief, den ca. 160 Organisationen weltweit unterzeichnet haben, aufgefordert, die Verfolgung Edward Snowdens aufzugeben und den Schutz für Whistleblower sicherzustellen.

*Oliver Degner* betrachtet den Ausspähskandal in seinem Beitrag *Die NSA, die Bespitzelung und die Ethik* unter ethischen Gesichtspunkten. Aus seiner Sicht benötigen wir Geheimdienste wie die NSA, doch *„die Begründung, dass die umfassende Überwachung aller Verdächtigen, also* aller *Bürgerinnen und Bürger dadurch legitimiert wird, dass Terroranschläge ‚wahrscheinlich' verhindert werden könnten ist fragil"*, stellt er zurückhaltend fest. *„Die Massensammlung und -verarbeitung von Daten durch die NSA und das passive Zusehen der Bundesregierungen entfernt uns derzeit vom liberalen Rechtsstaat und führt uns zu einer unkontrollierten Orwellschen Präventionsgesellschaft"*, so Degner weiter.

*In welchem Europa wollen wir leben?* fragt *Dagmar Boedicker* anschließend und fordert politische Konsequenzen. *„Gerade jetzt, wenn die USA auf einen Vertrag über* Transatlantic Trade and Investment Partnership (TTIP) *drängen, während sie mit* Prism, XKeyscore, Lopers, Juggernaut *und Co. ihre Partner bespitzeln, gerade jetzt muss die EU hart bleiben: Keine weiteren Verhandlungen über TTIP ohne umfassende Aufklärung über die Spionage- und Überwachungsaktivitäten und strenge, kontrollierbare Regelungen zum Datenschutz."*

*Big Data* ist der aktuelle Trend in der IT – und die methodische Grundlage für die Ausspähung. *Björn Schembera* setzt sich in seinem Beitrag *Big Data: Big Business, Big Brother, Big Chances?* kritisch damit auseinander. *Kai Nothdurft und Sylvia Johnigk* untersuchen die Rolle, die *US-Firmen bei der Datenausspähung* spielen: Wie glaubwürdig sind deren Beteuerungen, nichts von der Überwachung gewusst zu haben? In einem weiteren Beitrag untersuchen sie die Beteuerungen und Verlautbarungen der US-amerikanischen Behörden auf ihren bürgerrechtlichen Gehalt. Dabei ziehen sie Parallelen zu dem einige Jahre zurückliegenden Fall des Unternehmens *Inslaw* und der dort erstellten Software PROMIS.

Den Abschluss dieses Schwerpunkts bildet die Betrachtung von *Klaus Fuchs-Kittowski* zur *Ethik des Whistleblowing*. *„Sie haben in der Tat Verrat gegenüber ihren Auftraggebern und ihrem Vaterland verübt"*, stellt er zum Handeln von Chelsea (vormals Bradley) Manning und Edward Snowden fest, aber: *„Die weltgeschichtliche Bedeutung ihrer Entscheidung sollte deutlich genug sein und ihr muss eine höhere Präferenz beigemessen werden, denn sie besaß für die getroffene Entscheidung offensichtlich größere Kraft, als die Verpflichtung zur individuellen Loyalität gegenüber den nationalen Institutionen."* Er fordert Solidarität für beide Whistleblower.

Passend zum Schwerpunkt unsere Retrospektive: *Manfred Domke* setzte sich bereits 1990 mit der *Trennung der Verantwortung für militärisch-geheimdienstliche und zivile Informationssicherheit am Beispiel der USA* auseinander.

Der zweite, ursprünglich geplante Schwerpunkt, das Thema *Informatik und Bildung* spannt einen weiten, facettenreichen Bogen über zumindest zwei wesentliche Bereiche. Zum einen geht es darum, was Informatik konzeptionell, methodisch und von der Werkzeugunterstützung her zur Bildung beitragen kann, wobei insbesondere die digitalen Medien eine besondere Rolle spielen. Für diesen Gegenstandsbereich wird häufig der Begriff *eLearning* verwendet. Zum anderen drängt sich immer wieder neu die Frage auf, wie Bildung und Ausbildung in der Informatik sinnvoll gestaltet und weiterentwickelt werden können. Der Schwerpunkt Bildung in diesem Heft kann die Thematik in ihrer Gesamtheit nicht systematisch erfassen, aber mit seinen sieben Beiträgen ein paar Schlaglichter setzen.

In ihrem Artikel diskutieren *Iris Bockermann*, *Nadine Dittert* und *Heidi Schelhowe*, wie digitale Medien nicht nur eingesetzt, sondern im universitären Bildungsprozess im Sinne einer Medienkompetenz be-greifbar gemacht werden können. Die Beiträge von *Berthold Hoffmann*, *Lutz Frommberger* und *Klaus Fuchs-Kittowski* sind ebenfalls auf konkrete Lehrveranstaltungskonzepte bezogen – jeweils mit besonderen gesellschaftlichen Bezügen. *Berthold Hoffmann* berichtet von einer Lehrveranstaltung über Programmiersprachen und Compilerbau, die er an der Uni-

versität Maroua im Norden Kameruns gehalten hat, und ihre Einbettung in das dortige Informatikstudium, das sich vom Anspruch her nicht allzu stark von dem in Deutschland unterscheidet, aber unter extrem schwierigen Bedingungen realisiert werden muss. *Lutz Frommberger* stellt ein studentisches Projekt vor, in dem ein System zur besseren Kommunikation bei Naturkatastrophen in Laos entwickelt und vor Ort getestet worden ist. Beide Artikel stellen eindrucksvolle Beispiele dar, dass aus der Informatik heraus Entwicklungshilfe möglich ist. Der Beitrag von *Klaus Fuchs-Kittowski* skizziert eine Lehrveranstaltung mit Vorlesung, Seminar- und Projektarbeit zum Thema *Umweltinformatik und Gesellschaft* an der Hochschule für Wirtschaft und Technik in Berlin. Für ihn ist das Fachgebiet *Informatik und Gesellschaft* ein unverzichtbarer Teil der Informatik in Lehre und Forschung. *Andrea Wagner* hat in ihrer Rede auf der Absolventenfeier der Angewandten Informatik an der Hochschule Fulda, die hier abgedruckt ist, ebenfalls ein flammendes Plädoyer für das Lehrgebiet *Informatik und Gesellschaft* gehalten. *Reinhard Keil, Harald Selke und Felix Winkelnkemper* sehen das weitaus skeptischer. Sie diskutieren die Frage, ob und wie die Informatik überhaupt mit ausreichender wissenschaftlicher Kompetenz den Ansprüchen gerecht werden kann, die sich aus einer „und"-Verbindung mit Bildung, Gesellschaft oder Verantwortung ergeben. Schließlich bespricht, kommentiert und interpretiert *Bernard Robben* Bücher von Bernard Stiegler, in denen aus philosophischer Sicht die essentielle Rolle von Medien für die Bildung beleuchtet wird, was in neuerer Zeit vor allem die Rolle der digitalen und computergestützten Medien betrifft.

Neben den beiden Schwerpunkten halten wir Vorausschau auf die Ende Oktober in Siegen stattfindende Jahrestagung, die in diesem Jahr unter dem Motto *Cyperpeace – Frieden gestalten mit Informatik* steht. *Peter Bittner* untersucht in seinem Beitrag *Wenn der Mensch vermessen zur Information wird … über Biometrie im Masseneinsatz und ihren Grenzen* Eigenschaften und Grenzen der Biometrie. Der Beitrag bildet den Auftakt zur geplanten Reihe weiterer Beiträge zu diesem Thema. *Ralf Rebmann* berichtet von einem Notrufsystem für Menschenrechtsaktivisten. Ein Memorandum zu Abschaffung des Verfassungsschutzes – umso mehr nach der NSU-Affäre – haben *Humanistische Union*, *Internationale Liga für Menschenrechte* und der *Bundesarbeitskreis kritischer Juragruppen* veröffentlicht. Dazu kommen die Rubriken *Faire Computer* und das Log *3/2013* der bürgerrechtsrelevanten Ereignisse – auch außerhalb von PRISM, Tempora und XKeyscore ist einiges passiert. Im FIfF-Teil sei vor allem auf den Bericht aus unserer Geschäftsstelle in Bremen hingewiesen. Rezensionen, unter anderem zu den Bänden *Jenseits von 1984* und *Digitale Demenz*, runden die Ausgabe ab.

Wir wünschen unseren Leserinnen und Lesern eine interessante und anregende Lektüre – und viele neue Erkenntnisse und Einsichten.

*Hans-Jörg Kreowski und Stefan Hügel*
*für die Redaktion*

**Aus der Redaktion**

# FIfF-Kommunikation digital

## Ein Test

Liebe Leserinnen und Leser der *FIfF Kommunikation*,

wir haben im Frühjahr dieses Jahres begonnen, mit der Umsetzung der Printausgabe der *FIfF Kommunikation* in eine digitale Ausgabe im ePub-Format zu experimentieren. ePub ist ein gängiges Format für eBook-Lesegeräte. Tablet-Computer bieten geeignete Apps für dieses Format an. Zum Testen stehen inzwischen die FK 1/2013 und die FK 2/2013 bereit. Eine digitale Testausgabe des vorliegenden Heftes wird in Kürze erscheinen.

Angesichts unserer sehr begrenzten Ressourcen kann das Experiment nur gelingen, wenn wir den Produktionsprozess sehr effizient durchgestalten können. Das heißt, wir können uns nicht den Luxus leisten, die digitale Ausgabe optimiert für die Darstellung auf Lesegeräten oder mit eBook-Apps neu zu setzen. Wir nutzen statt dessen die (nicht in jedem Punkt befriedigenden) Möglichkeiten, die uns die Layout-Software bietet, die Druckausgabe bereits im ePub-Format zu exportieren, und versuchen den Nacharbeitungsaufwand zu minimieren – in der Hoffnung, dass das Ergebnis akzeptabel wird und die besonderen Optionen von eBook-Readern (Textinteraktion, Hyperlinks etc.) so weit es geht genutzt werden können.


Wenn Sie und ihr, liebe Leserinnen und Leser, Interesse haben, die *FIfF Kommunikation* in Zukunft – neben der Druckausgabe oder sogar stattdessen – als digitale Ausgabe zu beziehen, möchten wir um Ihre und eure Mithilfe werben: Schaut die Testausgaben an, lest probeweise darin – und teilt uns mit, was gefällt, was verbesserungsbedürftig ist und was vermisst wird! FIfF-Mitglieder können die Testversionen per Email über unsere Geschäftsstelle beziehen, Bestellungen bitte an *shop@fiff.de* mit der Angabe, welche Ausgabe(n) gewünscht werden. Weitere Informationen sind auf unserer Wiki-Seite *wiki.fiff.de/wiki/FKePub* zu finden.

**Brief an das FIfF**

# Der Traum ist aus


*Gibt es ein Land auf der Erde / wo der Traum Wirklichkeit ist?*
*Ich weiß es wirklich nicht.*
*Ich weiß nur eins / und da bin ich sicher*
*dieses Land ist es nicht.*
*(Ton Steine Scherben, Rio Reiser, 1972)*

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

es gibt historische Tage, deren Datum in das kollektive Gedächtnis der Menschen übergeht. Sie markieren geschichtliche Meilensteine – Tage, an denen sich Katastrophen ereignen, Tage, an denen sich – vielleicht nur ein wenig – die Richtung der Geschichte ändert, im Negativen oder im Positiven. Solche Tage waren der 6. August 1945, der 13. August 1961, der 9. November 1989 oder der 11. September 2001.

Vielleicht werden wir auch den 6. Juni 2013 einmal so sehen – obwohl an diesem Tag eigentlich nichts Besonderes passiert ist. Es war der Tag, an dem wir einer Illusion beraubt wurden: der Illusion der freien Kommunikation im Internet als eines Grundbausteins der freiheitlichen Demokratie.

Am 6. Juni 2013 wurden erstmals Unterlagen veröffentlicht, die auf eine umfassende Überwachung der Bevölkerung durch den US-amerikanischen Geheimdienst NSA – die *National Security Agency* – hinweisen. In den folgenden Wochen wurden immer weitere Enthüllungen öffentlich – über die Ausspähung durch die NSA, durch den britischen Geheimdienst GCHQ, zuletzt gab es Berichte über eine intensive Zusammenarbeit mit dem deutschen Bundesnachrichtendienst. Auch die anfänglichen Beteuerungen, die Überwachung würde sich im Rahmen des geltenden Rechts bewegen, wurden zunehmend angezweifelt. Was wäre das aber auch für ein Recht, das eine solche umfassende Ausspähung zulässt?

Die Reaktionen der verantwortlichen Bundesregierung waren auffällig verhalten. Artig fragte man bei den USA an, ob sie denn wohl deutsches Recht gebrochen hätten. Auf weitere Nachfragen erklärten Regierungsvertreter, sie wüssten von nichts. Am Ende wurde das Thema noch zum Wahlkampftheater, bevor Kanzleramtsminister Ronald Pofalla die Affäre kurzerhand für beendet erklärte.

In einem Interview hatte Bundesinnenminister Hans-Peter Friedrich die Datenausspähung bereits gerechtfertigt:

> *„Dieser edle Zweck, Menschenleben in Deutschland zu retten, rechtfertigt zumindest, dass wir mit unseren amerikanischen Freunden und Partnern zusammenarbeiten, um zu vermeiden, dass Terroristen, dass Kriminelle in der Lage sind, unseren Bürgern zu schaden."*

Angesichts der historischen Erfahrungen, die Menschen in Deutschland mit der Überwachung gemacht haben – zuletzt durch das Ministerium für Staatssicherheit der ehemaligen DDR – sind diese Reaktionen mindestens befremdlich. Umso mehr, als sowohl Bundespräsident Gauck als auch Bundeskanzlerin Merkel Erfahrungen mit dieser Ausspähung in der DDR machen mussten – und sonst auch nicht müde werden, sie zu verurteilen. Auffällig auch, auf welche Art von Überwachung politisch Verantwortliche reagieren: Wenn sie selbst überwacht werden, oder wenn es um Wirtschaftsspionage geht. Der Schutz der Bevölkerung ist da offenkundig weniger wichtig – der Schutz des deutschen Volkes, für das die Bundesregierung geschworen hatte, „Schaden von ihm (zu) wenden".

Doch kam das alles wirklich so überraschend? Viele netzpolitisch Aktive hatten immer wieder auf die Möglichkeiten umfassender Überwachung hingewiesen – das wurde stets als „Verschwörungstheorie" abgetan. Erst letztes Jahr veröffentlichte Professor Josef Foschepoth den Band *Überwachtes Deutschland*, in dem er die umfassende Post- und Telefonüberwachung in der „alten" Bundesrepublik untersucht hat – Überwachung, die offenbar von allen damaligen Bundesregierungen, teilweise unter bewusstem, offenem Verfassungsbruch zugelassen und unterstützt wurde. Selbstverständlich immer formaljuristisch korrekt – die juristischen Konstruktionen, die die Überwachung legitimieren sollten, waren der Untersuchung zufolge äußerst phantasievoll. Besatzungsrecht – das formal über der Verfassung stand – wurde auf Wunsch der deutschen Bundesregierung aufrechterhalten, um die Überwachung der eigenen Bevölkerung zu legitimieren.

1968 – ausgerechnet – wurde die Überwachung durch das G10-Gesetz formal festgeschrieben. Doch die Nachrichtendienste können weitgehend im Geheimen agieren – die parlamentarische Kontrolle ist offensichtlich ineffektiv, wie auch die Affäre um den *Nationalsozialistischen Untergrund* bereits eindrücklich gezeigt hat.

Zur Jahrtausendwende war die Überwachung durch US-Geheimdienste in der öffentlichen Diskussion – das System *Echelon*, im idyllischen Bad Aibling, wurde damals zu Ausspähung genutzt. Doch, wie wir heute sehen, war die damalige Debatte im Wesentlichen folgenlos. Auch dieses Mal wird der Bevölkerung ein Placebo verabreicht: eine Verwaltungsvereinbarung, die dem Vernehmen nach seit 1990 nicht mehr angewandt worden war, wird außer Kraft gesetzt. Gleichzeitig wurden Überwachungsvorhaben weiter vorangetrieben: Vorratsdatenspeicherung, Bestandsdatenauskunft, Online-Ausspähung. Dem ehemaligen Bundesinnenminister Otto Schily – dessen früher beachtlicher bürgerrechtlicher Ruf seit der Zeit seines Ministeramts arg ramponiert ist – haben wir die Feststellung zu verdanken, dass die Vorratsdatenspeicherung nichts anderes als die Ausspähprogramme der Geheimdienste sei – eine Erkenntnis, die seiner eigenen Partei überhaupt nicht ins Konzept passte.

Doch was muss nun geschehen? Von der nächsten Bundesregierung erwarte ich, dass sie klar gegen die Ausspähung nicht nur der politischen Institutionen und der Wirtschaft, sondern auch gegen die Ausspähung der Bevölkerung Stellung bezieht – nach innen und nach außen. Nach innen müssen die notwen-

digen gesetzlichen Regelungen geschaffen und effektive Institutionen zu ihrer Durchsetzung eingerichtet werden: Ein effektives Datenschutzrecht, das weder durch wirtschaftliche noch durch politische Lobbies verwässert werden darf. Effektive parlamentarische Kontrolle der Geheimdienste. Aufgabe der Gesetzesinitiativen zur Ausspähung der Bevölkerung, wie Vorratsdatenspeicherung und Bestandsdatenauskunft. Nach außen muss umfassende Aufklärung und Rücknahme der Ausspähung eingefordert werden. Es kann nicht sein, dass vor unseren Augen und mit Genehmigung deutscher Behörden Überwachungszentralen neu errichtet werden, wie es derzeit in Wiesbaden geschieht. Die Verhandlungen über einen Vertrag über ein *Transatlantic Trade and Investment Partnership (TTIP)* müssen bis zur umfassenden Aufklärung und beiderseitigen Vereinbarungen über ein Ende der Ausspähung ausgesetzt werden.

Verschiedentlich wurde bemerkt, dass die deutsche Bevölkerung von ihrer eigenen Ausspähung ja profitiere. „*Kampf gegen den Terror, wissenschon.*" Erich Kästner schrieb 1933:

> *„Was immer geschieht! Nie dürft Ihr so tief sinken, von dem Kakao, durch den man Euch zieht, auch noch zu trinken."*
>
> *[Erich Kästner: Gesang zwischen den Stühlen, 1933]*

Prägnant formulierte der letzte Minister für Staatssicherheit der DDR, Erich Mielke, die Einstellung, uns durch fürsorgliche Überwachung schützen zu wollen. Vor der Volkskammer erklärte er 1989:

> *„Ich liebe – Ich liebe doch alle – alle Menschen – Na ich liebe doch – Ich setze mich doch dafür ein."*

Damals lachten wir über den augenscheinlich verwirrten alten Mann. Heute sollten wir aus der Geschichte lernen.

Eine andere, ein wenig traurige Nachricht erreichte uns ebenfalls aus den USA. CPSR – *Computer Professionals for Social Responsibility* – wurde offenbar aufgelöst, nachdem, zumindest wenn man die Web-Site *www.cpsr.org* betrachtet, bereits in den letzten Jahren die Aktivitäten merklich zurückgegangen waren. CPSR spielte eine wesentliche Rolle bei der Gründung des FIfF und war praktisch dessen Mutterorganisation, besonders durch das Engagement von Joseph Weizenbaum.

Nachdenklich muss uns dabei auch ein Absatz der Erklärung zur Auflösung stimmen, in dem es heißt:

> *„Apparently, as many people know, the age of the participatory membership organizations is over – their numbers are certainly way down – and we in CPSR had certainly noticed that trend. I personally suspect that this development is not necessarily a good thing."*

Tatsächlich beobachten wir seit längerem eine Professionalisierung der Bürgerrechtsarbeit bei unseren Partnerorganisationen. Doch während dies sicherlich die politische Schlagkraft erhöht und damit eine gute Entwicklung sein kann, wäre es bedauerlich, wenn dabei die Partizipation der Mitglieder verloren ginge. Demokratie lebt vom Mitmachen – und vom Mit*entscheiden*! Auch das FIfF wird sich einer (behutsamen) Professionalisierung stellen (müssen) – wir tragen dem Rechnung, indem wir verstärkt inhaltliche Themen in der Geschäftsstelle ansiedeln. Doch die Idee einer ehrenamtlich getragenen Mitgliederorganisation wollen wir (noch) nicht aufgeben. *„I certainly would welcome another membership organization with CPSR's Big Tent orientation."* Ich auch. Wie notwendig sie ist? Siehe oben.

Mit FIfFigen Grüßen

*Stefan Hügel*

**FIfF e.V.**

# Arbeitskreis RUIN – RUestung und INformatik – wieder gegründet

## Experten des FIfF kritisieren zunehmende informatikgestützte Kriegsführung

*In Bremen hat sich am Sonntag, 9. Juni 2013, der Arbeitskreis RUIN – RUestung und INformatik – des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) wieder gegründet. Das FIfF bündelt damit seine umfassende Expertise zu diesen Themen, um Öffentlichkeit, Wissenschaft, Wirtschaft und politische Entscheidungsträger über die Risiken der Informatiknutzung in der Rüstung zu informieren und den Einfluss der Zivilgesellschaft auf sicherheitspolitische Prozesse geltend zu machen.*

Der Computereinsatz in der Kriegführung nimmt auch heute noch ständig zu. Dabei wird suggeriert, dass beispielsweise durch den Einsatz unbemannter Drohnen eine gezielte, „saubere" Kriegführung möglich ist – dies ist aber eine Illusion, wie große Opfer in der Zivilbevölkerung immer wieder zeigen. Auch der Cyberwar – elektronische Kriegführung, bei der gegnerische Computersysteme durch Schadsoftware lahmgelegt werden – birgt erhebliche Risiken auch für die Zivilbevölkerung. Solche „Kampfviren" machen keinen Unterschied zwischen zivilen und militärischen Zielen. Sind sie erst einmal in der Welt, ist kaum mehr zu kontrollieren, welche Systeme sie schädigen. Cyberwar nimmt die Sabotage und den Ausfall lebenswichtiger ziviler Systeme – etwa in Krankenhäusern – in Kauf.

Zum Cyberwar zählen die Experten des FIfF auch die umfassende Ausspähung des Internet durch Initiativen wie das US-amerikanischen Projekt PRISM. Dieses und die anderen bekannt gewordenen Spionagesysteme setzen die Ausforschung der Bevölkerung durch das bereits seit langem bekannte System Echelon fort und erweitern sie. Sie dienen der militärischen und geheimdienstlichen Aufklärung und durchforsten dafür weltweit die Kommunikation von Millionen völlig unbeteiligter Internet-

nutzer. Diese umfassende Spionage durch US-Regierungsbehörden und die Hackerattacken aus China sind Belege für den heute alltäglichen Cyberwar. Dem Internet als ziviler Raum für Kommunikation und Handel werden damit die Grundlagen von Vertrauen und Sicherheit entzogen. Das zeigt auch eindringlich die Bedeutung eines starken europäischen Datenschutzes, wie sie durch die EU-Datenschutz-Grundverordnung angestrebt wird. Gerade aus den USA wird aber versucht, die Bestimmungen durch massive Lobbyarbeit zu verwässern und damit den Schutz der Bevölkerung vor Überwachung weiter zu verringern.

Der Arbeitskreis RUIN wird das Thema Cyberwar ganzheitlich behandeln. Die Nutzung der Informatik zur Kriegführung im Äußeren und zur Überwachung der Bevölkerung im Inneren sind letztendlich nur zwei Seiten derselben Medaille. Ebenso wie Konflikte zwischen Staaten stehen heute innerstaatliche Konflikte im Brennpunkt. Im arabischen Frühling hat sich gezeigt, wie Überwachungstechnik – auch aus Deutschland – zur Unterdrückung von Freiheitsbewegungen durch diktatorische Regimes eingesetzt wird. Das FIfF wendet sich deswegen gegen Exporte von Rüstungs- und Überwachungstechnik.

Der Arbeitskreis RUIN wird durch Öffentlichkeitsarbeit, in Fachpublikationen und auf Tagungen seine Expertise nutzen, um die Öffentlichkeit und politische Entscheidungsträger im Sinne einer friedlichen Nutzung der Informationstechnik zu informieren und seine Positionen deutlich zu machen. Die diesjährige Jahrestagung des FIfF, die vom 25. bis 27. Oktober 2013 in Siegen stattfindet, steht unter dem Motto *Cyberpeace – Frieden gestalten mit Informatik*. Außerdem sind Schwerpunkthefte der *FIfF-Kommunikation*, eine Buchveröffentlichung und interdisziplinäre Konferenzen geplant.





**Sara Stadler**

## Zivilklausel der Universität Bremen – lebendiges Leitziel oder unnötiger Ballast?

*Bericht über eine Veranstaltung der Arbeitsgruppe Theoretische Informatik an der Universität Bremen und der FIfF-Regionalgruppe Bremen am 13. Juni 2013*

Die Verflechtung von Rüstung und Informatik ist seit seiner Gründung eines der zentralen Themen des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF). Ein Thema das nicht an Aktualität verliert, solange die Informationstechnologie beständig zur Weiterentwicklung der Militärtechnologie beiträgt. Dass an dieser Verflechtung die Hochschulen alles andere als unbeteiligt sind, nahmen die Arbeitsgruppe Theoretische Informatik an der Universität Bremen und die FIfF-Regionalgruppe Bremen zum Anlass, am vergangenen Donnerstag im Rahmen der antimilitaristischen Aktionstage, über das Für und Wider von universitären Zivilklauseln[1] zu diskutieren.

Die Titelfrage *Zivilklausel der Universität Bremen – lebendiges Leitziel oder unnötiger Ballast?* beantwortete der vortragende Prof. Dr. Hans-Jörg Kreowski direkt zu Anfang seines Vortrages: „Das Militär hat in der Bildung nichts verloren. Deshalb bin ich für eine Zivilklausel."

Dem aktuellen Trend, Krieg wieder salonfähig zu machen – sei es über Bundeswehr-Karriere-Trucks an Schulen und Arbeitsämtern, Bundeswehr-Briefmarken in den Postfilialen oder universitäre Forschung für die Rüstungsindustrie – gelte es ein klares *Nein* entgegenzusetzen.

Im Folgenden stellte Hans-Jörg Kreowski die Geschichte der Zivilklausel an der Universität Bremen von ihren Anfängen in der Mitte der 80er Jahre über ihr beständiges Infragestellen und ihre erneute Bestätigung – zuletzt am 25. Januar 2012 – dar. Dem aktuellen Bekenntnis zur Zivilklausel, welches mit einer großen Mehrheit erfolgt war, stellte er die tatsächlich immer wieder bekannt werdenden Verstöße dagegen gegenüber. Da es selbst Uni-intern keine vollständigen Listen über laufende Forschungsprojekte gäbe, sei es zudem schwer, solche Verstöße bekannt zu machen geschweige denn, sie zu verhindern.

In einem Exkurs wies Kreowski auf die besondere Relevanz einer Zivilklausel in Bezug auf die Informatik hin, indem er ihren Anteil an der Entwicklung sogenannter autonomer Waffen skizzierte.

In die anschließende Diskussion trug er unter anderem die Frage hinein, inwieweit die Zivilklausel auch auf die Lehre auszuweiten sei. Denn wenn Informatikstudienerde in Forschungsprojekten beispielsweise Unterwasserroboter bauten, stelle sich doch die Frage wie sehr diese nicht nur implizit militärisch verwertbar, sondern vielmehr explizit auf eine solche Verwertung ausgerichtet seien. Auch sei zum Beispiel ein großer Teil der Studierenden, die ein sogenanntes duales Studium[2] absolvierten, in Rüstungsunternehmen beschäftigt. Inwieweit sich die Kooperation der Universität mit den fraglichen Unternehmen im Rahmen des dualen Studiums noch im Rahmen der Zivilklausel bewege, sei überaus fraglich.

Eine Frage, die im Rahmen der Diskussion immer wieder aufgeworfen wurde und die Viele aus der Veranstaltung mitgenommen haben dürften, ist diejenige, warum sich scheinbar so wenige (InformatikerInnen), Studierende wie Lehrende, mit der so offensichtlichen Verflechtung von Informatik und Rüstung beschäftigen wollen, wie auch die eher übersichtliche TeilnehmerInnenzahl an diesem Donnerstag vermuten ließ.

### Anmerkungen

1 *Mit einer Zivilklausel verpflichten sich wissenschaftliche Einrichtungen, wie z. B. Universitäten freiwillig, ausschließlich für zivile Zwecke zu forschen.*

2 *Ein duales Studium verbindet das Studium mit einer Berufsausbildung in einem Unternehmen.*

# Cyberpeace – Frieden gestalten mit Informatik

## FIfF-Jahrestagung 2013

## 25.-27. Oktober 2013, Universität Siegen

Arthur-Woll-Haus, Am Eichenhang 50, 57076 Siegen, http://fiff.de/2013, 2013@fiff.de

Organisation: Prof. Dr. Volker Wulf, Universität Siegen

Die Jahrestagung mit dem Thema der gleichlautenden FIfF-Kampagne steht unter dem Leitmotiv: *Frieden gestalten mit Informatik.*

Das FIfF stellt mit der Tagung dem Wettrüsten mit Cyberwaffen einen konstruktiven friedenspolitischen Entwurf entgegen. Wir wollen einen Beitrag leisten, Erkenntnisse und Produkte der Informatik friedlich zu nutzen.

Dabei wollen wir ethische und rechtliche Probleme im Cyberwarfare diskutieren, an einer Sicherheitspolitik arbeiten, die Frieden und bürgerliche Freiheit bewahrt und beinhaltet, Strategien zur Beendung des Wettrüstens mit Cyberwaffen entwickeln und betrachten, wie Technik bei Konfliktlösung unterstützen kann. Kann zum Beispiel über soziale Netzwerke gewaltfrei kommuniziert werden?

Eine weitere wichtige Forderung der Cyberpeace-Kampagne des FIfF ist Transparenz. Diese kann dazu beitragen, Zensur und Kriegspropaganda entgegen zu wirken oder dem Attributierungsproblem zu begegnen, um die Verursacher von Cyberangriffen zu ermitteln. Sicherheitslücken und Schwachstellen müssen frei untersucht und veröffentlicht werden, um deren Missbrauch als Angriffswaffen zu verhindern.

Tagungsbeginn ist am Freitag, 25. Oktober 2013 um 18:00 Uhr. Am Freitagabend werden zwei Vorträge stattfinden. Als Eröffnung und Einleitung ins Tagungsthema werden Sylvia Johnigk und Kai Nothdurft die Cyberpeace-Kampagne des FIfF mit ihren friedenspolitischen Forderungen vorstellen. Auf der Mitgliederversammlung sollen die Forderungen diskutiert und beschlossen werden (siehe Einladung in diesem Heft).

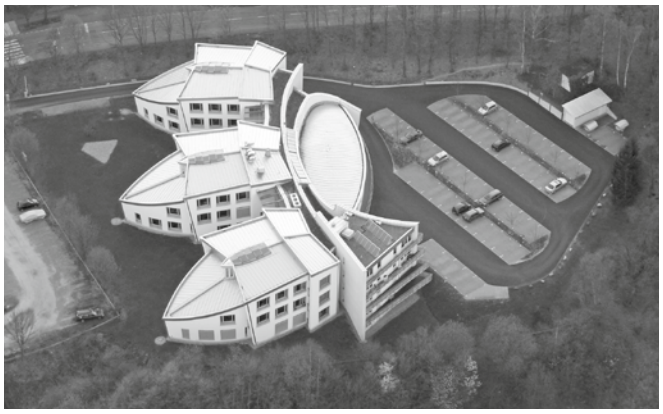
Am Samstag, 26. Oktober 2013 finden weitere Vorträge und die Workshops statt. Am Abend wird der FIfF-Studienpreis 2013 verliehen.

Am Sonntag, 27. Oktober 2013 wird am Vormittag der Abschlussvortrag gehalten. Im Anschluss findet die Mitgliederversammlung des FIfF und die Wahl des neuen Vorstands statt. Das Ende der Jahrestagung ist gegen 14:00 Uhr geplant.

Für die Tagung konnten bereits einige interessante Vortragende gewonnen werden:

### Jacob Appelbaum

Menschenrechtsaktivist, Wikileaks-Unterstützer und einer der Entwickler der Anonymisierungssoftware TOR wird einen Vortrag zum Themenbereich Internetüberwachung und Zensur halten.



### Stephan Gerhager

War bis 2012 bei einem großen deutschen Energieversorger verantwortlich für Informationssicherheit und forscht zu Sicherheitsrisiken des Smart Grids. Das „intelligente" Stromnetz wird zur Zeit in Deutschland eingeführt und soll eine wichtige Basis für die Energiewende liefern.

*Die Stromversorgung gilt als besonders kritische Infrastruktur und bildet damit ein äußerst attraktives Ziel für Cyberattacken. Schwachstellen in der Konzeption, Architektur und Implementierung stellen ein immenses Risiko dar.*

**Informationssicherheitsrisiken im zukünftigen Smart Grid**

Zukünftige Smart Meter werden als Kommunikationsendpunkt bei Stromkunden eine zentrale Rolle in den Kommunikationsbeziehungen zwischen den Kunden, dem Internet, dem Smart Home und dem Smart Grid spielen. Daher stellen diese Geräte ein interessantes Ziel für die unterschiedlichsten Angreifer dar.

Der Vortrag fokussiert zum einen auf die neu entstehenden Informationsrisiken und Bedrohungen im zukünftigen Smart Grid und zum anderen auf Ansätze, diese mit der Entwicklung einer ganzheitlichen Informationssicherheits-Architektur zu minimieren.

Zusätzlich gibt der Vortrag einen Einblick in die derzeitige Diskussion über Sicherheit im Smart-Metering- und Smart-Grid-Umfeld in Deutschland und Risikobetrachtungen aus dem Blickwinkel der Informationssicherheit sowie dem eines Energieversorgers.

## Rainer Rehak

*Preisträger des FIfF Studienpreises 2012*

### Geheimnisse und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Im Kontext der kürzlichen Enthüllungen des ehemaligen NSA-Mitarbeiters Edward Snowden kam unter anderem ans Tageslicht, dass sicherheitskritische Schwachstellen im weit verbreiteten Betriebssystem Microsoft Windows absichtlich von Microsoft geheimgehalten und nicht – oder nur verzögert – behoben werden. Einziger Grund sind die US-amerikanischen Geheimdienste, sie erhalten diese Informationen umgehend, um die offenen Sicherheitslücken für ihre Zwecke ausnutzen zu können.

Die Infrastruktur unserer digitalen Welt wird also ganz bewusst unsicher gestaltet. Dieser Umstand betrifft Privatpersonen genauso wie Behörden und Unternehmen und wie andere Organisationen, mindestens alle, die Windows Betriebssysteme von Microsoft einsetzen.

Wie verträgt es sich aber damit, dass das Bundesverfassungsgericht im Jahre 2008 das *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* formuliert hat?

Das Grundrecht wurde aus dem allgemeinen Persönlichkeitsrecht abgeleitet, weil das Gericht die Bedeutung solcher Systeme für den Menschen und die Gesellschaft erkannt hat. Dabei ist der Hinweis wichtig, dass sich das Grundrecht nicht auf Vertraulichkeit und Integrität allein richtet, sondern sogar auf deren Gewährleistung. Der Staat ist gewissermaßen in Bringschuld.

Welche Implikationen hat dieses Grundrecht also in einer globalisierten und digitalisierten Welt, in der Hersteller wissentlich unsichere Betriebssystemsoftware vertreiben, damit u. a. Geheimdienste die offenen Sicherheitslücken ausnutzen können? Muss man sich angesichts der Untätigkeit der deutschen Politik fragen, ob der Wesensgehalt des neuen Grundrechts dort überhaupt verstanden worden ist? Wie sehen tatsächliche Lösungsansätze aus, welche Rolle kann oder muss freie Software dabei spielen und vor allem warum? Diese und andere spannende Fragen sollen im Vortrag behandelt werden.

## Geplante Workshops und Arbeitsgruppen

**Arbeitskreis Ruestung und Informatik (RUIN)**

Der AK wurde im Sommer 2013 in Bremen neu konstitutiert und wird auf der Jahrestagung weiter arbeiten.

*Ansprechpartner: Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht*

**AG Videoüberwachung und Bürgerrechte**

Der „Hype" um die Videoüberwachung hat sich zu sehr gelegt. Immer noch steigt die Zahl der Kameras und der vorgeblichen Überwachungsanlässe. Es wird Zeit, das Thema dem Dornröschenschlaf zu entreißen. Im April 2013 hat das FIfF deshalb formell den überregionalen Arbeitskreis *Videoüberwachung und Bürgerrechte* wiederbelebt. Auf der FIfF-Klausurtagung fand im kleinen Kreis ein erster Workshop statt, dieser soll nun auf der Jahrestagung fortgesetzt werden.

Unter dem Titel *Strukturen des gesichtslosen Blicks – revisited* wollen wir interdisziplinär über das Thema Videoüberwachung diskutieren. Im Rahmen des ganztägigen Workshops soll die ganze Breite des Themas zur Sprache kommen:

- Was ist technologisch passiert – inwieweit haben sich die Kamerasysteme verändert?
- Was zeigt die Praxis – wer macht sich wie „Videoschutz" zu eigen?
- Was macht die Politik – welche Ziele werden wirklich verfolgt?
- Gibt es neue (internationale) gesetzliche Regelungen?
- Was sagt die Kriminologie – gibt es neue belastbare Evaluierungen?
- Wie ist es um die Kunst der Gegenwehr bestellt?

*Ansprechpartner: Peter Bittner peter@pbittner.de*

**AG Hackertools**

Keine Geheimwissenschaft, sondern teilweise kinderleicht zu bedienen. In Händen von „bösen Buben" eine potenzielle Gefahr. Trotzdem sollte man sie nicht verbieten, sondern dafür einsetzen, um Schwachstellen zu finden und zu schließen. Der Workshop zeigt wie leicht die Handhabung ist, und wie viele Möglichkeiten man bekommt, wenn man diese Tools einsetzt.

*Ansprechpartner: Matthias Bauer, Sylvia Johnigk*

**AG Crypto-Party**

It is Party Time! Wir wollen gute Laune gegen den Überwachungswahn verbreiten und zeigen, wie wir als Bürger das Heft des Handelns zurückgewinnen können. Es sollen Privacy-Tools zur Verschlüsselung und Anonymisierung vorgestellt und der praktische Umgang geübt werden. Der Staat kommt seiner Verantwortung nach Art. 1 und 2 des Grundgesetzes nicht nach, die Persönlichkeitsrechte der Menschen im Internet zu schützen. Informationelle Selbstbestimmung fängt mit dem eigenen Handeln an.

# Einladung zur Mitgliederversammlung 2013

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

Wir laden fristgerecht und satzungsgemäß zur ordentlichen Mitgliederversammlung 2013 ein.

Sie findet am Sonntag, den 27. Oktober 2013, von 11:00 bis 14:00 Uhr
an der Universität Siegen, Artur-Woll-Haus, Am Eichenhang 50, 57076 Siegen, statt.

### Vorläufige Tagesordnung

1. Begrüßung, Feststellung der Beschlussfähigkeit und Festlegung der Protokollführung
2. Beschlussfassung über die Tagesordnung, Geschäftsordnung und Wahlordnung
3. Bericht des Vorstands einschließlich Kassenbericht
4. Bericht der Kassenprüfer
5. Diskussion der Berichte
6. Entlastung des Vorstands
7. Neuwahl des Vorstands
8. Neuwahl der Kassenprüfer
9. Diskussion über Ziele und Arbeit des FIfF, aktuelle Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen
10. Anträge an die Mitgliederversammlung
    *Anträge müssen schriftlich bis drei Wochen vor der Mitgliederversammlung bei der FIfF-Geschäftsstelle eingegangen sein*
11. Verschiedenes

**gez. Stefan Hügel**
**für den Vorstand und die Geschäftsstelle des FIfF**

### Antrag

Die Mitgliederversammlung des FIfF möge beschließen:

### Forderungen des FIfF zum Cyberpeace

1. Verzicht auf Erstschlag und Offensive im Cyberspace: Staaten sollen öffentlich darauf verzichten, Cyberwaffen präventiv zum Angriff einzusetzen.

2. Rein defensive Sicherheitsstrategie: Staaten sollen sich verpflichten, keine Offensivwaffen für den Cyberwar zu entwickeln oder gar einzusetzen.

3. Digitale Genfer Konvention: Für die Zivilbevölkerung lebenswichtige Infrastrukturen wie Strom-, Wasser-, Gesundheitsversorgung, etc. dürfen nicht angegriffen werden. Eine Verletzung dieses Grundsatzes soll als Kriegsverbrechen gelten.

4. Anerkennung eines Grundrechts auf zivilen Ungehorsam und Onlineprotestformen im Internet: Derartige Aktionen dürfen nicht kriminalisiert werden geschweige denn als Kriegsgrund herhalten.

5. Wirtschaftliche Interessen, wie ein Verstoß gegen Intellectual Property Rights, sind kein legitimer Kriegsgrund.

6. Konventionelle Waffen dürfen nicht als Antwort auf eine Cyberattacke eingesetzt werden.

7. Staatliche Stellen, Unternehmen und Bürger müssen zur Offenlegung von Schwachstellen verpflichtet werden (ableitbar aus dem Grundrecht für Integrität, das der Staat schützen muss).

8. Betreiber kritischer Infrastrukturen müssen verpflichtet werden, sich selbst zu schützen, bzw. IT-Systeme sicher zu gestalten, zu implementieren und zu betreiben, anstatt nach dem Staat oder gar Militär zu rufen.

9. Kompetente, transparente Prüfungen und Tests müssen Voraussetzung für eine Betriebserlaubnis sein.

10. Wir fordern Entnetzung und Dezentralisierung kritischer Infrastrukturen (wie z. B. DE-CIX).

11. Abrüstung der politischen Sprache: Klare Trennung von Cyberwar, Cyberterror, Cybercrime, ethical Hacking, politischen Protestformen.

12. Demokratische Kontrolle, Gewaltenteilung, Parlamentsvorbehalt für Cybersicherheitsstrategien und deren Umsetzung.

**Sara Stadler**

# Aktuelles aus dem Büro

*Neues aus dem FIfF-Büro.*

Nachdem ich nun schon einige Monate in der Geschäftsstelle des FIfF in der Villa Ichon in Bremen tätig bin, hat meine Kollegin, Ingrid Schlagheck mich gefragt, ob ich nicht einen Artikel über die Geschäftsstelle schreiben mag – schließlich sollen auch die Mitglieder über die Neuerungen informiert werden. Gerne nutze ich diese Gelegenheit, auch, um mich den zahlreichen Mitgliedern einmal vorzustellen, die meinen Namen bislang nur aus den vielen E-Mails kennen, die wir über die Geschäftsstelle verschicken.

An die Informatik und damit an das FIfF bin ich eher spät gekommen. Nach einem abgeschlossenen Geschichtsstudium und verschiedenen, meist wissenschaftlichen, Tätigkeiten, habe ich im Oktober 2012 begonnen, den Internationalen Frauenstudiengang Informatik an der Hochschule Bremen zu studieren. Es macht mir großen Spaß, mir praktisches Wissen und Kompetenzen in diesem Bereich anzueignen. Die kritische Auseinandersetzung mit einer Technik, die nahezu alle gesellschaftlichen Bereiche durchdringt, erscheint mir aber mindestens ebenso wichtig. Entsprechend interessiert war ich, als ich von der freien Stelle in der Geschäftsstelle erfahren habe, die ich nun im April diese Jahres angetreten habe.

Hier arbeite ich zusammen mit meiner ebenso herzlichen wie kompetenten Kollegin Ingrid Schlagheck. Ingrid, die bereits seit April 2010 in der Geschäftsstelle tätig ist und seitdem die Geschäftsführung inne hat, ist mit allen organisatorischen Abläufen bestens vertraut. Auch sie kommt ursprünglich nicht aus dem Informatikbereich. Ihr beruflicher Werdegang führte sie über den Buchhandel, verschiedene Bibliotheken und die Pressestelle der Bremer Universität zum FIfF, dessen Vorstand sie seit 2011 angehört. Mitgebracht hat sie nicht nur jede Menge kaufmännisches und logistisches Fachwissen, sondern auch ein unglaubliches Organisationstalent.

*Ingrid Schlagheck*

Gemeinsam bewältigen wir hier einen ganzen Berg an Arbeiten, die die Verwaltung eines bundesweiten Vereins so mit sich bringt. Während Ingrid dabei vor allem auf der organisatorischen Ebene dafür sorgt, dass der Laden läuft, liegt mein Arbeitsschwerpunkt in der inhaltlichen Zuarbeit zum Vorstand und der Öffentlichkeitsarbeit. Zu unserem Tagesgeschäft gehören die Mitgliederverwaltung, Versandaktionen – wie alle drei Monate der Versand der FIfF Kommunikation –, die organisatorische Unterstützung von Sitzungen, Tagungen oder des FIfF-Studienpreises, und nicht zuletzt kümmern wir uns darum, dass immer ausreichend Flyer zum Verteilen und viele schöne FIfF-T-Shirts zur Verfügung stehen.

*Villa Ichon in Bremen*
*Foto: Jürgen Howaldt, CC BY-SA 3.0 DE*

Daneben ist es uns besonders wichtig, den Kontakt zu Mitgliedern und Interessierten zu halten und die verschiedenen Aktivitäten, Inhalte und Kritiken innerhalb des FIfF nach außen zu tragen. Wir bearbeiten die zahlreich eingehenden E-Mails, die oft Anfragen zu inhaltlichen Themen enthalten. Dafür steht uns im FIfF ein großer Kreis an AnsprechpartnerInnen mit Fachwissen zu verschiedenen Themen zur Verfügung. Wir verfassen auch Pressemitteilungen, oder bereiten solche vor, versuchen gemeinsam mit (Vorstands-) Mitgliedern die Homepage aktuell zu halten und übernehmen inhaltliche wie redaktionelle Arbeiten für die FIfF-Kommunikation.

Weil es immer jede Menge zu tun gibt und wir uns gerne mit anderen Mitgliedern austauschen, freuen wir uns über aktive Mitarbeit: Sei es über inhaltliche Anregungen oder fertige Beiträge für die *FIfF-Kommunikation* oder die Homepage, über die Betreuung des FIfF-Standes bei Tagungen, die Teilnahme an Arbeitsgruppen oder vieles mehr. Wenn Ihr Interesse habt, schreibt uns jederzeit gerne eine Mail an *fiff@fiff.de*.

In diesem Sinne bis bald.

Eure Geschäftsstelle

*Ingrid Schlagheck und Sara Stadler*

**Peter Bittner**

# Wenn der Mensch vermessen zur Information wird …

## über Biometrie im Masseneinsatz und ihre Grenzen

*In diesem Beitrag geht es um die Eigenschaften und die Grenzen der Biometrie mit Blick auf deren Masseneinsatz. Der Beitrag bereitet eine Reihe von Beiträgen vor, die die Geschichte(n) der Biometrie etwas anders erzählen sollen, nämlich aus der Sicht ihrer Unterwanderung.*



### 1. Eigenschaften biometrischer Merkmale und Systeme – eine kurze Einführung

Ganz grundsätzlich unterscheidet man bei der biometrischen Erfassung bzw. Messung *physiologische* (passive) Merkmale (z. B. Finger, Hand, Gesicht, Auge, Ohr) und *verhaltensabhängige* (aktive) Merkmale (z. B. Sprache, Unterschrift, Gang). Diese müssen nach Jain et al. (1999) vier Eigenschaften aufweisen, um „biometrisch optimal genutzt" werden zu können. Unter der Eigenschaft *Universalität* wird verstanden, dass das Merkmal bei jedem Menschen vorhanden ist. *Einzigartigkeit* bedeutet, dass das Merkmal bei jedem Menschen verschieden (ausgeprägt) ist. Zudem ist eine (gewisse) *Beständigkeit* notwendig, d.h. die Merkmalsausprägung verändert sich über die Zeit nicht. Soll die Merkmalsausprägung in einem System verarbeitet werden, dann muss diese *erfassbar*, d.h. durch ein technisches System quantitativ messbar sein.

Mit Blick auf die *Praxistauglichkeit* der biometrischen Systeme kommen weitere Eigenschaften hinzu. Die Systeme müssen technisch umsetzbar sein und notwendige Bedingungen an ihre Schnelligkeit und hinsichtlich ihrer Einbettung in die zugehörigen Prozesse eine gewisse Kompatibilität aufweisen. Sie sollen robust arbeiten, die notwendige Empfindlichkeit/Genauigkeit aufweisen sowie (aus Sicht der Sicherheit) überwindungsresistent sein. Die Einrichtung und der Betrieb der Systeme soll zu vertretbaren Kosten möglich sein (ökonomische Machbarkeit). Aus Sicht der Nutzerfreundlichkeit müssen die Systeme zuverlässig, einfach und komfortabel bedienbar sein sowie den hygienischen Standards genügen. Zu fordern ist natürlich eine rechtskonforme Ausgestaltung, d. h. es muss u. a. an die „Datenschutzfreundlichkeit" der Systeme gedacht werden.

Es bleibt festzuhalten: Keines der (biometrischen) Merkmale bzw. keines der Systeme erfüllt alle Anforderungen vollständig, sei es aus *praktischen* oder *prinzipiellen* Gründen.

Mit Blick auf den Masseneinsatz (z. B. in Ausweispapieren) werden als Merkmale hauptsächlich der Fingerabdruck, das Gesicht, die Iris (auch die Retina) und die Handgeometrie gehandelt. Für die Merkmale sind die *Rohdaten* und die gemessene Charakteristik zu unterscheiden. Bezüglich des Fingerbildes bildet der Abdruck der Hautleisten (Papillaren – ggf. auch der Poren) auf der Fingerkuppe das Rohdatum. Die zugehörige *Charakteristik* ergibt sich aus dem Grundmuster des Fingerabdrucks und den Minuzien, das sind z. B. besondere Stellen der Papillarleisten wie freie Enden, geschlossene Bereiche und Gabelungen. Vom Rohdatum (digitales) Gesichtsbild gewinnt man geometrische Merkmale z. B. von Augen, Kinn, Nase, Mund und deren Verhältnis zueinander. Aus einer digitalen Aufnahme der Iris kann man die verschiedenen Strukturen des Musters um die Pupille gewinnen.

Hinsichtlich der *Leistungsfähigkeit* unterscheiden sich die vorgenannten Merkmale (PB: „Seins-Zeichen"). Petermann (2004) hat dies genauer aufgeschlüsselt. Zusammengefasst kann man sagen, dass bezogen auf die Erfassbarkeit, also den Bevölkerungsanteil bei dem das Merkmal „zweifelsfrei" erfasst werden kann, sich eine Rangfolge Gesicht vor Iris dann Finger und Hand etwa gleichauf ergibt. Hinsichtlich der Nutzerfreundlichkeit (Verständlichkeit und Bedienungsaufwand) liegt der Finger vor dem Gesicht und dieses vor Iris und Hand. Bei der Erkennungsleistung, also der Wahrscheinlichkeit fälschlicher Zurückweisung bzw. Legitimation, liegen Finger und Iris vor Gesicht und Hand. Bei gleicher Gewichtung der technischen Parameter

**Peter Bittner**

**Peter Bittner** ist Grenzgänger zwischen den Disziplinen, er arbeitet in und zwischen Informatik, Wirtschaftswissenschaften, Philosophie und Soziologie. Als wissenschaftlicher Mitarbeiter beschäftigte er sich mit der Ethik und Profession der Informatik, arbeitete zu gesellschaftlichen, politischen und juristischen Fragen der Informatik, zur informationellen Selbstbestimmung und über Überwachungstechniken (mit dem Schwerpunkt auf Videoüberwachung und Biometrie). Viele seiner Arbeiten bündelte er in einem Entwurf einer Kritischen Theorie der Informatik. Er lehrte an den Universitäten TU Kaiserslautern, TU Darmstadt und HU Berlin sowie an der Berufsakademie Berlin. Daneben betreute er Studierende an der Hochschule München. Als IT-System-Berater konfigurierte er ERP-Systeme und entwickelte Betriebs-, Datenschutz- und Sicherheitskonzepte. Als Berater für Betriebsräte kämpfte er für *datenschutzgerechte* IKT-Systeme in den Betrieben und den Beschäftigtendatenschutz. Er war zehn Jahre im Bundesvorstand des FIfF und ist derzeit Mitglied des Beirats.

ergibt sich bezüglich Gesichts-, Iris- und Fingerabdruckerkennung eine (etwa) vergleichbare Leistungsfähigkeit. Die Handgeometrie fällt etwas in der Leistungsfähigkeit ab.

Für die Entscheidung & Implementierung gewinnen also nichttechnische Kriterien an Relevanz, also die Datenschutzfreundlichkeit, der Grad öffentlicher Akzeptanz, die internationale Kompatibilität und Interoperabilität, die mögliche Integration in bestehende Strukturen und die Kosten. Die Gewichtung der Kriterien unterliegt sehr verschiedenen Faktoren – nicht nur dem politischen Willensbildungsprozess.

## 2. Grundsätzliche Verfahrensmerkmale

Basis eines jeden biometrischen Verfahrens ist das *Enrolment* – es umfasst das erstmalige Erfassen und (Ver-)Messen des biometrischen Merkmals der zukünftigen Nutzer, die Umwandlung der „Rohdaten" in einen *Referenzdatensatz* und die Speicherung desselben, des sog. *Templates*. Das Template stellt den Vergleichswert dar, mit dem bei allen darauf folgenden biometrischen Überprüfungen die neuen Messdaten (zumindest zu einem hohen Grad) übereinstimmen müssen, um den Nutzer identifizieren zu können.

An den Vorgang des Enrolments sind sehr hohe Anforderungen zu stellen. Zunächst höchste technische Anforderungen bzgl. Empfindlichkeit und Genauigkeit, damit tatsächlich individuelle, aber auch reproduzierbare Datensätze entstehen. Hinzu treten höchste Sicherheitsanforderungen. Eine Erhöhung der Sicherheit ist nur gegeben, wenn der Referenzdatensatz, das Template, dauerhaft geschützt gespeichert werden kann. Insgesamt ist zu konstatieren, dass das Enrolment-Personal besonders zu schulen ist. Je nach Merkmal ist mit einem gewissen Prozentsatz (man spricht von 2 bis 5 %) der zu Erfassenden zu rechnen, bei denen es zu nicht oder nur sehr schlecht verwertbaren Ergebnissen des Enrolments kommt (vgl. Vielhauer, 2000). Im Falle eines solchen *Failure to enrol* benötigt man deshalb eine Ausweichstrategie.

Für biometrische Systeme unterscheidet man zwei Betriebsarten: *Verifikation* (1:1-Vergleich) und *Identifikation* (1:n-Vergleich). Diese sind u. a. in Köhntopp (1999: 178 und 179) beschrieben.

Bei der biometrischen Verifikation geht es um die Bestätigung der behaupteten Identität des Individuums (1:1 = die vermessene Person ist tatsächlich die, die sie zu sein behauptet), und bei der biometrischen Identifikation geht es um die Erkennung eines Individuums aus einer (definierten) Menge biometrisch registrierter Personen (1:n = die vermessene Person ist XY).

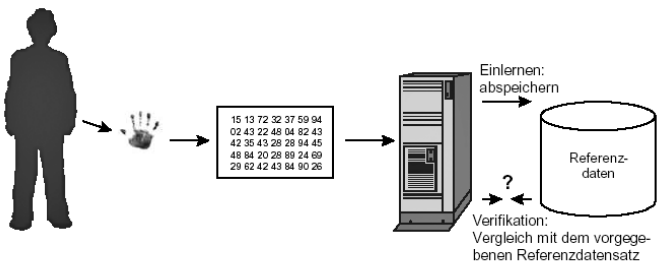



**Abb. 1:** Datenfluß bei biometrischen Verfahren: Einlernen und Verifikation

Als *Oberbegriff* für die Verifikation und Identifikation hat sich der Begriff der *Authentifizierung* (bzw. Authentifikation) im deutschen Sprachraum noch nicht wirklich durchgesetzt, oftmals wird verallgemeinernd von „biometrischer Personenidenfikation" gesprochen, was zu begrifflicher Verwirrung führt. Begrifflich abzusetzen von der Authentifizierung ist weiterhin die *Autorisierung*, als eigentlichem Ergebnis der Überprüfung der Identität des Nutzenden, also die Ermächtigung bzw. Bevollmächtigung für einen Zugang oder für eine Handlung.

## 3. „Tolerante" Biometrie

### 3.1 Praxisprobleme

Es können vielfältige Praxisprobleme auftreten. Hier einige Beispiele: Die verwendeten Instanzen der Sensoren können sich unterscheiden, Defekte aufweisen, altern, es kann zu Messfehlern kommen. Die Betroffenen verhalten sich bei den verschiedenen Messungen nicht gleichförmig. Die Erfassbarkeit muss nicht bei allen gegeben sein, sei es grundsätzlich oder auch zeitlich begrenzt – z. B. bei Krankheit. Systemisch können sich verändernde Umweltbedingungen zu Störungen (z. B. Licht bei Gesichtsbild, Temperatur bei Fingerabdruck) führen. Die rahmenden Prozesse können sich verändern, z. B. bei der mangelnden Reinigung optischer Fingerabdruck-Sensoren oder auftretender Inkompatibilitäten bei geänderten technischen Spezifikationen. Wir merken: *Biometrie ist praktisch nicht präzise. Biometrische Systeme müssen „Fehler" machen!*

Eine hundertprozentige Übereinstimmung wird wegen prinzipieller technischer, physiologischer als auch situationsbedingter Einschränkungen praktisch nie vorkommen. In biometrischen Systemen wird deshalb ein *statistischer Vergleich* (prozentuale Übereinstimmung) von Referenzdatensatz und Messdatensatz durchgeführt.

### 3.2 Schwellwerte, Toleranzen und Fehlerraten

Für jedes System muss daher eine Schwelle (ein Wert für den Grad der Übereinstimmung von Referenz- und Messwert) definiert werden (z. B. 95 %), ab der die Identifikation bzw. Verifikation als erfolgt betrachtet und der Nutzer als berechtigt akzeptiert wird. Diese Toleranzschwelle hat einen großen Einfluss darauf, wie viele Nutzer entweder fälschlicherweise akzeptiert werden oder aber fälschlicherweise zurückgewiesen werden (bzw. gezwungen sind, den Vorgang mehrfach zu wiederholen).

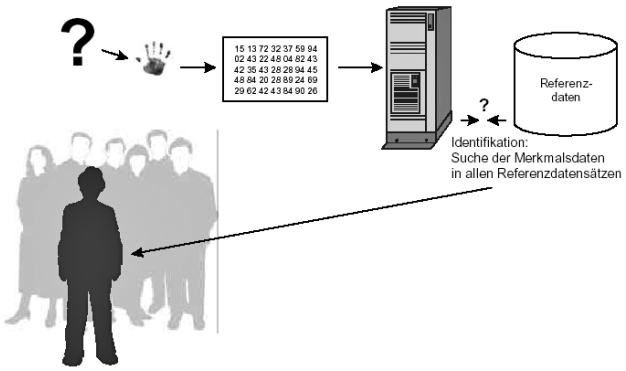



**Abb. 2:** Datenfluß bei biometrischen Verfahren: Identifikation

Die Raten falscher Ablehnung (FRR = False Rejection Rate) bzw. falscher Akzeptanz (FAR = False Acceptance Rate) eines biometrischen Systems können nicht theoretisch berechnet werden, sondern müssen empirisch ermittelt werden. Wichtig zu wissen ist, dass FAR und FRR sich dergestalt beeinflussen, dass eine Absenkung der falschen Akzeptanz die falsche Zurückweisung erhöht und umgekehrt. Die absolute Höhe der Fehlerraten ist allerdings abhängig von der Empfindlichkeit und Genauigkeit, also der Trennschärfe, des Gesamtsystems und wird daher von der Wahl der o. g. Toleranzschwelle direkt beeinflusst.

Ein „typischer" Verlauf der Fehlerkurven (siehe TeleTrusT/AG 6, 2006: 14) kann man Abbildung 3 entnehmen.

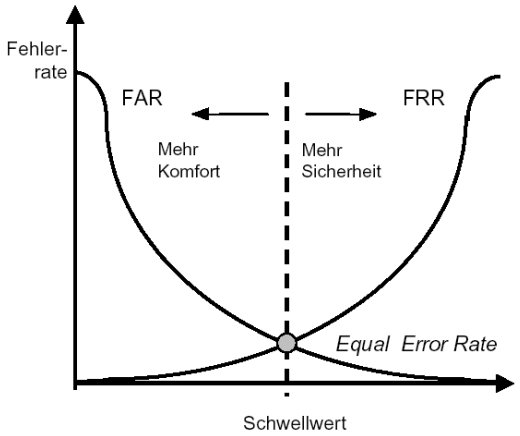



**Abb. 3:** Typischer Verlauf der Fehlerkurven

Die sogenannte *Equal Error Rate* markiert hier den geringsten Gesamtfehler des biometrischen Systems.

## 4. Massenanwendungen von Biometrie

### 4.1 Grenzkontrollen – Biometrie in Reisedokumenten

Für die Ausweiskontrolle genügt die Verifikation (Ausweis gegen Inhaber), eine Identifikation ist zunächst nicht notwendig! Ein wichtiger Teil der Grenzkontrolle ist auch die Echtheitsprüfung des vorgelegten Dokumentes (Prozess & Dokument). Es ergeben sich einige Probleme, exemplarisch seien hier folgende benannt: Bei der Erhebung vor Ort besteht keine wirksame Kontrolle hinsichtlich der Speicherung, Übermittlung oder weiteren Verarbeitung der offen gelegten biometrischen Daten. „Schattendatensammlungen" dürften eher die Regel als die Ausnahme sein. Allerdings sind heute schon Verfahren möglich, die ohne Speicherung der biometrischen Daten in (de-)zentralen Datenbanken auskommen. Die Prüfung kann auf dem Ausweis *(match-on-card)* erfolgen. Damit behielte man bei einem Grenzübertritt die (volle) Souveränität über die eigenen biometrischen Daten. Hilfsweise könnte man ein Verfahren etablieren, welches die notwendige Transparenz bezüglich Lesegerät/Sensor herstellt und zusichert, dass der Abgleich der Daten nur dort geschieht.

Die Zurichtung (oder sollten man besser Hinrichtung sagen) auf die Maschine führt zu Frontansichten auf den biometrischen Passbildern. Dadurch verliert man Erkennungsmerkmale (z. B. Ohr oder Kinnform beim Halbprofil), die für die Erkennung durch menschliches Grenzpersonal von erheblicher Bedeutung sind. Folgt man dem Ziel der Automatisierung von Grenzkontrollen, dann muss man sicher über eine möglichst nicht-diskriminierende Rückfallstrategie nachdenken, wenn die automatisierte Erkennung scheitert oder nicht möglich ist.

### 4.2 Immigrationsmanagement – Biometrie in Visa und Aufenthaltstiteln

Die „Identitätssicherung" zielt auf die Verhinderung der Einreise bzw. die Beantragung von Aufenthaltstiteln einer Person unter verschiedenen „Identitäten". Zudem geht es um die Registrierung von Personen, die keine Papiere haben oder deren Identität nicht zweifelsfrei geklärt werden kann. Biometrische Daten können solche Mehrfachidentitäten aufdecken – wie ein Pilotprojekt in Lagos gezeigt hat. Hierzu ist ein Datenbankabgleich (also eine Identifikation) notwendig. Im Vorfeld „notwendiger" Identifikationen kann man aber zumindest versuchen, den Prozess der Ausgabe von Ausweisdokumenten in den besonders betroffenen Ländern zu verbessern, eventuell mit dem „wirtschaftspolitisch gewünschten" Export sicherer Drucktechnik. Es darf nicht zu leicht möglich sein, sich echte Dokumente mit anderem Namen (anderer Identität) zu beschaffen und gefälschte Dokumente müssen hinreichend gut als solche erkannt werden können. Man muss sich dann aber dem Problem stellen, ob man eine generelle biometrische Erfassung aller Bürger wirklich wünscht? Darf man Einschränkungen auf bestimmte Staaten fordern? Was resultiert aus Ungleichbehandlungen?

### 4.3 Abgleich mit „Fahndungsdateien" und Terrorismusbekämpfung

Der Abgleich mit „Fahndungsdateien" ist einer der politisch oft genannten Gründe für die Betriebsart „Identifikation". Soll ein Abgleich aller Grenzgänger (anlasslos) erfolgen? Wenn nicht, wer ist dann wann warum „verdächtig" und erfährt deshalb die „Sonderbehandlung" des Abgleichs? Was ist mit der Unschuldsvermutung? Wer führt den Abgleich durch?

Es stellt sich natürlich die Frage, wie die „biometrischen Fahndungsdateien" gegen Verfälschung abgesichert werden? Warum kommt wer in eine Fahndungsdatei? Wie ist ein Verbund von Fahndungsdateien organisiert? Wie kommt man aus den Fahndungsdateien wieder heraus, falls ein Fehler passierte? In einem solchen Regime bleibt unbegründete Repression möglich!

Unsere „Terrorismusbekämpfungsgesetze" sind eher gekennzeichnet durch Grundrechtsabbau und die Diskriminierung von Ausländern als durch wirksame Verhinderung von Terrorismus (u. a. hierzu näher: Weichert 2002: 423ff.). Verhindern biometrische Dokumente Terrorismus? Eher nicht! Herzlich Willkommen in der Debatte über Sicherheit und Freiheit.

### 4.4 eGovernment & eCommerce – Biometrie in nationalen Ausweisen

Unsere nationalen Identitätsdokumente (elektronischer Personalausweis – ePA) bieten das „Feature" des elektronischen Identitätsnachweises (eID), u. a. zum Bezug staatlicher Verwal-

tungsleistungen oder zum „rechtssicheren“ Handeln im privaten Bereich bei eCommerce-Anwendungen. Die damit verbundenen Folgen des ePA wären einen eigenen Beitrag wert. Hier sei nur angemerkt, dass fälschungssichere Personalausweise durch Biometrie nichts in ihrem Sicherheitsniveau gewinnen. Dabei deckt sich die eID mit PIN nicht mit einer qualifizierten elektronischen Signatur. Biometrische Identifikationen als mögliche Folge einer (doch einfach sichereren biometrisch gestützten ;-) digitalen Signatur – wären dann endlich das ultimative Personenkennzeichen. Letztere gelten in der BRD aber als verfassungswidrig! (vgl. u. a. BT-Drs. 7/1059: 10; Bull, 1984: 190ff.; Bizer, 2004: 45).

## 5. Kritische Fragen

... muss sich die technisierte Biometrie gefallen lassen. Es sei hier auf einige zentrale Fragekomplexe hingewiesen.

### 5.1 Testbedingungen und Unabhängigkeit

Sensoren, Umweltbedingungen und Verfahren sind eng aufeinander abzustimmen. Die entstehenden Systeme weisen deshalb eine relativ hohe Fragilität auf. Die Ausrichtung der Systeme auf spezifische Test-Datenbanken machen die Systeme schlecht vergleichbar. Die Erwartungen an Fehlerraten werden beim Wechsel der Referenzdatenbasis regelmäßig enttäuscht. Die Repräsentativität des Testpersonenkreises ist oft nicht gegeben (am Flughafen bilden geschäftsreisende männliche Kaukasier den Hauptteil der Testpersonen). Es ist zu beachten, dass die Erfassbarkeit/Erkennungsrate ungleich verteilt ist über Ethnie, Alter, Berufsgruppen etc. In vielen Fällen wurden die Testbedingungen auf die Verfahren hin optimiert, statt es der „Erkennung“ besonders schwer zu machen.

### 5.2 „Skalierungsproblem“

Erwartungen an die Leistungsfähigkeit von biometrischen Systemen „skalieren in der Regel nicht“. Die FAR ist abhängig vom Verhältnis der Anzahl fälschlicher Akzeptanzen zur Anzahl unberechtigter Zutritte. Die FRR ist abhängig vom Verhältnis der Anzahl fälschlicher Rückweisungen zur Anzahl berechtigter Zutritte. Die Messung (eigentlich Vorhersage) der FAR eines Systems für die Sicherheitsklasse „sehr stark“ kann mehrere tausend Testpersonen erfordern. Oftmals basieren die Tests auf viel kleineren Gruppen, somit ergibt sich keine belastbare Vorhersage für das Produktiv-System.

### 5.3 Ökonomie

Im Rahmen des Aufbaus einer Biometrie-Infrastruktur für deutsche Ausweisdokumente gehen Booz Allen Hamilton et al. (2003: 126ff.) von erheblichen einmaligen und regelmäßigen Kosten aus (jeweils > 600 Mio. Euro). Dies wird dazu führen, dass in dieses System auf längere Sicht nicht erneut investiert werden dürfte. Diese Kosten können aber auch als „Subventionen“ in die Biometrie-Industrie verstanden werden, also als innovationspolitisches Instrument oder als „Stützung“ der (damals) „angeschlagenen“ Bundesdruckerei. Allerdings kann sich die „biometrische Grenzkontrolle“ auch als Hemmschuh für die Wirtschaft herausstellen. In den USA gab es verschiedentlich Presseberichte, die vom Absinken der Kundenkontakte bei amerikanischen Firmen berichtete. Patente auf Biometrie-Verfahren können auch ein industriepolitisches Problem darstellen. Bestimmte Länder/Firmen kämen in eine marktbeherrschende Stellung. Die Einführung und Persistenz bestehender Technologie kann bestehende Patentinhaber weiter schützen, auch wenn einige Patente in den kommenden Jahren auslaufen. Die Verhinderung einer Einigung auf Template-Verfahren im Rahmen der Standardisierung/Normung führt dazu, dass de facto Rohdaten in den Biometrie-Systemen gespeichert werden. Damit werden datenschutzfreundlichere Technologien behindert.

### 5.4 Bürgerrechte & Staatsverständnis

Abgesehen von entsprechenden internationalen Verträgen besteht eine staatliche Autonomie bei der Festlegung der Einreisebestimmungen. Erzeugen die amerikanischen „Einreiseerleichterungen nur bei biometrischen Pässen“ tatsächlich einen solchen Handlungsdruck? Wer erzwingt hier wie Inklusion? Es gab durchaus Staaten, die sich dem Druck nicht gebeugt haben (Kanada). Im übrigen fanden weitreichende (Vor-)Entscheidungen ohne nationale Parlamente statt. Inwieweit verändern die neuen Grenzregimes den kulturellen Austausch?

Auf dem Weg zur Massenbiometrie gefährden wir das gesellschaftlich notwendige Rollenspiel – wollen wir wirklich an den Grundfesten demokratischer Verfassung rütteln (siehe PKZ)? Unterschiede in der Erfassbarkeit (Ethnie, Alter, Beruf, Krankheit, ...) verstärken Ausgrenzungs- und Normierungsprozesse. Die Massenanwendung erhöht das Risiko des Diebstahls von Körperteilen (oder ersatzweise von Entführung und Erpressung bei funktionierender Lebenderkennung). RFID in Pässen macht den Identitätsdiebstahl einfach lohnenswert – das Klonen von Pässen ist ja schon vor einigen Jahren gelungen.

### 5.5 Datenschutz und verbundene Fragen

In diesem Abschnitt gebe ich gekürzt die Argumentation von Rossnagel und Hornung (2005: 69-73) wieder.

Rossnagel und Hornung weisen zunächst auf den weit reichenden *Grundrechtseingriff* bei *fehlender Bestimmtheit* (PersAuswG) hin. Vor der Gesetzesentwurfsänderung zum 18. Juni 2009 gab es eine Wahl zwischen drei Merkmalen, hybride Varianten und das Merkmal Iris waren nicht abgedeckt. Es bestand keine Regelung zur Art der Speicherung auf dem Ausweis oder in staatlichen Dateien.

In der Frage der *Verhältnismäßigkeit* liege im Falle der Verifikation (1:1-Vergleich) ein legitimer Zweck vor und das Verfahren sei verfassungsrechtlich akzeptabel. Dies gilt für die Identifikation erstmal nicht.

Hinsichtlich der *Eignung* müsste das biometrische Verfahren eine niedrigere FAR aufweisen als die Sichtkontrolle. Zugleich müsste die FRR niedriger sein, sonst drohen intensive Nachkontrollen. Aus dieser Sicht sei höchstens die Iris geeignet, ggf. hybride Verfahren. Zudem seien effektive Rückfallsysteme notwendig.

Zur *Erforderlichkeit*: Unterstellte man Eignung, dann gibt es kein weniger belastendes gleich geeignetes Verfahren. Es muss das Verfahren geringster Eingriffstiefe zur Anwendung kommen. In diesem Zusammenhang darf es nicht zu überschießenden Informationen kommen, flüchtige Merkmale (ohne dauerhafte Spuren) sind zu bevorzugen und es muss eine Mitwirkungsgebundenheit vorliegen.

Aus Sicht der *Zumutbarkeit* sind ungerechtfertigte Diskriminierungen und Belastungen zu vermeiden. Dies ist besonders wichtig, weil je nach Merkmal ein bestimmter Bevölkerungsanteil zeitweilig oder permanent keine ausreichende Ausprägung hat. Mit Blick auf Art. 3 GG ist bemerkenswert, dass einige Gesichterkennungsverfahren Männer signifikant besser erkennen als Frauen.

Hinsichtlich der Form der Daten (Volldaten vs. Templates) muss auf die Gefahr der Klassifikation oder Auswertung nach unzulässigen Kriterien oder die Profilbildung hingewiesen werden. Die mangelnde Standardisierung bei den Templates und der patentrechtliche Schutz bestimmter Verfahren erzeugen weltweite Monopole. Die BRD sollte auf die Standardisierung der Templates hinwirken.

Zu den notwendigen *Sicherungsmaßnahmen* gehört die Sicherung der Integrität der Daten, z. B. durch die gegenseitige Authentifizierung von Prüfgerät und Chip, die wirksame Verschlüsselung der Daten bei jeder Übertragung und die strikte Trennung hoheitlicher Daten von anderen Funktionen (Signatur). Ein Schutz vor Überwindung und missbräuchlicher Nutzung muss gewährleistet werden. Hinsichtlich des ePA ist eine abschließende Zweckbestimmung (in §3 Abs. 5 PersAuswG) mehr als fraglich. Wie steht es um die Durchsetzbarkeit des Verbots der Speicherung der Ausweisdaten außerhalb des Sperrlistenabgleichs mit sofortiger nachfolgender Löschung?

Eine bundesweite „Biometrie-Datei" wäre ein „leichtes" Ziel für Zugriffe, Weiterverwendung und Übermittlung für andere Zwecke. Für die Verifikation ist eine solche Datei sowieso nicht notwendig. Deren weitergehende Verwendung bedürfte einer eigenen rechtlichen Regelung. Leider schützt uns diese nicht vor dem Aufbau solcher Dateien in Drittstaaten.

Das eingeführte Verfahren (Dokumente, eID, QES, Technik) muss auch wirklich beherrscht werden (nicht nur im Sinne von §9 BDSG), dies betrifft die Hersteller, die Meldestellen, die (Grenz-)Kontrollstellen, die betroffenen Behörden und auch die „Handelspartner" im Rahmen des eCommerce. Biometrische Systeme müssen gegen Unterlaufen, Missbrauch und Einbruch abgesichert werden.

## 6. Ausblick: Was der Leserin/dem Leser in den nächsten Ausgaben der FIfF-Kommunikation bevorsteht

Das „Unterlaufen" biometrischer Systeme wird Gegenstand verschiedener Folgebeiträge sein. Dabei „entsteht" eine andere – alternative – Geschichte der Biometrie. Zur Überraschung vieler wird gezeigt, dass das Unterwandern, Hintergehen und Austricksen biometrischer Systeme überhaupt kein neues Phänomen ist. Die Untersuchung behandelt je Merkmalstyp folgende Themen: Spurenvermeidung, Elimination bzw. gezielte Veränderung von Merkmalsträgern, Déjà vu – Spuren jenseits ihres Ortes und ihrer Zeit, Ent-Eignungen, Merkmalsträger im Zeitalter ihrer technischen Reproduzierbarkeit, sowie den Transfer von Merkmalsträgern.

Im Rahmen der Biometrie stellt sich nicht nur die Frage des „authentischen Nutzers". Nach den „Angriffen von vorn" geht es in einem abschließenden Beitrag um die Manipulationen des technischen Systems, also der Datenbanken, in denen biometrische Rohdaten oder Templates abgespeichert sind (Backend-Angriff) oder Angriffe auf die Kommunikationsstrecken im System bzw. auf Systemkomponenten, z. B. durch Veränderung der Vergleichseinheit oder die Veränderung des Sensors. Man muss also auch der Frage nachgehen, unter welchen Umständen ein „Nutzer" überhaupt wissen kann, dass er es mit einem „authentischen" Biometrie-System zu tun hat.

## Referenzen


Behrens, Michael J.; Roth, Richard (2000): Sind wir zu vermessen, die PIN zu vergessen? In: Datenschutz und Datensicherheit (DuD), Jg. 24 (2000), Heft 6, Wiesbaden: Vieweg, S. 327-331.

Behrens, Michael J.; Roth, Richard (2001): Biometrische Identifikation. Grundlagen, Verfahren, Perspektiven. Wiesbaden: Springer Vieweg.

Bizer, Johann (2004): Personenkennzeichen. In: Datenschutz und Datensicherheit (DuD), Jg. 28 (2004), Heft 1, Wiesbaden: Vieweg, S. 45.

Booz Allen Hamilton GmbH, Bundesdruckerei GmbH, ZN Vision Technologies AG (2003): Leistungsfähigkeit biometrischer Identifikationssysteme zur Ausrüstung von Ausweispapieren. Bochum. [Gutachten zu TAB-Bericht 93]

Deutscher Bundestag (7. Wahlperiode), Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes über das Meldewesen (BMG), BT-Drs. 7/1059. http://dip21.bundestag.de/dip21/btd/07/010/0701059.pdf

Bull, Hans Peter (1984): Datenschutz oder die Angst vor dem Computer. München: Piper.

Jain, Anil; Bolle, Ruud; Pankanti, Sharath (1999): Introduction to Biometrics. In: Jain, Anil; Bolle, Ruud; Pankanti, Sharath: Biometrics: Personal Identification in Networked Society. New York: Springer, S. 1-42.

Köhntopp, Marit; Gundermann, Lukas (1999): Biometrie zwischen Bond und Big Brother. Technische Möglichkeiten und rechtliche Grenzen. In: Datenschutz und Datensicherheit (DuD), Jg. 23 (1999), Heft 3, Wiesbaden: Vieweg, S. 143-150.

Köhntopp, Marit (1999): Technische Randbedingungen für einen datenschutzgerechten Einsatz biometrischer Verfahren. In: Horster, Patrick: Sicherungsinfrastrukturen. Wiesbaden: Vieweg, S. 177-188.

Leopold, Nils (2003): Mehr Sicherheit durch Biometrie? Reader zur Fachanhörung Bündnis 90/ Die Grünen vom 19.05. 2003 in Berlin: „Mehr Sicherheit durch Biometrie?"

Petermann, Thomas; Sauter, Arnold (2002): Biometrische Identifikationssysteme – Sachstandsbericht. TAB-Arbeitsbericht Nr. 76, Berlin: Februar 2002. http://www.tab-beim-bundestag.de/de/publikationen/berichte/ab076.html bzw. http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab076.pdf

Petermann, Thomas; Scherz, Constanze; Sauter, Arnold (2003): Biometrie und Ausweisdokumente – Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung. 2. Sachstandsbericht. TAB-Arbeitsbericht Nr. 93, Berlin: Dezember 2003. http://www.tab-beim-bundestag.de/de/publikationen/berichte/ab093.html bzw. http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab093.pdf

Petermann, Thomas (2004): Vortrag vor dem Bundestags-Ausschuss BFTA, 26.05.2004.

Platanista GmbH (2001a): Biometrische Systeme – FuE, Diffusionstendenzen und Anwendung. Kommentar- und Ergänzungsgutachten, im Auftrag des Deutschen Bundestages (Autoren: Dittmann, J., Mayerhöfer, A., Vielhauer, C.). Darmstadt. [Gutachten zu TAB-Bericht 76]

Roßnagel, Alexander; Hornung, Gerrit (2005): Biometrische Daten in Ausweisen. In: Datenschutz und Datensicherheit (DuD), Jg. 29 (2005), Heft 2, S. 69-73.

TeleTrust/AG 6 – Biometrische Identifikationsverfahren (2006): Biometrische Identifikationsverfahren: Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren, Kriterienkatalog. Version 3.0, Stand: 18.08.2006. http://www.teletrust.de/uploads/media/KritKat-3_final_01.pdf

ULD: Unterlagen des ULD unter https://www.datenschutzzentrum.de/projekte/biometrie/

Vielhauer, Claus (2000): Handschriftliche Authentifikation für digitale Wasserzeichenverfahren. In: Sicherheit in Netzen und Medienströmen. Tagungsband des GI-Workshops „Sicherheit in Mediendaten", Berlin, S. 134-148.

Weichert, Thilo (2002): Datenschutz für Ausländer ... nach dem 11. September 2001. In: Datenschutz und Datensicherheit (DuD), Jg. 26 (2002), Heft 7, S. 423-428.



**Ralf Rebmann**

# Bei Panik Knopfdruck

## Bald online: ein Notrufsystem für Menschenrechtsaktivisten

Amnesty International *entwickelt mit Menschenrechtsaktivisten und Software-Experten den* Panic Button *– eine Notfall-App für Smartphones. Gefährdete Personen sollen damit schnell und sicher einen Hilferuf abschicken können. Gewerkschafter in Kolumbien, kritische Journalisten in Russland oder Frauenrechtlerinnen in Mexiko – sie alle arbeiten unter großem Risiko und geraten dabei selbst in den Fokus repressiver Sicherheitskräfte oder gewalttätiger Gruppen. Die Applikation soll es ihnen ermöglichen, per Smartphone einen Hilferuf an ausgewählte Personen zu senden.*

Zeitgleich mit dem Notruf sollen zudem Informationen über den eigenen Standort übermittelt werden. Als Übertragungsweg dienen SMS-Netze, eine Internetverbindung ist nicht notwendig. Der derzeitige Prototyp lässt sich ausschließlich bei Smartphones mit dem Betriebssystem Android nutzen. Zukünftige Versionen sollen jedoch auch für andere Systeme verfügbar sein. Bei der Entwicklung des *Panic Button* wird Amnesty von der Open-Source-Community und Partnerorganisationen wie der NGO *Front Line Defenders* unterstützt. *„Wir setzen auf einen offenen Entwicklungsansatz und versuchen kontinuierlich auf die Ideen der Aktivisten einzugehen"*, sagt Tanya O'Carroll, verantwortlich für den Bereich *Technologie und Menschenrechte* bei Amnesty.


*Courtesy of IDEO*

Der *Panic Button* ist das Ergebnis zahlreicher Workshops, an denen Vertreter von Amnesty International, Software-Entwickler und Menschenrechtsaktivisten in den vergangenen Monaten teilgenommen haben. Verschiedene Konzepte wurden vorgestellt und auf Sicherheitsaspekte und Durchführbarkeit überprüft. Der *Panic Button* wurde schließlich als Projekt ausgewählt. Die Sicherheit der App spielte in den Diskussionen eine Schlüsselrolle. Ein absolut sicheres Produkt könne es jedoch nicht geben, sagt O'Carroll. Auch mit der sichersten App seien Mobiltelefone ein Sicherheitsrisiko. Deshalb hänge der Einsatz des *Panic Button* auch von der allgemeinen Gefahrenlage in den betreffenden Konfliktgebieten ab.

Bei einem Workshop, der Ende 2012 in Nairobi stattfand, diskutierten rund 20 Menschenrechtsaktivisten nicht nur technische Details rund um den *Panic Button*, sondern auch allgemeine Aspekte zur Sicherheit und Anonymisierung von Nachrichten und Netzwerken. Unter den teilnehmenden Aktivisten war auch Nighat Dad. Die 32-Jährige ist Anwältin, Internetaktivistin und Frauenrechtlerin. In ihrem Heimatland Pakistan kämpft sie für ein freies Internet und gegen Zensur. Um dieses Ziel zu erreichen, hat sie die Organisation *Digital Rights Foundation* gegründet. Den *Panic Button* bewertet sie positiv: *„Die App unterstützt Aktivisten dabei, ein sicheres Netzwerk von Unterstützern aufzubauen"*, sagt sie. Eine Einschränkung sieht sie darin, dass die App derzeit nur bei Smartphones funktioniert. *„Aktivisten in Konfliktgebieten verfügen meist über einfachere Mobiltelefone, das könnte anfangs eine Hürde sein."* Zusammen mit anderen Aktivisten wird sie die weitere Entwicklung der App begleiten. Im September 2013 soll der *Panic Button* in die nächste Etappe gehen. Dann wollen rund 100 Menschenrechtsaktivisten

**Ralf Rebmann**

**Ralf Rebmann** ist Journalist und lebt in Berlin.

ihn einem weiteren Test unterziehen. Finanzielle Unterstützung erhielt Amnesty International jüngst durch einen von Google ausgerichteten Wettbewerb, den *Google Global Impact Challenge*. Neben weiteren Organisationen erhielt Amnesty 100.000 Britische Pfund, um den *Panic Button* weiterzuentwickeln.[1] Bis die Notfall-App einer größeren Anzahl von Aktivisten zur Verfügung steht, wird es allerdings noch eine Weile dauern. Die offizielle Veröffentlichung ist für das Frühjahr 2014 geplant.

*Übernommen aus Amnesty Journal 08/09-13 mit freundlicher Genehmigung des Autors.*

## Anmerkung

*1 http://livewire.amnesty.org/2013/06/04/thank-you-for-voting-amnestys-panic-button-will-become-a-reality/*





**Humanistische Union**
**Internationale Liga für Menschenrechte**
**Bundesarbeitskreis Kritischer Juragruppen**

# Brauchen wir den Verfassungsschutz? Nein!

## Memorandum

*Die Geschichte des Verfassungsschutzes ist eine Geschichte der Rechtsbrüche, des Machtmissbrauchs, der demokratischen Zumutungen. Diese Erkenntnis ist nicht neu, sie gerät über den ständigen (Terror-) Warnungen immer wieder in Vergessenheit. Um daran zu erinnern, hat die Humanistische Union zusammen mit anderen Bürgerrechtsorganisationen ein Memorandum zum Verfassungsschutz (VS) verfasst.[1] Es zeigt, wie überflüssig der VS ist. Weder kann noch soll er seine zentrale Aufgabe als „Frühwarnsystem" wahrnehmen, sie ist mit dem demokratischem Verständnis einer offenen Gesellschaft unvereinbar. Für seine weiteren Aufgaben erweisen sich andere Institutionen als viel effektiver. Die öffentliche Kontrolle eines im Verborgenen agierenden Geheimdienstes schließlich ist ein Ding der Unmöglichkeit. Daher gibt es nur eine Alternative: der Verfassungsschutz gehört ersatzlos abgeschafft. Wir dokumentieren hier einen Auszug aus dem Memorandum, das als separater Sonderdruck erhältlich ist (siehe Anzeige rechts).*

### Thesen

1. **Eine demokratische Gesellschaft lebt von der Meinungsvielfalt.** Radikale Auffassungen und Bestrebungen (die von den vorherrschenden Meinungsbildern abweichen) sind deshalb nicht nur zulässig, sondern auch wünschenswert – solange die Grenzen zur Strafbarkeit bzw. zu gewalttätigem Handeln nicht überschritten werden. Staatliche Behörden dürfen derartige Äußerungen weder als „verfassungsfeindliche" oder „extremistische" Bestrebungen abqualifizieren, beobachten oder gar verfolgen. Wir brauchen kein staatliches „Frühwarnsystem" zur Beobachtung derartiger Auffassungen und Bestrebungen.

2. **Geheimdienstlicher Verfassungsschutz ist schädlich**, wie auch die zahlreichen Verfehlungen und Skandale in der Geschichte der Bundesrepublik zeigen. Es handelt sich dabei nicht um zufällige, persönliche oder vermeidbare Fehler, sondern systematisch bedingte Mängel eines behördlichen und geheimdienstlichen „Verfassungsschutzes".

3. **Die gesetzlichen Aufgaben der Verfassungsschutzbehörden sind überflüssig.** Bei ihrem Wegfall entsteht keine Sicherheitslücke. Eine Aufgaben- und Befugnisüberleitung von den Verfassungsschutzbehörden auf die Polizei ist daher nicht erforderlich. Der Schutz vor Gewalt und Straftaten obliegt der Polizei, der Staatsanwaltschaft und den Gerichten.

4. **Eine Kontrolle geheim arbeitender Verfassungsschutzbehörden, die rechtsstaatlichen und demokratischen Ansprüchen genügt, ist nicht möglich.** Auch Kontrollverbesserungen sind untauglich: ein transparenter, voll kontrollierbarer Geheimdienst ist ein Widerspruch in sich.

5. **Die Verfassungsschutzbehörden sind ersatzlos abzuschaffen** – allein schon deshalb, um nicht in Zeiten knapper Kassen und in Beachtung der verfassungsrechtlichen Schuldenbremse jährlich eine halbe Milliarde Euro für überflüssige, ja schädliche Behörden auszugeben. Es bedarf auch keiner ersatzweisen, mit offenen Quellen arbeitenden staatlichen Informations- und Dokumentationsstelle über extremistische Bestrebungen. Das Problem besteht nicht in einem mangelnden Wissen über radikale, bisweilen auch menschenverachtende Meinungen und Haltungen in unserer Gesellschaft. Die Auseinandersetzung darüber muss mit politischen, demokratischen Mitteln geführt werden; sie ist innerhalb der Gesellschaft zu führen.

### Bemerkungen zum „Verfassungsschutz"[2]

Was seit November 2011 über den Nationalsozialistischen Untergrund (NSU) und die von ihm begangenen Morde bekannt geworden ist, brachte das Vertrauen von Politik und öffentlicher Meinung in die Arbeit der deutschen Sicherheitsbehörden ins Wanken – zumindest für einen kurzen Augenblick. So unfassbar waren die Pannen und Fehler, die Ignoranz und ideologischen Scheuklappen von Polizei, „Verfassungsschutz" und anderer Geheimdienste, dass die Chance für einen kompletten Neuanfang realistisch schien. Selbst in Zeitungen, die revolutionärer Neigungen unverdächtig sind, erschienen Beiträge, die das Ende der Verfassungsschutzbehörden verkündeten oder jedenfalls für erwägenswert hielten.

Diese Umbruchstimmung hielt jedoch nur kurze Zeit an. Während sich der vom Bundestag eingesetzte Untersuchungsausschuss[3] noch um die Aufklärung und Analyse der Versäumnisse bemühte (sein Abschlussbericht wird für Juni 2013 erwartet), begann die Politik bereits mit dem von ihr verkündeten „Neustart". Er beschränkt sich beim überwiegenden Teil der politischen Parteien[4] jedoch auf einen bloßen Pannendienst.

Die eine oder andere vorgeschlagene Maßnahme mag gut gemeint sein. Alle Reformvorschläge werden jedoch nicht dem Problem gerecht, das geheim arbeitende Behörden für ein demokratisches und rechtsstaatliches Gemeinwesen aufwerfen; ja sie verstärken wie im Falle weiterer Zentralisierung noch deren fatale Wirkungsweise.

### Statt Pannendienst: Frage nach der Notwendigkeit von Geheimdiensten

Vielmehr muss endlich von Grund auf die Frage gestellt werden, ob die Konzeption staatlicher Sicherheitswahrnehmung[5] überhaupt noch stimmt, sofern sie überhaupt jemals gestimmt hat: Sind die bestehenden staatlichen Einrichtungen zur Sicherheitsvorsorge und Gefahrenabwehr alle erforderlich? Vor allem aber: Sind sie auch einer Gesellschaft angemessen, die sich in ihrer Verfassung zu den unveräußerlichen Grundrechten und Grundfreiheiten ihrer Bürgerinnen und Bürger bekennt?

Staatliche Sicherheitspolitik hat die grundrechtlich zuerkannten Freiheitsrechte zu achten und schützen. Dazu gehören namentlich die Meinungsfreiheit und die Versammlungsfreiheit als Recht auf die kollektive Geltendmachung von Grundrechten. Die Grenzen der Grundrechtsausübung ergeben sich aus der Verfassung, genauer: aus den Artikeln 18 und 21 Abs. 2 des Grundgesetzes, und aus den kollidierenden Grundrechten Dritter, der Menschenwürde, der körperlichen Integrität, und nicht zuletzt aus dem Strafrecht, das diese Grenzen nachzeichnet.

Solange und soweit sich die Ausübung von Grundrechten, insbesondere die Meinungs(äußerungs)freiheit innerhalb der genannten Grenzen bewegt, kann es nicht staatliche Aufgabe sein, die Bürgerinnen und Bürger zu beobachten, zu registrieren, zu stigmatisieren, zu verfolgen, zu diskreditieren oder zu zensieren und auszugrenzen. Genau dies ist aber unter Anwendung des ideologiebeladenen und daher missbrauchsgeneigten Kampfbegriffs der „streitbaren Demokratie" seit langem der Fall; in zunehmendem Maße und mit unterschiedlichen Schwerpunkten nach Maßgabe wechselnder politischer Opportunität. Es sind vor allem die verschiedenen Geheimdienste, namentlich die 17 Verfassungsschutzbehörden von Bund und Ländern, die den politischen Diskurs der Bundesrepublik überwachen – nachzulesen in ihren jährlichen Verfassungsschutzberichten und ausweislich ihrer Skandalgeschichte.

Bedarf es vor diesem Hintergrund zur Sicherheitswahrnehmung „nach innen" neben der Polizei und speziellen Gefahrenabwehrbehörden (z. B. Bauaufsicht, Brandschutz oder Lebensmittelsicherheit, Verkehrsbehörden) auch noch geheimdienstlich arbeitender Verfassungsschutzbehörden?

### Gesellschaftliche Vergesslichkeit als Bedingung des Weiterbestehens des „Verfassungsschutzes“

Der Rückblick in die bundesdeutsche Geschichte der Geheimdienste zeigt, dass eine Bedingung ihrer Fortexistenz im Vergessen besteht, dem permanenten gesellschaftlichen Vergessen der vielen Skandale und Anmaßungen der Geheimdienste. Dem wollen wir mit dieser Broschüre vorbeugen. Wir können heute nicht mehr darauf vertrauen, dass die fortwährenden Skandale im Sicherheitsbereich unsere unter Mühen erreichten demokratischen Strukturen unbeschadet lassen. Wir wollen, wie auch andere Akteure[6], das Bewusstsein dafür wach halten, wie fragwürdig die Konstruktion eines staatlich administrativen „Verfassungsschutzes“ ist, der selbst zu dem Problem geworden ist, das er zu lösen vorgibt.

Unsere Schrift beschränkt sich auf die Ämter bzw. Behörden für Verfassungsschutz in Bund und Ländern. Unsere Kritik und Sorge gilt in gleicher Weise den weiteren Geheimdiensten unseres Landes, namentlich dem Militärischen Abschirmdienst, den abzuschaffen ja bereits in der etablierten Politik diskutiert wird, und dem Bundesnachrichtendienst (BND), der als Auslandsgeheimdienst weitgehend rechtsfrei agiert.

Demokratie, wenn sie mehr sein will als eine periodische Schönwetter-Demokratie, muss sich gegen die Zumutungen solcher Art autoritärer Zuteilung von bürgerlichen Freiheiten wehren. Es gibt sie, die alternativen Lösungen. Sie liegen allein im lebendigen demokratischen gesellschaftlichen Diskurs, den es auszuhalten gilt.

*Humanistische Union, Internationale Liga für Menschenrechte, Bundesarbeitskreis Kritischer Juragruppen (Hg.): Brauchen wir den Verfassungsschutz? Nein! Memorandum, erarbeitet von Dr. Rolf Gössner, Johann-Albrecht Haupt, Dr. Udo Kauß, Dr. Till Müller-Heidelberg, Thomas von Zabern. Humanistische Union: Berlin 2013*

## Anmerkungen

1 *Das FIfF zählt zu den Unterstützern des Memorandums.*

2 *Dieser Abschnitt ist eine leicht gekürzte Fassung des Einleitungskapitels zum Memorandum: Einleitende Bemerkungen zum „Verfassungsschutz“*

3 *Siehe den gemeinsamen Antrag der Fraktionen CDU/CSU, SPD, FDP, DIE LINKE. und Bündnis 90/Die Grünen zur Einsetzung eines Untersuchungsausschusses, BT-Drs. 17/8453 v. 24.1.2012.*

4 *Ausnahme DIE LINKE und Teilausnahme bei Bündnis 90/Die Grünen: Fraktionsbeschluss vom 27.11.2012 „Für eine Zäsur in der deutschen Sicherheitsarchitektur – Auflösung des Verfassungsschutzes, Neustrukturierung der Inlandsaufklärung und Demokratieförderung“.*

5 *Wir benutzen bewusst nicht das schönfärberische Modewort der ‚Sicherheitsarchitektur‘, weil dieses eine in unseren Augen nicht vorhandene, souveräne Gestaltungsmacht suggeriert.*

6 *U. a. Claus Leggewie und Horst Meier, Nach dem Verfassungsschutz, Berlin 2012.*

**Sebastian Jekutsch**

## Betrifft: Faire Computer

*Fair wie in* Fairer Kaffee.

Wie mühselig die Arbeit für eine sozialverträglichere IT-Herstellung ist, zeigen am besten die beiden Vorzeigeprojekte. Das holländische **FairPhone** hat bis Redaktionsschluss knapp 13.000 Geräte verkauft. Das genügt zwar locker für eine Vorfinanzierung der Produktion der nun geplanten 20.000 Geräte, aber erst wenn man bedenkt, dass eine der Foxconn-Fabriken diese Menge in wenigen Stunden produzieren kann, werden einem die Relationen bewusst. Bis zur Lieferung der ersten Geräte wird in Amsterdam an größerer Transparenz gearbeitet. **NagerIT**, der bayerische Hersteller der teilfairen gleichnamigen Computermaus, ist dort Vorreiter und hat die Zuliefer- und Herkunftskette so detailliert wie eben möglich veröffentlicht. Ziel in den nächsten Wochen ist es, ein durch und durch faires USB-Kabel herzustellen. Das Schöne: Es könnte eine Kooperation zwischen den beiden Projekten geben, denn für das FairPhone wird auf Wunsch ebenfalls ein USB-Kabel geliefert.

Was passiert bei den Großen? **Googles Motorola** überrascht mit der Nachricht, dass ihr neues Handy in Texas zusammengeschraubt wird, was in den U.S.A. ein echtes Pro-Argument ist. Apple überrascht mit der Zusage, der Herkunft des Zinns in ihren Geräten nachgehen zu wollen, freilich erst nach monatelangem öffentlichem Druck von *Friends of the Earth* (England), die umwelt- und menschenfeindliche Zustände in Indonesiens Minen aufdeckte. Weniger überraschend ist, dass **Foxconn** sein Versprechen, einen Betriebsrat einzurichten, schlicht nicht umgesetzt hat. Zu viel versprochen hat vermutlich auch **Apple**: Sie wollten bis 1. Juli 2013 durchgehend maximal 60 Arbeitsstunden in der Woche zulassen – dabei ist auch das nach chinesischem Gesetz illegal –, behaupteten sogar, dass dies zu 98 % schon umgesetzt sei. Komisch allerdings, dass unabhängige Interviews mit Arbeitern dem widersprechen. Man wundert sich nicht selten über die häufige Diskrepanz zwischen vom Markenhersteller in Auftrag gegebenen Audits und den Erkenntnissen von Arbeitsaktivisten.

Klärung bietet der Bericht von *China Labor Watch* mit Sitz in New York über den Kontrakthersteller **Pegatron**. Undercover gingen sie in die chinesischen Fabriken, arbeiteten mit und interviewten Kollegen. Ergebnis: Auch hier Überstunden in unerlaubtem Maß, unbezahlte Zwangs„besprechungen“, Akkordarbeit, stundenlanges Stehen beim Arbeiten, Verweigern von

*Am Rande einer IT-Konferenz zur nachhaltigen öffentlichen Beschaffung von IT in Rostock trafen sich NagerIT (links Susanne Jordan, mit Maus auf dem Knie) und FairPhone (rechts Miquel Ballester, mit Bart), zwischen Ihnen ein Schaubild der Lieferkette der Maus. Dabei auch Salve Valenciano (hinten im Bild), die auch bei einer FIfF-Veranstaltung in Hamburg einen Vortrag über die Arbeitsbedingungen in der Elektronikindustrie der Philippinen hielt.*

versprochenen Pausen, Verzögern von Gehaltszahlungen, ausbildungsfremde Beschäftigung von Schülern und Praktikanten. Aber auch: Die Arbeiter werden von den Vorgesetzten gezwungen, ihre Stundenzettel zu fälschen: „**The document's only purpose is to deceive Apple during inspections**." Pegatron fertigt außerdem vermutlich für Nokia, Panasonic, HP, Dell, Lenovo, Acer, Sony, Toshiba und natürlich Asus, dem Unternehmen aus dem Pegatron vor wenigen Jahren hervorgegangen ist.

Samsung schafft es bei alledem auf magische Weise, kaum Aufmerksamkeit zu erregen. Ohne Widerhall in den Medien blieb z. B. dass die Organisation SHARPS, die seit Jahren auffällige Leukämie-Fälle in Samsung-Werken aufdeckt, ebenfalls in die Zuliefererbetriebe gegangen ist und Unanständiges zu berichten hatte. Derweil machte **Samsung** wahr, was viele als Trend erwarten: Es expandiert nicht mehr im zunehmend teureren China, sondern geht nach Vietnam. Geschickt auch, was sie für ihr Image geschafft haben: Der bekannte Zertifizierer **TCO Development** (ich habe in der letzten Ausgabe davon berichtet) hat als erstes ge-label-tes Smartphone ein Samsung-Gerät in ihren Listen. Das Zertifikat umfasst auch Sozialkriterien, die nicht sehr streng sind, aber immerhin über die üblichen Selbstverpflichtungen der Industrie hinausgehen.

TCO hat aus den Reihen der Nichtregierungsorganisationen dafür sogleich Prügel bekommen: Wie könne man trotz oben genannter Probleme und der Anti-Gewerkschafts-Politik bei Samsung diesem alles Gute bescheinigen? TCO will nun untersuchen, ob bei der Herstellung des zertifizierten Produkts tatsächlich die Vorwürfe zutreffen. Dazu muss Samsung ihnen Dokumente aushändigen und sie in die Fabriken lassen, sonst verliert es das Label. Und das ist die gute Nachricht: Samsung wird nun hochoffiziell kontrolliert.

Mühsam ist, wie gesagt, die Arbeit für eine sozialverträglichere IT-Herstellung. Sollte man nicht besser gleich alles in gesetzliche Regelungen gießen? Ja, sollte man. So gibt es derzeit drei relevante Richtlinienvorhaben der EU, über die hier berichtet werden könnte. Wir verweisen an dieser Stelle aber lieber auf die nächste FIfF-Kommunikation im Dezember, die dieses und andere Themen zu *Faire Computer* behandelt, denn es wird das Schwerpunktthema sein.

**Sebastian Jekutsch**

**Sebastian Jekutsch** ist aktiv beim AK Faire Computer des FIfF. Unser Angebot: News über Twitter per *@fairecomputer* und tiefergehende Analysen unter *blog.faire-computer.de*.
Wir suchen noch MitstreiterInnen! Kontakt: *fairit@fiff.de*.

**Stefan Hügel**

# Log 3/2013

## Ereignisse, Störungen und Probleme der digitalen Gesellschaft

*Immer wieder gibt es Ereignisse, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau von Bürgerrechten stehen. Wir dokumentieren hier einige davon. Die Aufzählung ist sicherlich nicht vollständig; mit einigen besonders bedeutsamen Ereignissen wollen wir aber auf die weiterhin besorgniserregende Entwicklung hinweisen.*
*In den vergangenen Wochen wurde das Thema durch die Enthüllungen zur weltweiten Ausspähung des Internet durch Geheimdienste überschattet, diese haben wir in einer eigenen Chronologie zusammengestellt (Seite 24). Viele weitere Ereignisse erscheinen vor diesem Hintergrund fast lächerlich. Dieses Log erscheint in gekürzter Form, wir wollen aber die Ereignisse über PRISM, Tempora, XKeyscore & Co. hinaus nicht außer Acht lassen.*



### Mai 2013

**3. Mai 2013:** Der Gesetzentwurf zur Bestandsdatenauskunft wird vom Bundesrat bestätigt. Nachdem das umstrittene Gesetz zum Zugriff auf Informationen von Anschlussinhabern, wie Passwörtern und IP-Adressen, bereits zuvor auch vom Bundestag verabschiedet worden war, kann es nun in Kraft treten. Datenschützer und Bürgerrechtler sehen erneut erhebliche verfassungsrechtliche Mängel; die Politiker der Piratenpartei Patrick Breyer und Katharina Nocun kündigen wenig später eine Verfassungsbeschwerde gegen das Gesetz an (Quelle: Bundesrat, Heise).

**13. Mai 2013:** Parallel zu den Debatten im europäischen Parlament diskutiert der europäische Rat seine Position zur EU-Datenschutz-Grundverordnung. Einer Notiz der irischen Ratspräsidentschaft zufolge wird dabei vorgeschlagen, die bisher geforderte explizite Einwilligung in die Datenverarbeitung aufzuweichen. Durch die Ersetzung von „explizit" durch „unzweideutig" sollen die Standards gesenkt werden. Firmen sollen personenbezogene Daten sammeln dürfen, wenn dies adäquat, relevant und „nicht ausufernd" ist. Die Datenschutzbeauftragten von Bund und Ländern hatten zuvor gefordert, die bisher vorgesehenen Regeln zur expliziten Einwilligung ohne Abstriche beizubehalten (Quelle: Heise).

**14. Mai 2013:** Zur Nutzung des von Microsoft übernommenen Dienstes Skype gibt der Nutzer sein Einverständnis, dass alles mitgelesen werden darf. Von diesem Recht macht Microsoft offenbar auch Gebrauch: Werden in Chats HTTPS-URLs verschickt, wird kurz danach von Microsoft-Servern aus auf diese Adressen zugegriffen. Microsoft erklärt dies mit der Filterung von Phishing- und Spam-Seiten – dies ist aber wenig glaubwürdig, da solche Seiten in der Regel kein HTTPS verwenden. Seiten, die über HTTP zu erreichen sind, bleiben offenbar unangetastet (Quelle: Heise).

**16. Mai 2013:** Nachdem zuvor Journalisten der Nachrichtenagentur AP illegel bespitzelt worden waren, kündigt US-Präsident Barack Obama einen verbesserten Schutz für Whistleblower und Journalisten an. Dadurch soll eine bessere Balance zwischen Freiheit der Berichterstattung und nationalen Sicherheitsinteressen erreicht werden. Der entsprechende Entwurf stammt von 2009, wurde aber angesichts der Wikileaks-Veröffentlichungen zunächst zurückgezogen (Quelle: Heise).

**27. Mai 2013:** Der Bundesdatenschutzbeauftragte Peter Schaar wirft Microsoft vor, mit seiner Xbox One ein Überwachungsinstrument auf den Markt zu bringen. Durch die Xbox One würden ständig alle möglichen Informationen registriert und auf externen Servern verarbeitet. Microsoft will die gewonnen Daten für personalisierte Angebote nutzen; in einem Patentantrag ist auch eine Technik beschrieben, mit der Abrechnungsmodelle anhand der Zuschauer- bzw. Spielerzahlen umgesetzt werden können. Schaar geht aber nicht davon aus, dass durch die Technik die Wohnzimmer der Nutzer ausspioniert werden sollen (Quelle: Spiegel, Heise).

**28. Mai 2013:** Das Bundeskriminalamt (BKA) tauscht „Informationen und Erfahrungen zu polizeilichen Überwachungsmöglichkeiten" mit anderen Staaten aus. Hintergrund ist offenbar die zunehmende IP-Telefonie und damit verbundene Verschlüsselungsmöglichkeiten. Beteiligt sind Belgien, Dänemark, Frankreich, Großbritannien, Luxemburg, die Niederlande, Österreich, Liechtenstein, die Schweiz, Israel und die USA. Bereits zuvor war das BKA an der nach dem Hersteller der umstrittenen und offenbar nicht verfassungsgemäßen Trojanersoftware benannten DigiTask User Group – die später in Remote Forensic Software User Group umbenannt wurde – beteiligt (Quelle: Andrej Hunko MdB, Heise).

**30. Mai 2013:** Der europäische Datenschutzbeauftragte Peter Hustinx ermahnt den europäischen Gesetzgeber, „unangemessenen Druck" von Wirtschaft und Drittstaaten bei der Debatte über die EU-Datenschutz-Grundverordnung abzuwehren. Er kritisiert die „außergewöhnlich intensiven" Lobby-Aktivitäten (Quelle: EU-Datenschutzbeauftragter, Heise).

**31. Mai 2013:** Das dänische Justizministerium legt einen Bericht vor, nach dem die Vorratsdatenspeicherung bei der Aufklärung von Straftaten im Internet nicht hilfreich sei. Die Polizei habe keinen Nutzen aus den gelieferten Daten gezogen. Stattdessen ergäben sich aus der Protokollierung erhebliche Probleme in der Praxis (Quelle: Dänisches Justizministerium, Heise).

### Juni 2013

**4. Juni 2013:** Der UN-Sonderbeauftragte für den Schutz der Meinungs- und Informationsfreiheit, Frank La Rue, warnt vor der zunehmenden Überwachung des Internet. Viele Staaten griffen beispielsweise unter dem Vorwand der Terrorismusbekämpfung in die Grundrechte ihrer Bürger ein; die Gesetzgebung halte damit nicht Schritt. Seiner Ansicht nach ist die vollständige Überwachung der Kommunikation möglich und bezahlbar. Die Einschränkung der unbeobachteten und anonymen Kommuni-

kation dürfe nur in Ausnahmefällen unter Aufsicht einer unabhängigen Justiz erfolgen (Quelle: UN – Office of the High Commissioner for Human Rights, Heise).

**6. Juni 2013:** Einem Bericht des Guardian zufolge sammelt der US-amerikanische Geheimdienst National Security Agency (NSA) umfassend Daten über Telefongespräche von US-Bürgern im In- und Ausland. Detaillierte Daten würden nach einem Gerichtsbeschluss auf Basis des Foreign Intelligence Surveillance Act (FISA) durch den Telefonanbieter Verizon an die Behörde übermittelt. Als Beleg wird die mutmaßliche Kopie eines streng geheimen Gerichtsbeschlusses vorgelegt (Quelle: The Guardian, Heise).

*Der Bericht ist der Auftakt einer Reihe weiterer Enthüllungen über die umfassende Ausspähung der weltweiten Kommunikation durch Geheimdienste. Wir haben den Verlauf dieser Enthüllungen in einer eigenen Chronologie (ab Seite 24) zusammengestellt.*

**6. Juni 2013:** Nachdem die Justizminister der europäischen Union sich nicht über die Grundzüge einer Novelle des europäischen Datenschutzrechts einigen konnten – obwohl der ursprüngliche Vorschlag bereits verwässert worden war – wird sich die Reform des Datenschutzes voraussichtlich weiter hinziehen. Viele der beteiligten Staaten, darunter Deutschland, melden Klärungsbedarf an (Quelle: Heise).

**12. Juni 2013:** Big-Data-Techniken werden bei Xerox zur Durchleuchtung von Bewerbern im Niedriglohnsektor verwendet. Eine Software des Unternehmens Evolv wird dabei eingesetzt, um mit Hilfe von Methoden aus der Datenanalyse ideale Kandidaten für die Stellenbesetzung herauszufiltern. Die Analyse erfolgt anhand von Kriterien, die sich aus Persönlichkeitsmerkmalen ergeben (Quelle: Technology Review, Heise).

**21. Juni 2013:** Bereits durch Verbindungsdaten können detaillierte Profile von Personen gebildet werden. Beteuerungen, dass bei der Kommunikationsüberwachung wie der Vorratsdatenspeicherung keine Kommunikationsinhalte erfasst würden, sind damit irreführend. Für die Analysen können auch anonymisierte Daten verwendet werden; so konnten anhand von vier Datensätzen aus Anrufen die Bewegungen von 95 % der Anrufer nachvollzogen werden. Dafür waren keinerlei Informationen über Gesprächsinhalte erforderlich (Quelle: Technology Review, Heise).

**27. Juni 2013:** Die meisten tödlichen Drohnenangriffe der USA in Pakistan gelten nicht namentlich bekannten Terroristenführern, sondern häufig Milizionären unterer Ränge. Sie werden getötet, obwohl weder ihre Identität, noch ihre Beziehung zu Al-Qaida bekannt sind. Angriffe erfolgen aufgrund von Hinweisen – aufgezeichnet von Drohnenkameras, Satelliten, Mobilfunkfallen, Agenten vor Ort oder anderen „Quellen und Methoden" der Geheimdienste – dass es Mitglieder einer Organisation sein könnten, die als „legitimes" Ziel eines Drohneneinsatzes gelten (Quelle: Technology Review, Heise).

## Juli 2013

**9. Juli 2013:** Vor dem europäischen Gerichtshof (EuGH) werden mehrere Klagen gegen die Richtlinie zur Vorratsdatenspeicherung (2006/24/EG) verhandelt. Dabei fragten die Richter kritisch und detailliert nach; die Befürworter taten sich schwer damit, die Notwendigkeit der Richtlinie in der Verhandlung darzustellen (Quelle: Heise).

**10. Juli 2013:** Die Fähigkeit von Smartphones, die Position ihrer Nutzer jederzeit genau bestimmen zu können, nutzt das Unternehmen Sense Networks dafür, Schlüsse auf Lebensgewohnheiten und Vorlieben zu ziehen. Ziel ist dabei, potenziellen Käufern zielgerichtete Werbung zum richtigen Zeitpunkt zu präsentieren und damit einen sicheren Kaufanreiz zu schaffen (Quelle: Technology Review, Heise).

**12. Juli 2013:** Die Browser-Erweiterung 1Button-App von Amazon ermöglicht einen detaillierten Einblick in des Surfverhalten des Nutzers. Die URLs der aufgerufenen Web-Seiten werden an einen Amazon-Server und an den Statistikdienst Alexa übermittelt. Zusätzlich protokolliert sie die Nutzung von Google und wertet angezeigte Treffer aus, wie Heise Security reproduzieren konnte (Quelle: Heise).

**22. Juli 2013:** In Großbritannien soll ein landesweiter Internet-Filter installiert werden. Dies kündigt Premierminister David Cameron in einer Rede an. Der Filter soll automatisch aktiviert sein, wenn nicht ein Erwachsener explizit die Abschaltung wünsche. Durch den Filter sollen vorgeblich Kinder und Jugendliche vor Pornographie geschützt werden; später werden auch weitere Ideen für zu filternde Inhalte bekannt (Quelle: gov.uk, Heise).

**24. Juli 2013:** Ungeachtet des Datenausspähskandals fordern die US-Finanzaufsichtsbehörden Securities Exchange Commission (SEC) und Commodity Futures Trading Commission (CFTC), im Rahmen der Verhandlungen über die Regulierung des außerbörslichen Derivatehandels selbst auf Unterlagen in den Zentralen europäischer Banken, wie Kontodaten oder Verträge, zuzugreifen. Die europäischen Verhandlungspartner sehen die Gefahr von Wirtschaftsspionage (Quelle: Heise).

**27. Juli 2013:** Allen Kunden, die Geld vom Arbeitsamt überwiesen bekommen, hat die österreichische Bank BAWAG/PSK, unabhängig von der tatsächlichen Bonität, den Rahmen für die Kontoüberziehung gestrichen. Von der Streichung sind auch die Mitarbeiter des österreichischen Arbeitsservice betroffen. Die Entscheidungen werden automatisiert getroffen, indem Kontobewegungen nach Stichwörtern durchsucht werden. Es besteht der Verdacht, dass das Vorgehen gegen Datenschutzbestimmungen verstößt (Quelle: Kurier, Heise).

**28. Juli 2013:** Einem Bericht der Organisation China Labor Watch (CLW) zufolge, werden bei dem chinesischen Apple-Zulieferer Foxconn weiterhin mehr als 10.000 Schüler und Studenten unter inakzeptablen Arbeitsbedingungen beschäftigt. Schichten dauerten nach den Berichten 12 und mehr Stunden, Arbeiter müssen teilweise ganztägig stehen, auch Schwangere und Minderjährige müssen acht und mehr Stunden täglich arbeiten. Der Umgangston sei durch Pöbeleien und Einschüchterungen geprägt. Teile des Lohns würden durch die vermittelnden Lehrer und Schulen einbehalten (Quelle: China Labor Watch, Spiegel, Heise).

# Schwerpunkt „Weltweite Datenausspähung“



**Sara Stadler**

## Telefon- und Internetüberwachung

### Chronologie der Enthüllungen

*Seit mehr als 2 Monaten nimmt der Skandal um die Internetüberwachung unter anderem durch US-amerikanische und europäische Geheimdienste einen zentralen Platz in den täglichen Nachrichten ein. Beinahe jeden Tag wird eine neue Enthüllung präsentiert und oft empören sich die selben sogleich über die NSA, die am nächsten Tag die Notwendigkeit vergleichbarer Überwachungsmaßnahmen in der EU, wie der Vorratsdatenspeicherung, unterstreichen. Die Fülle der Ereignisse und Berichte ist uns eine detaillierte Übersicht wert.*

#### Juni 2013

**6. Juni 2013:** Die britische Zeitung *The Guardian* berichtet, dass der US-Geheimdienst NSA Telefondaten von Millionen US-EinwohnerInnen sammele. Einem streng geheimen Gerichtsbeschluss zufolge müsse der Telefonanbieter Verizon Informationen wie Rufnummern, Standort und Dauer bezüglich aller Telefonate innerhalb der USA und von dort aus ins Ausland an den Geheimdienst weitergeben (Quelle: Heise, The Guardian).

**7. Juni 2013:** Die Berichte über die Spionageaktionen der US-Geheimdienste weiten sich aus. Laut dem *Wall Street Journal* sammelt die NSA neben den Telefondaten von Verizon auch jene der Kunden von AT&T und Sprint Nextel, sowie Metadaten über E-Mails, Internetsuchen und Kreditkartenzahlungen.

Der *Guardian* berichtet, dass NSA und FBI seit 2007 im Rahmen des streng geheimen Programms PRISM die zentralen Rechner von Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube und Apple anzapfe und damit Zugriff auf alle dort gesammelten Daten, wie Fotos, Emails, Dokumente oder Kontaktdaten erhalte. Dass dies mit ihrer Genehmigung erfolge, bestreiten die genannten Unternehmen. US-Präsident Barack Obama rechtfertigt die Telefon- und Internetüberwachung durch seine Regierung als Mittel zur Terrorismusbekämpfung.

Am selben Tag berichtet der *Guardian*, dass auch der britische Geheimdienst GCHQ seit 2010 von dem Netzspionage-Programm PRISM profitiere und insgesamt 197 Berichte auf Grundlage der so gewonnen Daten erstellt habe. Diese könnten über ein gesondertes Programm abgegriffen werden, dass speziell für den GCHQ eingerichtet worden sei. Wie lange und unter wessen Mitwisserschaft auf PRISM zugegriffen wurde, bleibe unklar (Quelle: The Guardian, Heise, Wall Street Journal).

**8. Juni 2013:** Der 29-jährige Techniker Edward Snowden bekennt sich in einem Videointerview mit dem *Guardian* öffentlich, die Quelle der Enthüllungen um das US-Spionageprogramm PRISM gewesen zu sein. Während die US-Regierung das ausufernde Sammeln von Daten leugnet und PRISM lediglich als ein internes Computersystem zur legalen Datensammlung darstellt, spricht Snowden, der als Mitarbeiter externer Unternehmen für den Geheimdienst tätig war, von einer „*infrastructure that allows it to intercept almost everything*“ (dt: „Infrastruktur, die es erlaubt, fast alles abzufangen“) (Quelle: The Guardian, Heise).

**12. Juni 2013:** Aus Kanada wird bekannt gegeben, dass dort ebenfalls seit Jahren eine massive Telefon- und Internetüberwachung stattfindet. Der Verteidigungsminister Peter MacKay gibt zu, den Geheimdienst CSE zur weltweiten Ausspähung von Verbindungsdaten autorisiert zu haben (Quelle: Heise).

**13. Juni 2013:** Edward Snowden bringt einen neuen Aspekt in die Debatte um Hackerangriffe aus China gegen die USA, indem er berichtet, dass der US-Geheimdienst NSA China seit Jahren durch Hacker angreifen lasse. Seit 2009 habe es mehrere hundert Hackerangriffe auf China, weltweit mehr als 61.000 gegeben (Quelle: The Guardian, Heise).

**14. Juni 2013:** Die Finanznachrichtenagentur *Bloomberg* berichtet unter Bezugnahme auf nicht namentlich genannte InsiderInnen, dass die Zusammenarbeit zwischen Unternehmen und Geheimdiensten in den USA noch umfangreicher gewesen sei als bisher angenommen. Die Rede ist von tausenden Firmen, unter anderem Microsoft, die die Geheimdienste mit Informationen versorgt hätten. Dabei gehe es jedoch nicht um Kundendaten, sondern vor allem um Software-Schwachstellen, die das Hacken fremder Rechner erleichtern (Quelle: Bloomberg, Heise).

**16. Juni 2013:** Einem Bericht des *Spiegel* zufolge will der Bundesnachrichtendienst (BND) trotz des Skandals um PRISM & Co die Internetüberwachung wesentlich ausweiten. Mit einem 100 Millionen Euro teuren „Technikaufwuchsprogramm“ sollen sowohl der MitarbeiterInnenstab, als auch die technischen Möglichkeiten hierfür erweitert werden. 5 Millionen Euro seien bereits durch die Bundesregierung freigegeben worden.

Gleichzeitig spricht sich der Präsident des Bundeskriminalamtes (BKA) weiterhin vehement für die Vorratsdatenspeicherung, also die generelle, verdachtsunabhängige Speicherung von NutzerInnendaten, aus (Quelle: Spiegel, Heise).

**19. Juni 2013:** Die *New York Times* rückt erneut die enge Verbindung zwischen US-Geheimdiensten und Internetunternehmen in den Fokus. So berichtet sie, dass Max Kelly, ehemals Sicherheitschef bei Facebook, inzwischen für die NSA arbeite.

Weiter legt die Zeitung dar, dass Skype 2008 mit der Entwicklung eines geheimen Programms *Project Chess* begonnen habe, das den Sicherheitsbehörden den Zugang zu der Kommunikation der NutzerInnen erleichtern solle. Dies steht der Behauptung der in den PRISM-Skandal verwickelten Unternehmen entgegen, den Behörden sei kein direkter Zugriff auf ihre Server gewährt worden (Quelle: New York Times, Heise).

**20. Juni 2013:** Einem Bericht der *Times of India* zufolge, hat Indien im April 2013 ein *Central Monitoring System* (CMS) eingeführt, das Sicherheits- und Steuerbehörden eine umfangreiche Überwachung von Internetkommunikation und Telefonanrufen ohne richterliche Genehmigung ermöglicht.

Der *Guardian* veröffentlicht am gleichen Tag zwei streng geheime Dokumente, welche die Zielgruppe der Überwachungsprogramme in den USA konkretisieren. Danach könne eine Person, von der „vernünftigerweise" angenommen werden kann, dass sie keinE US-StaatsbürgerIn ist und sich nicht in der USA aufhält, ohne richterliche Genehmigung von der NSA überwacht werden (Quelle: The Guardian, Heise).

**21. Juni 2013:** Edward Snowden gibt, wie der *Guardian* berichtet, belastende Informationen über den britischen Geheimdienst GCHQ preis. Dessen vor 18 Monaten in Betrieb genommenes Spionageprogramm *Tempora* sei sogar noch umfangreicher als PRISM. So fange der Geheimdienst in großem Stil Daten, wie E-Mails, Telefongespräche oder Einträge bei Facebook, über die transatlantischen Glasfaserkabel ab. Diese Daten würden auch der NSA zur Verfügung gestellt. In einem von Snowdem überlassenen Dokument rühme sich der Geheimdienst damit, den *„biggest internet access"* (dt.: umfassensten Internet-Zugang) in einer Verbindung der Geheimdienste der USA, Großbritanniens, Kanadas, Neuseelands und Australiens unter dem Namen *Five Eyes* zu haben und *„larger amounts of metadata than NSA"* (dt.: größere Mengen an Metadaten als die NSA) zu erfassen (Quelle: The Guardian, Heise).

**22. Juni 2013:** Die *New York Times* berichtet, dass von den USA am 14. Juni eine Anklage gegen Edward Snowden wegen Spionage und Diebstahl von Regierungseigentum beim Bundesgericht in Virginia eingereicht worden sei. Snowden hält sich zu diesem Zeitpunkt in Hongkong auf (Quelle: New York Times, Heise).

**23. Juni 2013:** Edward Snowden berichtet in einem Interview mit der *South China Morning Post*, dass die NSA in China Millionen Mobilfunknachrichten abgehört und Datenübertragungsleitungen der Pekinger Tsinghua-Universität überwacht habe. Weiter habe es Snowden zufolge 2009 Angriffe auf Computer von Pacnet, Betreiber eines der größten Glasfasernetze in der Asien-Pazifik-Region und verantwortlich für den Internetverkehr mit den USA, gegeben. Diese seien jedoch wieder eingestellt worden (Quelle: Heise).

**24. Juni 2013:** Die *Süddeutsche Zeitung* berichtet, dass im Rahmen des britischen Überwachungs-Programms *Tempora* auch das Glasfaserkabel TAT-14 ausgespäht worden sei, über das ein beträchtlicher Teil der Übersee-Kommunikation aus Deutschland laufe. Entsprechend sei auch der deutsche Telefon- und Internetverkehr Gegenstand der Überwachung gewesen. Die Bundesregierung und der Bundesnachrichtendienst (BND) bestreiten, davon Kenntnis gehabt zu haben (Quelle: Süddeutsche Zeitung, Heise).

**30. Juni 2013:** Aus neu ausgewerteten NSA-Dokumenten geht dem *Spiegel* zufolge hervor, dass die Bundesrepublik Deutschland in besonderem Maße von den US-Geheimdiensten überwacht wurde. Rund eine halbe Million Kommunikationsverbindungen seien betroffen. Auch die EU sei den Dokumenten zufolge Ziel der Spionageattacken geworden. In einem anderen Dokument, das dem *Guardian* vorliegt, werden 38 Botschaften und diplomatische Vertretungen aufgeführt, die von der massiven Ausspähung durch den US-Geheimdienst betroffen seien, unter ihnen auch die Botschaften Frankreichs, Italiens, Griechenlands, sowie Japans, Mexikos, Südkoreas, Indiens und der Türkei.

Die *Washington Post* veröffentlicht unterdessen neue Folien zum US-Überwachungsprogramm PRISM, aus denen hervorgeht, dass Daten von Microsoft, Google, Facebook, Youtube, Skype und anderen nicht einfach abgefragt, sondern in Echtzeit überwacht wurden. Mit einer beim Dienstanbieter installierten Filtersoftware seien Daten nach Schlüsselwörtern durchsucht worden, um die Datenströme auszudünnen (Quelle: Der Spiegel, Heise, The Guardian, Washington Post).

## Juli 2013

**2. Juli 2013:** Wie Experten aus dem Umfeld des deutschen Internet-Knotens De-CIX in Frankfurt am Main gegenüber *heise online* bestätigten, wird ein nicht näher definierter Teil der über den Knoten laufenden Daten an den BND und andere „Bedarfsträger" übermittelt. Dem Vorsitzenden der G10-Kommission Hans De With zufolge, der die Abhörtätigkeit wie auch die Justizministerien Sabine Leutheusser-Schnarrenberger bestätigte, bestünde eine Obergrenze von 20 Prozent des Datenverkehrs (Quelle: Heise).

**3. Juli 2013:** Über einen Bericht der *New York Times* wird bekannt, dass die US-Geheimdienste den gesamten Briefverkehr innerhalb des Landes registrieren lassen. Im Rahmen des Programms *Mail Isolation Control and Tracking* wurden den InformantInnen aus Justizministerium und FBI zufolge AbsenderInnen und EmpfängerInnen von rund 160 Milliarden Postsendungen abfotografiert und gespeichert (Quelle: New York Times, Heise).

**4. Juli 2013:** Wie die Tageszeitung *Le Monde* berichtet, überwacht und speichert der französische Auslandsnachrichtendienst

**Sara Stadler**

**Sara Stadler** studiert Informatik an der Hochschule Bremen und arbeitet in der FIfF-Geschäftsstelle.

*Direction Générale de la Sécurité Extérieure* (DGSE) die Kommunikation der französischen StaatsbürgerInnen seit Jahren. Zu den gespeicherten Daten, die bei Bedarf an andere Behörden weitergeleitet würden, gehörten die Metadaten aller Telefongespräche, Emails, SMS, sämtliche Aktivitäten bei Google, Facebook, Microsoft, Apple oder Yahoo (Quelle: Heise).

**6. Juli 2013:** Die *New York Times berichtet* von einer erheblichen Erweiterung der NSA-Befugnisse durch den *Foreign Intelligence Surveillance Court* (FISC). In geheimen Urteilen sei der NSA unter anderem gestattet worden, Daten etwa bei Verdacht auf einen Zusammenhang mit Cyberangriffen oder dem iranischen Atomwaffenprogramm auch ohne richterliche Genehmigung auszuspähen (Quelle: Heise, New York Times, Süddeutsche Zeitung).

**7. Juli 2013:** Einem Bericht der brasilianischen Zeitung *O Globo* zufolge wurden auch brasilianische BürgerInnen konstant durch die NSA überwacht. E-Mails und Telefongespräche seien hier in noch größerem Ausmaß abgefangen worden als in anderen lateinamerikanischen Ländern. Der Zeitung vorliegenden Dokumenten zufolge seien die Daten mit Hilfe des Programms *Fairview* ausgespäht worden, das gemeinsam mit einer großen US-Telekommunikationsfirma genutzt werde. Partnerschaften des Unternehmens mit anderen Firmen der Telekom-Branche, unter anderem in Brasilien, ermöglichten es der NSA schließlich auf die Daten in verschiedenen Ländern der Welt zuzugreifen. Inwieweit die Telekom-Firmen darüber informiert sind, sei nicht bekannt.

Der *Spiegel* veröffentlicht ein Interview mit Edward Snowden, in dem dieser erklärt, dass der BND und andere ausländische Geheimdienste, ebenso wie verschiedene Telekom-Firmen, eng mit der NSA zusammenarbeiten. So habe die NSA dem BND etwa Analyse-Werkzeuge zur Verfügung gestellt, mit denen der BND Datenströme aus fünf digitalen Knotenpunkten anzapfe und an die Zentrale *in* Pullach weiterleite. Ob auch die NSA selbst Internetknotenpunkte in Deutschland ausspioniere, sei nicht geklärt. Weiter ist die Rede von einem geheimen NSA-Abhörzentrum namens *Consolidated Intelligence Center* in Wiesbaden, dessen Neubau durch den BND genehmigt worden sei.

Nach dem Bekanntwerden der Post-Überwachung in den USA räumt auch die deutsche Post auf einen entsprechenden Tweet des CCC-Sprechers Frank Rieger hin ein, Adressdaten auf Briefen und Paketen automatisch zu scannen und zu speichern (Quelle: Heise, Spiegel).

**9. Juli 2013:** Anlässlich mehrerer Klagen vor dem EuGH gegen die Vorratsdatenspeicherung verteidigen VertreterInnen der EU-Gremien und -Mitgliedsstaaten die Richtlinie zur verdachtsunabhängigen Speicherung aller Verbindungsdaten in einer Anhörung.

Das Urteil zu dem nun beendeten Verfahren wird in etwa 6 Monaten erwartet. Das Gutachten des Generalanwalts soll am 9. November 2013 veröffentlicht werden (Quelle: Heise, Netzpolitik.org).

**12. Juli 2013:** Einem Bericht des *Guardian* zufolge hat Microsoft die NSA darin unterstützt, auch verschlüsselte NutzerInnendaten auszuspähen. So sei etwa vor dem Start des Mail-Portals *Outlook.com* sichergestellt worden, dass die NSA auf Daten zugreifen könne, bevor sie verschlüsselt werden. Auch an der Erleichterung des Zugangs zu Daten in dem Online-Speicherdienst SkyDrive und der Kommunikation via Skype sei gemeinsam gearbeitet worden (Quelle: The Guardian, Heise).

**15. Juli 2013:** Nachdem bereits in der vergangenen Woche Edward Snowden im *Spiegel* von einer umfangreichen Zusammenarbeit zwischen NSA und BND berichtet hatte, schaltet sich nun auch die *Bild* in die Debatte ein, die anführt, aus US-Regierungskreisen weitere Details dieser Zusammenarbeit erfahren zu haben. Der BND habe über Jahre von der umfangreichen Überwachung durch die NSA profitiert, etwa im Falle einer Entführung deutscher StaatsbürgerInnen. Es sei, so folgert die Zeitung, daher nur naheliegend, dass er über die umfangreiche Überwachung und Datensammlung durch den US-amerikanischen Geheimdienst informiert gewesen sei. Auch zieht die *Bild* die Behauptung des jüngst von einer umstrittenen USA-Reise zurückgekehrten Bundesinnenministers Hans-Peter Friedrich in Zweifel, dass die Überwachungsprogramme Daten gezielt nach Inhalten scannen würden – die Kommunikation würde vielmehr flächendeckend gespeichert (Quelle: Heise, Bild.de).

**17. Juli 2013:** Auch die Bundeswehr arbeite, so die *Bild*, mit der NSA zusammen. Einem geheimen Nato-Dokument zu Folge sei sie seit Herbst 2011 über PRISM informiert. Die Vorwürfe würden durch das Auftauchen einer zweiten Datenbank mit dem Namen PRISM erhärtet, die im Kommandobereich der Bundeswehr in Afghanistan zur Überwachung von Terrorverdächtigen genutzt worden sei. Ein Zusammenhang zwischen den beiden Programmen weisen SprecherInnen der Bundesregierung und des BND zurück. Bei PRISM II handele es sich um ein nicht geheimes Isaf-Programm zur Radaraufklärung und Luftüberwachung. Dies steht Berichten der *Bild* entgegen, denen zufolge beide Programme auf dieselben NSA-Datenbanken zugreifen würden.

Das ARD-Magazin FAKT berichtet, dass es sich bei der vom BND verwendeten Software der Boeing-Tochter Naurus um PRISM-Software handele (Quelle: Heise, Bild.de).

**18. Juli 2013:** Die *Mitteldeutsche Zeitung Halle* berichtet, dass in Wiesbaden-Erbenheim aktuell ein Zentrum für militärische Aufklärung, *Consolidated Intelligence Center*, durch die US-amerikanischen Streitkräfte gebaut werde. Der Zeitung zufolge handele es sich dabei um ein Abhörzentrum der NSA (Quelle: Heise).

**20. Juli 2013:** Wie der *Spiegel* berichtet, nutzen deutsche Geheimdienste die Ausspähdatenbanken der NSA stärker als sie zugeben wollen. Geheimen Unterlagen zufolge setzten BND und BfV eine NSA-Software namens *XKeyscore* ein, die quasi eine „digitale Totalüberwachung" ermögliche. Von dem Programm sei ein Teil der monatlich bis zu 500 Millionen Datensätze aus Deutschland, unter anderem Telefonnummern, E-Mail-Adressen und Zeitstempel von Nutzeraktivitäten, erfasst, auf die auch die NSA Zugriff habe.

In den USA wird die die Genehmigung zum Sammeln von Telefonverbindungsdaten durch die US-Behörden derweil verlängert (Quelle: Heise, Spiegel).

**26. Juli 2013:** Die Gewerkschaft der Polizei spricht sich trotz der jüngsten Überwachungsskandale für die Vorratsdatenspeicherung aus.

US-Medien berichten, dass Regierungsbehörden von Dienstanbietern im Internet die Herausgabe der geheimen Schlüssel ihrer Server mit SSL-Verschlüsselung verlangten. Die Konzerne würden die Herausgabe der *Master-Keys,* mit denen die gesamte Kommunikation des Servers auch im Nachhinein entschlüsselt werden könne, jedoch bislang verweigern (Quelle: Heise).

**27. Juli 2013:** Der frühere Bundesinnenminister Otto Schily (SPD) räumt in einem Interview mit dem *Spiegel* ein, dass PRISM im Grunde nichts anderes sei als die Vorratsdatenspeicherung (Quelle: Spiegel).

**31. Juli 2013:** Der *Guardian* veröffentlicht weitere Details zum NSA-Programm *XKeyscore*. Folien aus dem Fundus Edward Snowdens zufolge ermögliche das Programm eine nahezu vollständige Überwachung der Internetnutzung (E-Mails, Chats, Browser-Chroniken, Aktivitäten auf Facebook) sowie die Möglichkeit einer vollständigen Überwachung jeder beliebigen Person bis hin zum US-Präsidenten (Quelle: Heise, The Guardian, Spiegel).

## August 2013

**1. August 2013:** Unter Berufung auf weitere von Edward Snowden ausgehändigte Dokumente berichtet der *Guardian* von einer umfangreichen Finanzierung des britischen Geheimdienstes GCHQ durch die NSA. Mindestens 100 Millionen Pfund seien in der vergangenen drei Jahren geflossen. Dass dafür auch US-BürgerInnen vom GCHQ überwacht worden seien, weise die NSA zurück. Weitere aus den Dokumenten gewonnene Erkenntnisse beziehen sich auf die Telefonüberwachung, in die der GCHQ massiv investiert habe sowie den GCHQ-Standort in der Küstenstadt Bude, an dem der Geheimdienst Berichten der *Süddeutschen Zeitung* und des *NDR* zufolge Daten aus dem Glasfaserkabel TAT-14 abgefangen habe. Für die Sanierung diese Standortes habe Großbritannien 15,5 Millionen Pfund von der NSA erhalten (Quelle: Heise, The Guardian).

**2. August 2013:** Die *Süddeutsche Zeitung* und der *NDR* veröffentlichen die Namen derjenigen Telekom-Firmen, die dem britischen Nachrichtendienst GCHQ bei der Internetüberwachung behilflich waren. Genannt werden unter anderem die international tätigen Unternehmen British Telecom, Verizon und Vodafone.

Aus Neuseeland werden einstweilen Pläne bekannt, die Befugnisse des Geheimdienstes GSCB auszuweiten und den bestehenden Apparat zur Überwachung von Telefon und Internetkommunikation fortan auch für die Überwachung von StaatsbürgerInnen und Personen mit einem dauerhaften Aufenthaltsstatus zu nutzen (Quelle: Süddeutsche Zeitung, NDR, Heise).

**3. August 2013:** *CNET News* berichtet, dass die US-Regierung und das FBI NetzbetreiberInnen zur Installation von Port Readern zwängen (Quelle: Heise, CNET).

**4. August 2013:** Aus einem Bericht des *Spiegel* geht hervor, dass der BND Daten aus der eigenen Fernmeldeaufklärung an die NSA übermittele. Hinter einer der Datensammelstellen, über die die NSA im Dezember vergangenen Jahres rund 500 Millionen Metadaten aus der Bundesrepublik erfasst habe, verberge sich möglicherweise der BND-Standort Bad Aibling. Auch ansonsten sei die Zusammenarbeit zwischen BND und NSA enger als bisher angenommen. Die Zeitschrift berichtet von Schulungen – unter anderem im Umgang mit dem Programm *XKeyscore* – die VertreterInnen des BND und des Bundesamtes für Verfassungsschutz von NSA-SpezialistInnen erhalten hätten (Quelle: Heise, Spiegel).

**5. August 2013:** Die New York Times berichtet, dass die NSA Informationen an Ermittlungsbehörden weiterleite, obwohl deren Einsatz gegen in den USA lebende StaatsbürgerInnen nicht ohne weiteres möglich sein sollte (Quelle: Heise, New York Times).

**7. August 2013:** Der ehemalige NSA-Direktor Michael Hayden bestätigt in einem Interview mit *CNN* alle aus den von Snowden veröffentlichten Folien hervorgehenden Daten über das Programm *XKeyscore* und bewertet diese als positive Errungenschaft.

Die *Tagesschau* berichtet einstweilen unter Berufung auf den stellvertretenden Sprecher der Bundesregierung Georg Streiter, dass die Zusammenarbeit zwischen BND und NSA im April 2002 von der rot-grünen Bundesregierung vertraglich festgelegt und von dem damaligen Kanzleramtsminister Frank-Walter Steinmeier (SPD) abgesegnet worden sei (Quelle: Heise, Tagesschau.de).

**8. August 2013:** Die EU-Kommission legt ein Papier zum *Nachweis der Erforderlichkeit der Vorratsdatenspeicherung* vor.

Die *New York Times* fördert unterdessen neue Informationen über das Ausmaß der Online-Überwachung in den USA durch die NSA zutage. So sei nicht, wie von offizieller Seite stets betont wurde, „lediglich" die Kommunikation mit Nicht-US-BürgerInnen ohne Genehmigung überwacht, sondern jegliche Kommunikation nach Verweisen auf überwachte Personen gescannt worden (Quelle: Heise, New York Times).

**9. August 2013:** Die US-amerikanischen E-Mail-Anbieter *Lavabit* und *Silent Circle* machen dicht. Beide hatten ihren NutzerInnen verschlüsselte Kommunikation angeboten. Auch wenn die Anbieter die Gründe für das Aus nicht nennen (dürfen), legen die Aussagen des Lavabit-Chefs Ladar Levison nahe, dass sie, zumindest in diesem Fall, etwas mit der Weigerung zu tun hatten, den US-Behörden Zugriff auf Kommunikationsdaten zu ermöglichen (Quelle: Heise).

**16. August 2013:** Nach Berichten der *Washington Post* hat die NSA entgegen anderslautender Beteuerungen in erheblichem Umfang illegal US-BürgerInnen überwacht. Ein geheimer Bericht, der den Großraum Washington D.C. abdeckt, berichte von 2776 „Vorfällen" über einen Zeitraum von 12 Monaten. Nach Angaben der NSA sei die Überwachung „versehentlich" aufgrund eines Programmierfehlers erfolgt. Offenbar wurde bei der Telefonüberwachung die Vorwahl von Washington D.C. (202) mit der Ländervorwahl von Ägypten (20) verwechselt (Quelle: Washington Post, Spiegel).

# The Washington Statement

## In Support of Data Protection

*Privacy advocates from the United States, Canada and Europe have gathered in Washington, D.C. for the conference on Computers, Freedom and Privacy (CFP). In light of recent revelations about the collection of personal data from Internet companies by the US government and other dragnet surveillance techniques that impact the rights of Internet users, the North American and European privacy advocates issued the following consensus statement.*

Privacy is a basic human right set out in Articles 17 and 19 of the International Covenant on Civil and Political Rights (ICCPR) and Article 12 of the Universal Declaration of Human Rights (UDHR).

**We, the undersigned civil society groups from North America and Europe, are outraged because:**

- Under PRISM and related surveillance programs, the US government is collecting personal data that individuals have given to companies such as Google or Facebook. These data were given freely or inadvertently, trusting that they would only be used for stated commercial purposes and not secretly shared with governments in order to monitor innocent people worldwide;
- At the same time, the US companies and the US administration are lobbying in Europe against European data protection law at a time when the world needs strong privacy protections most;
- EU citizens currently have significant privacy rights that US citizens do not have – thereby creating a level of trust in the public and private sectors in the European Union that is not available to US citizens.

Currently, the European Union is reforming its general data protection framework for the private sector. **We therefore call on EU policy makers:**

- to oppose corporate lobbying and to prevent the erosion of privacy protections in the European Union;
- to set a high standard and ensure that EU data protection law sets a global standard for privacy;
- to ensure specific rights of individuals are being preserved, such as explicit consent to personal data processing, the right to access, rectification and certain rights to erasure that are in the existing European legal framework;
- to ensure basic principles that would help protect citizens against untargeted and disproportionate surveillance measures, such as data minimization, purpose limitation, limited storage periods and notification procedures;
- to ensure that personal data processed in the EU is not transferred to third country authorities without a determination that there are adequate privacy safeguards.

**We further call on US policy makers:**

- to repeal provisions of the PATRIOT Act and the FISA Amendments Act that permit unlawful surveillance of users of Internet services;
- to enact the "Consumer Privacy Bill of Rights" into law;
- to cease the US opposition to EU efforts to strengthen data protection;
- to support ratification of Council of Europe Convention 108.

**Our common future, on both sides of the Atlantic, needs privacy and a strong European law. We call on European policy makers to defend this human right now, as an essential prerequisite for preserving privacy, freedom of thought and of expression in vibrant democracies.**

*June 24, 2013*

**Promoters:** *Access, American Civil Liberties Union (ACLU), Bits of Freedom (BoF), British Columbia Civil Liberties Association (BCCLA), Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), Consumer Federation of America (CFA), Consumer Action, Center for Digital Democracy (CDD), Defending Dissent Foundation, Electronic Privacy Information Center (EPIC), European Digital Rights (EDRi), Friends of Privacy USA, Privacy International, Privacy Rights Clearinghouse*

*Das FIfF hat sich der Erklärung angeschlossen.*

**Oliver Degner**

# Die NSA, die Bespitzelung und die Ethik

*Schwarzer Anzug. Sonnenbrille. Auf das Ziel lauernd. Kompetent. Zu allem bereit. Das sind wahrscheinlich die ersten Assoziationen, die uns einfallen, wenn wir an CIA und FBI denken. Die amerikanische Filmindustrie und das Außenmarketing entsprechender Behörden haben das kulturelle und psychologische Bild des Geheimagenten bzw. des „Special Agent" stark geprägt. In unserer Vorstellung sind es nicht nur Bürger, die einen nicht alltäglichen Beruf ausüben, sondern Menschen, die durch Schläue und mit Hilfe technischer Gadgets Terroranschläge oder, wie in dem Film „Stirb Langsam 4.0", einen nationalen Angriff auf die Energie- und IT-Infrastruktur verhindern. Sie kämpfen dabei häufig unter schwersten Bedingungen für Freiheit und Demokratie, aber auch für die Abwehr von Gefahrenquellen aus dem In- und Ausland. Waren FBI und CIA bereits gut bekannt, so ist die NSA weitaus seltener in öffentliche Erscheinung getreten.*



Die spannende Frage: Ist die Realität tatsächlich nahe an der Eigendarstellung der Geheimdienste oder passt die Orwell'sche Zeichnung der Welt weitaus besser für das Jahr 2013? Ist die NSA also im Namen der Bürger und zum allgemeinen Schutze des Staates im Einsatz, oder ist bereits jeder Bürger selbst zum potentiellen- und unkontrollierbaren Ziel geworden? Geht es noch um den Schutz der Demokratie, wenn ich dafür das Opfer verlangen muss, jeden Bürger überwachen zu dürfen? Oder hält die NSA tatsächlich die Fäden in der Hand und bewahrt uns im Geheimen vor dem „Krieg eines Jeden gegen Jeden", wie Thomas Hobbes es ausdrückte? Um diese Fragen beantworten und auch eine mögliche Legitimität prüfen zu können, ist ein Blick auf die eigene Aufgabenbeschreibung der NSA nötig.

## Die Aufgabe der NSA

In der Aufgabenbeschreibung[1] heißt es, dass es Ziel ist, Terroristen und Schaden bringende Organisationen im Rahmen der amerikanischen Gesetzgebung zu besiegen (*to defeat*) und dabei in Einklang von Privatheit und Bürgerrechten zu handeln. Weiter heißt es in der Executive Order 12333, dass Daten und Informationen zum Schutze der nationalen Interessen gesammelt werden und die NSA als *National Manager* für die nationalen Sicherheitssysteme agiert und auch entsprechende Regularien zur Weitergabe, Übertragung sowie Verwendung von Daten entwirft und überwacht.

Im Gegensatz zu anderen Geheimdienstbehörden wie FBI und CIA liegt der Fokus der NSA auf der Informationsbeschaffung und -verwendung. Ein Tätigkeitsschwerpunkt im IT-Bereich legt eine informationsethische Analyse der Tätigkeiten nahe. Dies in Einklang zu bringen mit Bürgerrechten und der Wahrung der Privatheit ist ein hehres Ziel. Zur seiner Überprüfung ist die Frage wichtig, warum oder ob wir überhaupt Nachrichtendienste brauchen.

## Warum wir Nachrichtendienste wie die NSA benötigen

Waren die Unternehmensnetzwerke bis etwa 1990 noch isoliert von der Außenwelt, und wurden die häufigsten IT-Sicherheitsfragen nur in Bezug auf Ausfallsicherheit und Verfügbarkeit von Systemen gestellt, so wurden bis 1995 erste Rechner mit niedrigen Bandbreiten ans Internet angeschlossen[2]. Die Kommunikation veränderte sich damit deutlich. Aktuell werden die „internen Netzwerke [...] von eigenen und externen Mitarbeitern sowohl von intern wie von extern und sowohl mit firmeneigenen wie mit fremden PCs […] verbunden."[3] Das Schad- und Risikopotential erhöhte sich drastisch. Dabei sind sowohl Mensch als auch Maschine potentielle Gefahrenverursacher. Würmer, Viren, Trojaner wie *Sasser.ftp* oder *Conficker* wurden bedrohlich. Dazu kam der psychologische Faktor durch menschliche Fehler wie unsichere Passwortvergabe, Social Engineering und Ähnliches. Neue Verwundbarkeiten eröffnen eine neue Sphäre, in der zwischenstaatliche Konflikte ausgetragen werden: feindliche Aktionen im Cyberraum, von Spionage über Sabotage bis hin zum Cyberangriff mit drastischen Folgen für Menschen und Einrichtungen.

Unsere Industriestaaten sind in einer Machtspirale gefangen. Fehlende oder mangelnde Investition in die Entwicklung von Cyberwarfare-Technologie setzt die staatliche IT-Infrastruktur einer potentiellen Gefahr aus. Es entsteht Druck von außen, in entsprechende Forschung zu investieren mit dem Anreiz, selbst größtmöglichen Schutz und gleichzeitig größtmögliches Angriffspotential zu besitzen. Rüstet ein Staat seine Cyberspionage auf, müssen andere Nationen nachziehen, um sich zu schützen und um informationstechnische Gegendruckmittel zu bieten. Dadurch entsteht, was eigentlich verhindert werden sollte, ein ‚kalter Krieg' im Internet. Wie bei der Abrüstung von Atomwaffen würde es allein helfen, gemeinschaftlich auch in diesem Sektor die Investitionen zurückzufahren – Zukunftsmusik …

Schon 2001 kündigte der israelische Präsident Sharon an, notfalls einen Krieg im Internet gegen die Palästinenser zu führen[4]. Die Entwicklung ist weiter gegangen. 2008 führte das Bundesamt für Verfassungsschutz in seinem Entwicklungsbericht aus, dass internetbasierte Angriffe auf die Computersysteme von Wirtschaft und Regierung zunehmen würden und Deutschland ein bedeutendes Aufklärungsziel für andere Staaten darstelle.[5] Sicherheitsfirmen wie *G Data Software AG* gehen zwar nicht von einem regelrechten Cyberwarfare aus, prognostizieren aber, dass zielgerichtete Attacken zunehmen werden.[6] Das *Cyber Security Summit*[7], eine Sicherheitskonferenz mit Sitz in München, initiiert durch die Telekom und Topmanager deutscher Konzerne und Politiker, beweist, dass das Gefahrenpotential ernst genommen wird. Als Konsequenz dieser Entwicklung wird es zur Aufgabe des Staates, seine Bürger und Institutionen zu schützen. Die Frage ist lediglich, welche Mittel und welches Ausmaß legitim sind. Wenn jedoch Staaten nicht mehr andere Staaten ausspionieren, sondern ihre Geheimdienste die eigenen Bürger, muss zunächst geklärt werden, worin und wie sich informationstechnisch der private Mensch von einer zu schützenden Institution unterscheidet.

## Sind Bürgerinnen und Bürger wirklich IT-mündig?

Wie steht es heute um die oft geforderte Medienkompetenz unserer Bürgerinnen und Bürger? Und um den Weg aus der informationstechnischen Unmündigkeit? Können wir uns wenigstens ansatzweise privat schützen? Bei der Studie des *medienpädagogischen Forschungsverbandes Südwest* (2012)[8] wurde ermittelt, dass Soziale Netze, hier speziell Facebook, von 77 % der Jugendlichen im Alter von 14-15 Jahren genutzt werden, bei den über 16-Jährigen sogar von bis zu 88 %. Wie steht es dabei um die Aktivierung der Privacy-Funktion? Überraschend gut, denn 87 % der Mädchen und 79 % der Jungen nutzen die Funktion. Bei der Frage nach der gefühlten Datensicherheit gaben über 50 % der Befragten an, dass sie ihre Daten als sicher bis sehr sicher einstuften – da verwundert es dann nicht, dass über 73 % der Befragten Informationen über ihre Hobbies veröffentlichen oder 65 % eigene Filme oder Fotos hochladen. In einer in Auftrag gegebenen Studie der *Landesanstalt für Medien Nordrhein-Westfalen* wurde festgestellt, dass „die Sorge um die eigene Privatsphäre das Verhalten nur bedingt beeinflusst. Trotz ausgeprägter Sorge um die Privatsphäre wird auf sozialen Netzwerkplattformen viel Privates „offenbart"[9]. Dies ist insbesondere problematisch, wenn Videos und Fotos von und mit anderen Personen hochgeladen werden. Durchschnittlich besitzt jeder Facebook-Nutzer nach der Stephen-Wolfram-Studie 342 ‚Freunde'[10] – dies bei über 1 Milliarde Nutzern[11], die Informationen über sich und ihre ‚Freunde' verbreiten können, ob gewollt oder ungewollt. Die Ergebnisse zeigen, dass die Diskussion weitergehen muss, um dieses Gefahrenpotential klar zu machen. Denn dass nicht nur die Freunde oder Arbeitskollegen auf unsere Informationen im Netz zugreifen, ist spätestens seit dem NSA-Skandal evident. Als mündige Bürger sollten wir um unseren eigenen Schutz bemüht sein. Aber: In einer Bitkom-Studie[12] von 2010 gaben 21 % der Befragten an, kein Virenschutzprogramm zu nutzen, 33 % nutzten keine Firewall und nur 19 % nutzten Verschlüsselungssoftware. Dementsprechend gingen 98 % der Befragten davon aus, dass ihre persönlichen Daten nicht ausgespäht oder illegal genutzt wurden.

In Deutschland und anderen Ländern gibt es nun einen Aufschrei über die Bespitzelung durch die NSA. Er ist berechtigt. Aber es muss angesichts der Faktenlage auch klar sein, dass wir zwar fordern können, dass unsere Daten geschützt werden sollen und wir nicht ausgespäht werden möchten, dass es jedoch ebenfalls unsere Eigenverantwortung ist, darüber zu reflektieren, wie wir selbst mit unseren Daten umgehen. Empörung allein schafft keine Abhilfe. Die kann nur durch Handeln erreicht werden. Und da sind Staat und Bürger gleichermaßen in der Pflicht. Dennoch bleibt, neben Appellen an Staat und Bürger, die entscheidende Frage, ob die Handlungen der NSA informationsethisch legitim sind.

## Die NSA, die Bespitzelung und die Ethik

Sich gegen Terrorismus und für ein sicheres Leben der Bürgerinnen und Bürger einzusetzen, ist fraglos ein hehres Ziel. Die NSA hat sich in ihrer Handlungsabsicht dabei die Selbstbeschränkung auferlegt, die Privatheit zu schützen und im Namen der Gesetze zu handeln. Auch dies ist anzuerkennen. Gesetze sind und bleiben jedoch ein menschliches Konstrukt. Wenn sich Situationen ändern, können durch dieselben Gesetze plötzlich Handlungen legitimiert werden, die vorher nicht denkbar waren. Wer hätte noch vor wenigen Jahren prognostiziert, dass es eine Vorratsdatenspeicherung, eine Bestandsdatenauskunft oder eine Einschränkung der Netzfreiheit geben könnte? Durch Gesetze können Bürgerrechte gestärkt werden, z. B. durch die Ermöglichung des Frauenwahlrechts, die Gleichbehandlung von Patchwork- und Regenbogenfamilien. Im Fall von PRISM wurde informationsethisch der umgekehrte Weg begangen. Hier werden Bürgerrechte abgebaut.

Nach Kant[13] kommt es bei einer ethischen Bemessung nicht darauf an, ob der Gegenstand der Willensbildung an sich gut ist, sondern ob diese aus Pflicht und Achtung vor dem Sittengesetz geschieht. Aus dieser Sicht ist es schwer vorstellbar, dass wir uns als Individuen wünschen könnten, dass unsere eigenen Daten auch ohne Verdachtsmoment aufgezeichnet, analysiert, interpretiert, verwahrt und weiterverteilt werden. Das Handlungsmotiv der NSA wäre, positiv formuliert, zwar „Schutz der Bürgerinnen und Bürger". Auf Seiten der Betroffenen – das sind ja leider fast alle Bürgerinnen und Bürger – wird aber empfunden, dass es sich eher um eine Massenbespitzelung handelt, dass tief greifende Eingriffe in unsere Gedanken- und Gefühlswelt vorgenommen werden und dass wir unser Recht auf freien Informationsfluss und weiterführend auch auf unsere Meinungsfreiheit zunehmend verlieren. Dies hat nicht mehr viel mit Schutz der Bevölkerung gemein. Denn in einem durch Geheimdienste kontrollierten Netz muss damit gerechnet werden, dass unsere Ängste berechtigt sind und vieles, z. B. Staatskritik, zu Repressalien führen kann. Wenn Geheimdienste die volle Kontrolle über viele Nutzerdaten (Mail, Facebook, Telefon, Suchanfragen)[14] erhalten und eine systematische Massenüberwachung stattfindet, dann ist unsere Demokratie auf einem gefährlichen Weg. Der hieße, die Demokratie zu schützen, indem wir sie abschaffen.

Die NSA führt bei der Überprüfung von Personen zwei bis drei so genannte *Hop Queries* durch.[15] Beim Vorliegen eines Verdachts kann dies dazu führen, dass Bekannte von Bekannten von Bekannten überprüft werden.[14] Legt man die durchschnittlich 342 Freunde der Wolfram-Studie zu Grunde, sind dies $342^3$, also über 40 Millionen Überprüfungen ohne konkrete Verdachtsmomente. Was durch informationelle Missverständnisse oder auch nur durch mögliche *Query Hops* passieren kann, zeigt der Fall des Journalisten Mathias Priebe. Dieser steht nach eigenen Auskünften in Amerika derzeit unter Terrorverdacht und stellt einen so genannten ‚Geheimen Vorgang' dar[16]. Grund dafür könnten nach seiner Mutmaßung Missverständnisse sein: Freundschaft zu einem palästinensischen Kameramann, Zeitsoldat bei der NVA, Urlaub in Aserbaidschan und ein Geschäftskontakt zu einer Firma für Bohr- und Sprengtechnik. Ob dies tatsächlich die Gründe sind, werden nur die Geheimdienste wissen. Aber alleine, dass das eine realistische Vorstellung ist, ist erschreckend und beunruhigend. Genau wie die Tatsache, dass der Griesheimer Daniel Bangert lediglich bei Facebook einen scherzhaften Spaziergang zum Dagger-Komplex der NSA plante und dass kurz nach dieser Ankündigung die deutsche Polizei, eingeschaltet durch die US-Militärpolizei, und der Staatsschutz, bei ihm zu Hause vorbeischauten.[17]

Erfreulich, dass die Staatsorgane in einem konkreten Verdachtsmoment eingreifen, aber war dieser hier gegeben? Es handelte sich nicht um eine Terrordrohung oder um eine grobe Störung

der öffentlichen Ordnung. Der Hinweis der Polizei, diese Veranstaltung als Versammlung anzumelden, falls sie größer würde, ist legitim. Ob aber die Einschaltung der US-Militärpolizei und des Staatsschutzes dafür notwendig waren, ist schwer zu rechtfertigen. Beunruhigend ist zudem, dass die US-Militärpolizei von diesem Spaziergang wusste. Denn: es handelte sich um einen kleinen Interessentenkreis, nicht um eine Massendemonstration. Die Überwachung funktioniert also. Leider nur an der falschen Stelle.

Die Begründung, dass die umfassende Überwachung aller Verdächtigen, also **aller** Bürgerinnen und Bürger dadurch legitimiert wird, dass Terroranschläge „wahrscheinlich" verhindert werden könnten ist fragil. Eine ähnliche Diskussion gab es bereits in Bezug auf die flächendeckende Videoüberwachung. Durch die Überwachung von Tankstellen, Bahnhöfen, Toiletten und öffentlichen Plätzen sollte damit eine erhöhte Sicherheit erreicht werden. Die Kriminalitätsstatistiken sprechen gegen die These, dass eine umfassende Überwachung zu einer umfassenden Sicherheit führt[18]. Auch in Bezug auf die NSA greift die Argumentation „Datenschutz ist Terrorismusschutz" nicht. In einer stichhaltigen Argumentation führt Schaar (2007, S. 25-30) aus, dass nach einer Studie von 2006 durch *Privacy International* Deutschland in Bezug auf den Datenschutz den Spitzenplatz einnimmt[19]. Die USA, Großbritannien und Russland schneiden bei der Analyse deutlich schlechter ab. Schaar folgert, dass das Ranking genau entgegengesetzt sein müsste, wenn Datenschutz die Kriminalitätsbekämpfung behindern würde. Denn die Kriminalitätsrate ist in Deutschland trotz des stärkeren deutschen Datenschutzgesetzes deutlich niedriger als in beispielsweise in den USA. Datenschutz und Privatheit sind nicht das Rüstzeug, mit dem sich Täter oder Terroristen schützen. Sie sind das Handwerkszeug, um unser Grundrecht auf freie Persönlichkeitsentfaltung und unser Recht auf Privatheit zu schützen. „Das entscheidende Kriterium für die erfolgreiche Regulierung der Privatsphäre ist [...] auf der einen Seite die Offenheit und die Preisgabe von Informationen an andere, und zum anderen der gezielte Rückzug und die Einsamkeit."[20]

Es gibt nun zwei Perspektiven: die aktuelle Rechtsprechung und den durch Geburt verliehenen Anspruch auf menschliche Grundrechte, unabhängig von vorhandenen Rechtslagen. Aus Sicht der aktuellen Gesetzgebung handelt es sich bei PRISM um einen Rechtsverstoß. PRISM verstößt gegen das Prinzip vom Schutz des Privatlebens – nach Landesdatenschützer Weichert insbesondere gegen

- die allgemeine Erklärung der Menschenrechte von 1948 (Artikel 12),
- den Internationalen Pakt über bürgerliche und politische Rechte von 1966 (Artikel 17),
- die Europäische Menschenrechtskonvention von 1950 (Artikel 8),
- das Grundrecht auf Datenschutz beziehungsweise auf informationelle Selbstbestimmung, wie es in der europäischen Grundrechte-Charta (Artikel 7, 8) und im deutschen Grundgesetz (Artikel 2 Absatz 1 und Artikel 1 Abs. 1) gewährleistet wird.

*„Die bekannt gewordenen Praktiken von US-Sicherheitsbehörden missachten zugleich die ‚vernünftigen Erwartungen an Privatheit' (reasonable expectations of privacy), wie sie vom Supreme Court aus der US-Verfassung abgeleitet werden."*[21]

Selbst ohne eine detaillierte Betrachtung der einzelnen Chartas und Erklärungen oder des deutschen Grundgesetzes wird deutlich, dass die Maßnahmen durch die NSA auf dem Papier und vor der Judikative keinen Bestand haben können und auch nicht dürfen. Denn zum Abbau von Grundrechten haben maßgeblich zwei Umstände beigetragen[22]: die „rasanten Fortschritte der technischen Möglichkeiten von Überwachung und Kontrolle", sowie der tendenzielle „Wandel im Staatsverständnis vom Rechtsstaat zum Präventionsstaat." Die rechtsstaatliche Einschreitschwelle solle nach diesem Konzept daher so niedrig wie nötig, aber so hoch wie möglich gelegt werden. Zudem müsse ein hinreichendes Wissen über die Sachlage vorliegen, bevor der Staat aktiv würde. Weiterhin dürfe sich die Handlung prinzipiell nur gegen die Personen richten, die für Gefahren oder Schäden verantwortlich seien[23]. Die Grundsätze einer Präventionsgesellschaft mit weit reichender Überwachung der BürgerInnen, mit Mutmaßungen als Handlungsgrundlage und einer Einschreitschwelle „so niedrig wie möglich" stehen dem liberalen Rechtsstaat konträr entgegen[24].

Die Massensammlung und -verarbeitung von Daten durch die NSA und das passive Zusehen der Bundesregierungen entfernt uns derzeit vom liberalen Rechtsstaat und führt uns zu einer unkontrollierten Orwellschen Präventionsgesellschaft, in der jede Information gesammelt, ausgewertet, verteilt und korreliert wird. So wird unser Leben systematisch katalogisiert, schematisiert und psychologisiert. In dieser Datenwelt ist es bereits ausreichend, dass ein Bekannter eine missverständliche Information in einem Sozialen Netzwerk kund gibt, um selbst ins Fadenkreuz der Ermittlungen zu geraten. In einer derartigen Daten-Welt werden Misstrauen, Beobachtung und auch Wut die Werte unserer Demokratie, des Vertrauens und des friedlichen Miteinanders zerstören. Die Informationstechnologie hat die vorrangige Aufgabe, allen Menschen in der Gesellschaft gleichermaßen zu dienen, „ihnen die Arbeit [zu] erleichtern, ihre Lebensumstände [zu] verbessern und [dabei zu] helfen, Schaden von ihnen abzuwenden"[25]. Hierhin müssen wir als Gesellschaft gelangen.

**Oliver Degner**

**Oliver Degner** hat an der Universität Duisburg-Essen Wirtschaftsinformatik mit dem Schwerpunkt IT-Management studiert. Er ist Begründer der konsensbasierten Wirtschaftsinformatik.

Technik ist so gut, wie ihr Verwendungszweck und die Absichten der handelnden Akteure. Nur in der Verwendung der Technik kann ihr Nutzen positiv sein und den Menschen helfen – oder ihnen schaden. Heute möchte kaum einer auf die Errungenschaften der modernen IT mit ihren Navigationsgeräten, Smartphones, Hochleistungsrechnern zur Analyse medizinischer Daten oder der bequemen Kommunikation über Landesgrenzen hinweg verzichten. Je komplexer die Systeme aber werden, umso vielfältiger werden sie Hintertüren für Hacker, Saboteure, Datensammler und wissenshungrige Dienste bieten. Um die Vorteile der Informationstechnologie freizügig nutzen zu können, brauchen wir ein staatliches Schutzsystem. Dieses muss jedoch kontrollierbar bleiben. Es darf nicht jeden Menschen als potentiellen Täter einstufen, alle seine Handlungen überwachen und schon bei Abweichungen einer (zweifelhaften?) Norm Alarm schlagen. Grenzen müssen gesteckt werden.

„*Liberté, Égalité, Fraternité*“, die Parole der französischen Revolution, ist dabei eine gute Leitlinie:

- Freiheit in der Datenkommunikation und in unserem Handeln,
- Gleichheit durch ein internationales Datenschutzrecht, welches allen umfassende informationelle Grundrechte einräumt, und ein
- „brüderlicher“ konsensbasierter Umgang in einer gesamtgesellschaftlichen Diskussion.

Fest steht, in einer technologisierten Welt, die von IT-Systemen durchdrungen ist, muss ein ausreichender Schutz von Nutzerinnen und Nutzern und Systemen gewährleistet werden. Man bedenke nur die nicht absehbaren Folgen eines totalen Stromausfalles, die Abschaltung der nationalen Kommunikationsnetze, die Sabotage lebenswichtiger Einrichtungen wie z. B. Versorgungsnetze oder staatliche Behörden. Klar ist auch, dass der Versuch, sich vor jeglicher potenziellen Gefahr schützen zu lassen, dazu führen würde, dass wir unsere Freiheit, Privatheit und Selbstbestimmung verlören. Datenschutz ist weder Täterschutz, noch ein notwendiges Übel. Datenschutz schützt uns Menschen hinter den Maschinen vor Übergriffen auf unser Grundrecht der informationellen Selbstbestimmung, stärkt unsere Bürgerrechte und gibt uns den metaphorischen und physischen Raum, uns frei und unbeobachtet zu bewegen, im Internet zu suchen was uns interessiert, mit Freunden und Bekannten über unsere Erlebnisse, Sorgen und Freuden zu schreiben. All das ohne die Angst, dass Unbekannte mitlesen oder unsere Schritte beobachten, dass wir zum Ziel einer Datensammelwut und zu informationstechnischen Objekten in einer Datenbank degradiert werden. So banal diese Forderungen klingen, so wichtig ist es, sie einzufordern. Um das zu gewährleisten, müssen Sicherheit und Bürgerrechte in einem internationalen Dialog fair und offen abgewogen werden. Ein wirksamer Schutz der Informationssysteme und ihrer Nutzerinnen und Nutzer – und damit eine Wahrung der Bürgerrechte – kann nur gewährleistet werden, wenn auch den Bürgerinnen und Bürgern eine Verantwortung über ihre eigene Daten übertragen wird.

## Anmerkungen

1 *National Security Agency (2013): Mission. http://www.nsa.gov/about/mission/index.shtml , Abruf 2013-07-18*
2 *Laudon, Kenneth C.; Laudon, Jane P.; Schoder, Detlef (2010): Wirtschaftsinformatik.2. Auflage, Pearson Studium, München*
3 *ebd.*
4 *Borchers, Detlef (2010): Zoff im Netz. http://www.sueddeutsche.de/digital/cyberwar-zoff-im-netz-1.610411, Abruf am 2013-07-18*
5 *Bundesamt für Verfassungsschutz: 2008. Spionage gegen Deutschland. Aktuelle Entwicklungen. Köln*
6 *G Data: IT-Security Trends in 2013: Cyverwar ist nicht in Sicht. http://www.gdata.de/index.php?id=11170&tx_ttnews[tt_news]=3027, Abruf 2013-07-18*
7 *CyberSecurity Summit (o.J.): http://www.cybersecuritysummit.de/, Abruf 2013-07-18*
8 *Medienpädagogischer Forschungsverbund Südwest (2012): JIM-Studie 2012. Jugend, Information, (Multi-) Media. Stuttgart*
9 *Michael Schenk, Julia Niemann, Gabi Reinmann, Alexander Roßnagel (2012): Digitale Privatsphäre: Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen. Schriftenreihe Medienforschung der LfM, Band 71, Berlin*
10 *Stephan Wolfram (2013): Data Science oft he Facebook World. http://blog.stephenwolfram.com/2013/04/data-science-of-the-facebook-world/ , Abruf 2013-07-18*
11 *Facebook (2013): Facebook Reports First Quarter 2013 Results. http://investor.fb.com/releasedetail.cfm?ReleaseID=761090, Abruf 2013-07-18*
12 *Bitkom (2010): Studie „Internet-Sicherheit“. Verbrauchermeinungen zur Datensicherung im Web. http://www.bitkom.org/files/documents/BITKOM_Internet_Sicherheit_Extranet.pdf, Abruf 2013-07-18*
13 *Ralf Ludwig (2012): der kategorische Imperativ. 14. Auflage, Deutscher Taschenbuch Verlag, München*
14 *Jens Ihlenfeld (2013): Gaben Microsoft, Google, Facebook & Co. Daten an die NSA? http://www.golem.de/news/prism-geben-microsoft-google-facebook-co-daten-an-die-nsa-1306-99676.html, Abruf 2013-07-19*
15 *Patrick Beuth (2013): Wie aus einem Verdächtigen eine Million werden. http://www.zeit.de/digital/datenschutz/2013-07/anhoerung-kongress-nsa-verbindungsdaten, Abruf 2013-07-19*
16 *Mathias Priebe (2013): Classified Matter. Mein Briefwechsel mit der NSA, http://www.golem.de/news/classified-matter-mein-briefwechsel-mit-der-nsa-1307-100335.html, Abruf 2013-07-19*
17 *Judith Horchert (2013): Spaziergang in Griesheim: Neue Spion-Safari am Dagger Complex. http://www.spiegel.de/netzwelt/netzpolitik/daniel-bangert-laedt-zum-dagger-complex-nach-griesheim-a-912041.html, Abruf 2013-07-19*
18 *Peter Schaar (2007): Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft. 1. Auflage, Goldmann Verlag, München*
19 *ebd. S. 25-30*
20 *Sabine Trepte (2012): Privatsphäre aus psychologischer Sicht. In: Schmidt, Jan-Hinrik; Weichert, Thilo (Hrsg.): Datenschutz. Grundlagen, Entwicklungen und Kontroversen, 1. Auflage, Bundeszentrale für politische Bildung, Bonn, S. 59-66 (Zitat S. 60)*
21 *Thilo Weichert (2013): Pressemitteilung. ULD: Schutz unserer Daten durch Schutz für Edward Snowden. https://www.datenschutzzentrum.de/presse/20130718-snowden.html, Abruf am 2013-07-21*
22 *Bettina Sokol (2012): Grundrechte sichern! In: Schmidt, Jan-Hinrik; Weichert, Thilo (Hrsg.): Datenschutz. Grundlagen, Entwicklungen und Kontroversen, 1. Auflage, Bundeszentrale für politische Bildung, Bonn, S. 137-144*
23 *Marion Albers (2012): Das Präventionsdilemma. In: Schmidt, Jan-Hinrik; Weichert, Thilo (Hrsg.): Datenschutz. Grundlagen, Entwicklungen und Kontroversen, 1. Auflage, Bundeszentrale für politische Bildung, Bonn, S. 107-114*
24 *ebd., S. 108*
25 *FIfF, mission statement*

**Dagmar Boedicker**

*„Es lässt sich zur Zeit schwer vorhersagen, ob wir einer Ära der internationalen Herrschaft des Rechts oder einer Renaissance des Faustrechts entgegengehen."*[1]



# In welchem Europa wollen wir leben?

## Eine geopolitische Betrachtung

*Der frühere wohlwollende Hegemon USA hat seinen Fokus verlagert. Er ist klamm und überschuldet, er pfeift auf die Verbündeten. Er pfeift aber auch auf das Völkerrecht, auf nationale Souveränität anderer Staaten und die Grundrechte fremder Staatsbürger. Europa muss selbst zusehen, wie es sich positioniert und in Frieden mit Nachbarn und Partnern kooperiert. Das müssen Europas Bürgerinnen und Bürger verstehen und die Konsequenzen daraus ziehen.*

Es ist nicht neu, dass die USA wie andere Staaten außenpolitisch das tun oder lassen, was ihnen nützt. Nach dem Fall der UdSSR hat US-Amerika seine Prioritäten neu geordnet und konzentriert seine wirtschaftliche, militärische und diplomatische Kraft nun um den Pazifik und in Asien. Es umwirbt Indien und beargwöhnt die aufstrebende Volksrepublik China. Die Akzeptanz seiner Vorrangstellung durch die Partner bestimmt immer weniger sein Handeln. In einer multipolaren Welt sind die USA nicht mehr Weltpolizist oder die Schutzmacht Europas, die bisher erhebliche Ressourcen für den Erhalt ihres imperialen Einflussbereichs[2] gegenüber einem starken Ostblock und im Nahen Osten bereithielt. Das wird zu teuer und findet keinen Rückhalt in ihrer tief gespaltenen Gesellschaft.

### Ungesetzlichkeiten der USA

Absolutes Souveränitätsgefühl ist eine Konstante US-amerikanischer Befindlichkeit. Es gibt den USA aber nicht das Recht, sich über das Völkerrecht, insbesondere die Menschenrechte, hinwegzusetzen. Nach dem zweiten Weltkrieg haben sie vor allem in Lateinamerika Folterer ausgebildet, Umstürze gefördert und Diktaturen eingeführt. Das war in den 1970er Jahren ein offenes Geheimnis. Auch die Abhöraktivitäten sind nicht neu, der Spiegel schrieb schon im Februar 1989:

> *„Die National Security Agency (NSA), der geheimste aller Geheimdienste, lauscht rund um den Erdball und rund um die Uhr [...] Wie in der Bundesrepublik, wo die eingeschränkte Souveränität der Deutschen freie Betätigung garantiert, unterliegt das Nachrichtenimperium nirgendwo einer Kontrolle. Pläne und Aktionen bleiben geheim, Namen der Mitarbeiter anonym. Weil das Budget des undurchsichtigen Großunternehmens in verschleierten Etatposten verschiedener US-Ministerien versteckt war, wußten selbst amerikanische Abgeordnete jahrelang nichts von der Bedeutung des Dienstes."*[3]

Nach dem 11. September 2001 fielen weitere Rechtsschranken: Der Präsident erhielt vom Parlament Generalvollmacht, nach Gutdünken Krieg zu führen. Der *Patriot Act* schuf kaum kontrollierte Kompetenzen für die Geheimdienste. Im Irak haben die USA einen völkerrechtswidrigen Krieg geführt, ihre Kampfdrohnen exekutieren Islamisten, Verdächtige wurden von Geheimdienstlern gekidnappt, in CIA-Flügen zu Foltergefängnissen und später nach Guantanamo verschleppt[4]. Was die USA dabei übersehen: „Der reine Verlaß auf die militärische Gewalt kann den Terror verstärken."[5]

Im Fall Snowden scheinen sie Anfang Juli Druck ausgeübt zu haben, damit das Flugzeug von Evo Morales, Boliviens Präsident, in Spanien, Portugal, Frankreich und Italien keine Lande- bzw. Überflugrechte erhielt. In Österreich, bei einer erzwungenen Zwischenlandung, wurde das Flugzeug in Augenschein genommen, wenn auch nicht durchsucht. Derartige Einflussnahme auf die Präsidentenmaschine ist eine klare Missachtung der nationalen Souveränität Boliviens.

Auch im internationalen Strafrecht lassen die USA die Welt ihre Übermacht spüren. Obwohl sie ursprünglich zu den Befürwortern eines Internationalen Strafgerichtshofs gehörten, erkennen sie ihn bis heute nicht an[6] und drohten, eigene „Staatsangehörige, gegen die vor dem Internationalen Strafgerichtshof verhandelt würde, notfalls mit Gewalt zu befreien."[7]

### Verlorene Autorität

Die Wirtschaft hatte nicht erfüllt, was Reagans Deregulierungs- und Privatisierungsstrategie versprochen hatte, und Clintons Eigenheim-Förderung trieb den Immobilienmarkt auf, bis die Blase platzte. Offshoring dezimierte die produzierende Industrie, Outsourcing als umfassende Strategie eroberte das Militär. Ganz offensichtlich war es den USA nicht mehr wichtig, private Unternehmen der (rechts-)staatlichen Kontrolle zu unterwerfen. Was nicht bedeutet, dass die Vereinigten Staaten Unternehmen nicht mehr kontrollieren wollen. Da, wo auch nur die kleinste Möglichkeit besteht, dass von den Kunden dieser Unternehmen eine Bedrohung ausgehen könnte, da ist die Überwachung schon

**Dagmar Boedicker**

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

lange Brauch. Damit verraten die Vereinigten Staaten die Ideale der Demokratie, Bürgerrechte und Freiheit, die sie im 20. Jahrhundert der Welt gepredigt haben. Es bleibt ihnen kaum Glaubwürdigkeit.

### Deutschland und die anderen

Margaret Thatcher wurde zitiert, sie liebe Deutschland so sehr, dass sie am liebsten zwei davon hätte. Nach beinahe 50 Jahren der Teilung war 1990 die Einheit Deutschlands umstritten, und Vorbehalte der Drei Mächte sind in den Verträgen zur Einheit Deutschlands als Ausnahmen vom Einigungsvertrag dokumentiert. Das Misstrauen ist kein Wunder, hatten wir doch bis zur Befreiung durch die Alliierten Europa terrorisiert und tragen die Verantwortung für die Toten zweier Weltkriege. Vor der Vereinigung hatten beide Teile unseres Landes ihre Erfahrungen mit Diktaturen gemacht, beide fühlten sich mehr oder weniger aufrichtig je einer anderen Siegermacht verpflichtet. Das nun vereinte Deutschland gehörte zur NATO, zur EU, zu den Vereinten Nationen, die USA wurden als guter Partner betrachtet, ihr Wohlstand und Lifestyle waren erstrebenswert, nicht nur hier sondern weltweit. Die GUS und dann Russland dagegen wurden misstrauisch beäugt: Ein Nachbar, dessen Entwicklung zunächst in Auflösungschaos und dann in eine gelenkte Demokratie mündete.

Ganz offensichtlich ist mittlerweile in der NATO die Rolle der Europäer gegenüber den USA geschwächt. Herfried Münkler vergleicht das Verhältnis mit der Situation des antiken Athens und seiner Bündnispartner:

> *„Solange die Konfrontation mit dem persischen Großreich akut war, behandelte Athen seine Bündner als zwar schwächer, aber dennoch gleichberechtigt. Als jedoch die Bedrohung mit dem Osten schwand, die Bündner die Friedensdividende kassierten und die Athener damit einverstanden waren, dass diese ihren Verpflichtungen in Form von Geldzahlungen nachkamen, verwandelten sie sich aus gleichberechtigten Verbündeten in abhängige Beherrschte, die den Wünschen und Vorgaben der Athener zu folgen hatten. Dass sie sich dabei gegeneinander ausspielen ließen, hat diese Entwicklung beschleunigt. Will Europa dem entgehen, so muss es sich als eine politische Einheit konstituieren, in der Außenstehende bei zentralen Entscheidungen nicht mitzureden haben – auch nicht der engste Verbündete.“*[8]

Klar war jedenfalls: Auch das vereinte Deutschland gehörte in die Europäische Union. Eine Einbindung, die uns vor größenwahnsinnigem Dominanzstreben bewahren und in einem solidarischen Entwicklungszusammenhang Europas einhegen sollte, durchaus mit Zustimmung der meisten deutschen Bürgerinnen und Bürger. Und bei aller Kritik am Demokratiedefizit der EU sollten wir uns auch davor hüten, „die empirische Qualität der Demokratie auf Ebene der Mitgliedstaaten zu idealisieren.“[9]

Fast fünf Krisenjahre von der Subprime- zur Finanzmarkt- und daraus folgend Schulden- und Staatskrisen haben die Einstellung der Deutschen zur EU verändert, der einfältige Krieg gegen den Terror mit der folgenden Sicherheit-statt-Freiheit-Ideologie die zu den USA.


### Die Rolle Europas

Keine Frage: Europa ist angezählt. Es hat Wachstumsschmerzen, die institutionelle Vertiefung musste 2004 verschoben werden, als die neuen Mitgliedstaaten aus Osteuropa beitraten. Trotz einer beeindruckenden Wertetradition, verkörpert durch den Europarat, die europäische Menschenrechtskonvention (EMRK) oder den Europäischen Gerichtshof für Menschenrechte, fährt der europäische Geleitzug so langsam wie sein langsamstes Schiff. Trotzdem ist das völkerrechtlich einmalige Experiment EU schneller und wirkungsvoller als die UN, in der die großen Mächte USA, China und Russland je nach Interessenlage auch da kräftig bremsen, wo ein gemeinschaftliches Vorgehen nötig wäre. Und es ist unser Experiment, das die Bürger Europas gewollt haben, mit dem sie Lehren aus Furcht und Schrecken zweier Weltkriege mit um die 70 Millionen Toten gezogen haben. Zwar hat es den Makel, dass wirtschaftliche Ziele immer den stärksten Antrieb lieferten, aber es waren eben nicht die einzigen Ziele. Ziel ist auch der Schutz der Grundrechte! Inzwischen ist die Grundrechte-Charta rechtskräftig, die EU wie ihre Mitgliedstaaten sind verpflichtet, die Bürgerrechte gemäß der Charta zu verteidigen. Der Vertrag von Lissabon ermöglicht ein besser abgestimmtes Handeln der Mitgliedstaaten und der EU-Institutionen. Es gibt tüchtige Politikerinnen und Politiker in der EU, Justizkommissarin Viviane Reding beispielsweise, die den Entwurf der Grundverordnung bewirkt hat. Oder Jan-Philipp Albrecht, Berichterstatter im LIBE-Ausschuss, der mit seinem Team den Entwurf gegen geballte Lobby-Macht entscheidend verbessert hat. Reding kämpft energisch für einen wirksamen Datenschutz in der EU, sie will das Safe-Harbor-Abkommen mit den USA überprüfen, einen Schandfleck auf dem europäischen Datenschutz.[10]

Wenn wir also eine Renaissance des Faustrechts vermeiden und statt dessen zumindest in Europa die Werte der Aufklärung und demokratischen Freiheiten hoch halten wollen, dann werden wir sie verteidigen müssen. Ohne informationelle Selbstbestimmung wird das nicht gehen, denn wer sich beobachtet fühlt, verliert den Mut für die Ziele einzutreten, die sie oder er will. Ohne einen gemeinsamen europäischen Datenschutz, nur auf nationaler Ebene, sind aber weder unsere informationelle Selbstbestimmung noch die Vertraulichkeit und Integrität informationstechnischer Systeme zu gewährleisten.

> *„… die europäischen Gemeinschaften [sind] gegründet worden, um die Schwächen der Nationalstaaten und ihre begrenzte Handlungsfähigkeit in Fragen von Wohlstand und Sicherheit durch Integration, durch Übertragung von Souveränität, zu verbessern.“*[11]

In den letzten Jahren ist in Europa eine Sehnsucht nach der nationalen Kuschelecke zu beobachten. Aber, wie Martin Schulz, Präsident des Europäischen Parlaments, in einem Gastbeitrag für den Deutschlandfunk am 6. März 2013 sagte: „Ein Zurück in den angeblich so sicheren Schoß des Nationalstaates kann es nicht geben.“ Ganz abgesehen davon, dass dieses nostalgische Zurück populistische und unerfreuliche Züge tragen kann, wie derzeit in Ungarn zu besichtigen.

### Ausblick

Die Europäische Union ist mehr als eine Freihandelszone. Horst Bacia zitiert Helmut Schmidt: „Obwohl Amerikaner und Briten wohl nichts dagegen hätten, wenn die ‚politische Union zu einer Freihandelszone verkümmern' würde …“ . Gerade jetzt, wenn die USA auf einen Vertrag über Transatlantic Trade and Investment Partnership (TTIP) drängen, während sie mit Prism, XKeyscore, Lopers, Juggernaut und Co. ihre Partner bespitzeln, gerade jetzt muss die EU hart bleiben: Keine weiteren Verhandlungen über TTIP ohne umfassende Aufklärung über die Spionage- und Überwachungsaktivitäten und strenge, kontrollierbare Regelungen zum Datenschutz. Ich wünsche mir, dass wir nach vorn statt zurück gucken: Für eine menschenfreundliche und zeitgemäße IT!

- Wir brauchen eine datensparsame und sichere Technik und Datenschutz-freundliche Voreinstellungen.
- Technische Schutzmechanismen wie Vertraulichkeit, Authentizität und Verfügbarkeit, Transparenz, Zweckbindung und Intervenierbarkeit müssen in den Systemen angelegt und kontrollierbar sein.
- Wir brauchen defensive IT-Sicherheit statt Offensiven im Cyberspace, wie es das FIfF schon lange fordert.
- Wir brauchen eine europäische Datenschutz-Verordnung, die auch für Anbieter außerhalb der EU greift.

Mit solchen Alleinstellungsmerkmalen könnten europäische Forschung und Industrie international glänzen. Ob sie das wohl verstanden haben?

## Anmerkungen

1 *Weigand, Thomas. Zitiert nach Wesel, Uwe: Geschichte des Rechts in Europa, S. 656. Verlag C. H. Beck oHG, München, 2010*

2 *Gemeint ist hier eine Imperialmacht im Sinne von Herfried Münkler, nicht ein imperialistischer Staat.*

3 *Der Spiegel vom 20.2.1989*

4 *Marty, Dick, CIA-Sonderberichterstatter des Europarats, im Interview mit dem Deutschlandfunk vom 9.7.2013 über eine NATO-Sitzung im Oktober 2001 zu Geheimgefängnissen und geheimen Entführungen: „… alle Operationen liegen bei der CIA. Die Mitgliedsstaaten der NATO, aber auch die, die Kandidaten zur NATO waren, die verpflichten sich, eine totale Immunität dieser Agenten zu gewähren, was übrigens unrechtmäßig ist. Die ganze Operation wird auf die höchste Stufe des Geheimnisses gesetzt, nach dem berühmten Prinzip ‚need to know'. Das, was in Brüssel damals entschieden wurde, war nur einzelnen Mitgliedern der europäischen Regierungen bekannt.“*

5 *Czempiel, Ernst-Otto: Weltpolitik im Umbruch. Verlag C. H. Beck oHG, München, 2002. Lizenzausgabe für die Bundeszentrale für politische Bildung, Bonn 2002, S. 186*

6 *Im März 2013 hatten allerdings auch China, Russland, Pakistan und Indien das Statut noch nicht ratifiziert.*

7 *Czempiel, Ernst-Otto, a.a.O., S. 128*

8 *Münkler, Herfried: Imperien, S. 249. Rowohlt – Berlin Verlag GmbH, Berlin. 2005. Lizenzausgabe für die Bundeszentrale für politische Bildung, Bonn 2005*

9 *Lippert, Barbara: Die EU zusammenhalten – aber wie? S. 11. Arbeitspapier der Forschungsgruppe EU-Integration, Stiftung Wissenschaft und Politik, Deutsches Institut für Internationale Politik und Sicherheit. SWP Berlin. März 2013*

10 *„The Safe Harbour agreement may not be so safe after all. … the Commission is working on a solid assessment of the Safe Harbour Agreement which we will present before the end of the year.“ http://europa.eu/rapid/press-release_MEMO-13-710_en.htm (abgerufen 31.7.13)*

11 *Lippert, Barbara: Die EU zusammenhalten – aber wie? a.a.O. S. 16.*

12 *Bacia, Horst: Ausgang ungewiss – die Verhandlungen über einen Beitritt zur EU. In: Steinbach, Udo (Hrsg.): Länderbericht Türkei. Bundeszentrale für politische Bildung, Bonn 2012. S. 448*


*alle Fotos Dagmar Boedicker*

**Björn Schembera**

# Big Data: Big Business, Big Brother, Big Chances?

*Seit einiger Zeit taucht immer wieder der Begriff* Big Data *auf – zunächst im akademischen Bereich, dann in der Fachpresse und schließlich widmete im Mai selbst der* Spiegel *dem Begriff eine Titelstory. Big Data ist die neue Cloud, zumindest was die Tragweite und die Wichtigkeit der Technologie angeht, die sich hinter diesem Begriff verbirgt. Folgt man* Google Trends*, welches die Suchhäufigkeit von Begriffen bei Google relativ zueinander darstellt, so ist Big Data gerade dabei,* Cloud Computing *zu überholen [1]. Brisanz gewinnt der Begriff vor dem Hintergrund der Enthüllungen von Edward Snowden. Umso wichtiger wird eine kritische Reflexion über die Technologie von Big Data.*



Im Folgenden wird kurz auf die Begriffsgeschichte eingegangen, um dann näher zu beleuchten, was unter Big Data momentan verstanden wird. Dann werden einige Bespiele genannt. Schließlich soll es zu einer kritischen Auseinandersetzung kommen.

Zwar gibt es Anfang der 2000er schon einige Publikationen, die die Wichtigkeit der Verarbeitung von großen, unstrukturierten Datenmengen herausstellen, allerdings findet sich der Begriff *Big Data* erst seit 2008 in der Literatur. 2012 ist er im Mainstream angekommen: Kaum eine Konferenz trägt nicht das Schlagwort im Titel, kaum ein Hersteller von Hard- oder Software labelt sein Produkt nicht damit. Ebenfalls widmen Magazine wie der *Spiegel* dem Begriff Titelstories, schon bevor dieser durch Snwodens Enthüllungen wirklich politisch aufgeladen wurde.

2001 waren es Wissenschaftler der *META Group*, die die theoretischen Grundsteine für Big Data legten. Dabei sprechen sie von dreidimensionalem Datenmanagement, das heißt nicht nur von der Datenmenge (Volume), sondern auch von der Datenvielfalt (Variety) sowie der Datengeschwindigkeit (Velocity) [2]. Die Zusammenführung dieser Aspekte ist zentral für Big Data; sie sollen hier noch einmal kurz getrennt voneinander beschrieben werden:

- **Datenmenge/Volume:** Hier ist das steigende Datenvolumen gemeint, das sich allein ob der Größe nur noch schwer handhaben lässt. Hierbei geht es einerseits um das globale Datenvolumen, welches allein für 2012 auf 2,8 Zettabyte ($2{,}8*10^{21}$ Bytes) veranschlagt und auf 40 Zettabyte im Jahr 2020 geschätzt wird [3]. Andererseits geht es um das für ein spezifisches Problem zu verarbeitende Datenvolumen, welches heute im Bereich von Petabyte ($10^{15}$ Bytes), in wenigen Jahren schon im Bereich von Exabyte ($10^{18}$) liegt. Dieser Aspekt wird eher vom klassischen wissenschaftlichen Rechnen und im Supercomputing behandelt.

- **Datenvielfalt/Variety:** Dieser Aspekt beschäftigt sich mit dem Umstand, dass Daten aus verschiedenen Quellen kommen und dabei strukturiert, semistrukturiert oder unstrukturiert sein können. Getrennt betrachtet ist dies der klassische Gegenstand von Datenbankforschung und deren Produkten, wobei feststeht, dass das Paradigma der relationalen Datenbanken oft nicht mehr ausreichend ist.

- **Datengeschwindigkeit/Velocity:** Hierbei ist von Bedeutung, dass Daten heute immer schneller generiert werden und diese auch immer schneller zirkulieren. Dies ist auch mit der Ubiquität von Daten gemeint. Daten werden nun ständig und überall mittels Smartphones und breitbandigen Mobilfunkverbindnungen erzeugt und weiterverbreitet.

Gibt es in den einzelnen Bereichen getrennte Lösungsansätze, so will Big Data eine Zusammenführung der Bereiche und eine gemeinsame Lösung für Probleme, die sich im Spannungsfeld der 3 „V" abspielen, leisten. Dabei geht es um die Analyse von Zusammenhängen in großen (riesigen) Datensätzen aus unterschiedlichen Quellen unter Berücksichtigung der Aktualität, also darum, die *„vielfältigen, meist unstrukturierten Informationen [..] im richtigen Kontext schnell auszuwerten und nutzbar zu machen"* [3].

Selbstverständlich müssen dafür auch gewisse technologische Randbedingungen erfüllt sein: Diese finden sich in den Bereichen Storage, verteilte Rechenressourcen und der Verfügbarkeit von Daten. Im ersten und zweiten Bereich wachsen die Kapazitäten nach wie vor, neue Technologien wie SSDs oder neue Prozessorgenerationen und Clustertechnologien bringen hier den erfordlichen Leistungszuwachs. Brisant ist der letzte Punkt, die Verfügbarkeit von Daten. Hier kam es in den letzten 5-10 Jahren zu einer maßgeblichen Veränderung, wie und wann Personen Daten erzeugen und verbreiten. Einerseits werden Daten im Hintergrund erzeugt und gesammelt, ohne dass sich die Person dessen bewusst ist. Beispielsweise werden bei Smartphones oft Daten wie Positionsinformationen mitgeschnitten. Selbstverständlich sammeln aber auch staatliche Institutionen Daten jeglicher Art, wie die Enthüllungen der letzten Wochen zeigten. Andererseits veröffentlichen Individuen heute auch freiwillig Informationen aus ihrer Privatsphäre wie Position, momentane Beschäftigung, Bilder usw. Diese Informationen werden über Social Networks wie Facebook, Twitter, flickr und anderen teilweise weltweit öffentlich gemacht.

## Anwendungsfälle für Big Data sind in verschiedenen Gebieten zu finden

Im wissenschaftlichen Bereich liegt der Fokus zwar eher auf der Datenmenge, allerdings kommt auch hier die Datengeschwindigkeit ins Spiel, wenn beispielsweise der *Large Hadron Collider* 40 mal pro Sekunde Daten von 150 Millionen Sensoren holt, wobei 600 Millionen Teilchenkollisionen pro Sekunde aufgezeichnet werden. Diese Datenmenge wird so reduziert, dass nur noch die 100 Kollisionen pro Sekunde, die wirklich von Interesse sind, bestehen bleiben.

Generell wird die Wissenschaft eher empirisch, anstatt sich an theoretischen Diskussionen über die Modelle aufzuhalten – genau hier trifft der Begriff Big Data [4].

Ein Beispiel aus der Business-Welt ist die Analyse von Google-, Twitter- und Facebook-Daten, um den Erfolg von Werbeaktionen zu messen. Dabei werden solche frei zugänglichen Datenquellen

angezapft, die Suchergebnisse verknüpft und daraus Rückschlüsse auf den Erfolg einer Werbekampagne gezogen. Mit den gewonnen Informationen kann evtl. direkt die Logistik optimiert werden [3].

## Zwei der wichtigsten Techniken zur Verarbeitung

An erster Stelle steht der von Google 2004 vorgestellte *MapReduce*-Algorithmus [5], welcher einem algorithmischen *Divide&Conquer*-Ansatz auf (Schlüssel, Wert)-Paaren entspricht: Ein parallelisierbares Problem wird zunächst im sog. Map-Schritt in kleinere Teilprobleme zerlegt und von den Rechenknoten in einem Cluster bearbeitet. Dieser Schritt kann auch rekursiv über mehrere Ebenen zerteilt werden. Im Reduce-Schritt werden die Teilergebnisse zu einer Gesamtlösung zusammengeführt. Als Trivialbeispiel sei hier die Textanalyse genannt, in der beispielsweise ein Text in seine Sätze oder Zeilen zerteilt wird, die dann parallel durchsucht werden. Am Schluss wird das Gesamtergebnis aus den Einzelergebnissen konstruiert. Die bekannteste Implementierung dieses Verfahrens trägt den Namen *hadoop* und wurde von der Apache Foundation geleistet [6].

Eine weitere Technologie ist *NoSQL*, das für *„Not only SQL"* steht. Es handelt sich dabei um eine Bewegung für analytische Datenbanken, mit denen das – für die Problemstellungen innerhalb von Big Data – zu strenge SQL-Konzept mit seiner Relationalität angegriffen und das ACID-Konzept zu Gunsten von Leistung aufgeweicht werden soll. Auch die Datensätze können hier beliebig strukturiert sein, ebenso können Datenbanken leicht verteilt werden und skalieren somit besser. Es finden sich bereits verschiedene Implementierungen oder Produkte wie *Cassandra*, *Greenplum*, *MongoDB*.

Die vorangehende Untersuchung zeigt, dass Big Data aufs *große Ganze* zielt. Mussten früher unterschiedliche (Daten-)strukturen noch mit menschlichem Zutun zusammengeführt werden, soll dies jetzt vollautomatisch und in Echtzeit geschehen – dies ist bei den heutigen riesigen Datenmengen auch nicht mehr anders möglich.

## „Cui bono?" ist hier die entscheidende Frage

Die Technologien sind – wenn auch noch nicht komplett ausgereift – verfügbar. Wie ich sie nutze, ist die entscheidende Frage. Dass die Industrie großes Interesse an Forschung und Nutzung von Big Data hat, sollte schon durch oben genanntes Beispiel klar geworden sein.

Wie politisch aufgeladen und höchst brisant diese Technologie ist, zeigen die Berichte Edward Snowdens. So schreibt Florian Rötzer auf Telepolis über das *XKeyscore* Überwachungsprogramm:

> *„Die gesammelten Datenmengen sind enorm. Nach einem Bericht aus dem Jahr 2007 seien bereits 850 Milliarden ‚call events' und 150 Milliarden Internetdaten gesammelt und gespeichert worden, jeden Tag kämen 1-2 Milliarden dazu. Es handelt sich also wirklich um Big Data, für die man gewaltige Serverfarmen benötigt, wie sie für die NSA gerade fertiggestellt werden." [7]*

Momentan stellt der amerikanische Staat in Bluffdale bei Utah ein Rechenzentrum von gigantischem Ausmaß für 1,7 Mrd. US-Dollar fertig, dessen Speicherkapazität 5 Zettabyte ($5*10^{21}$ Bytes) beträgt, was auf die Erdbevölkerung umgerechnet 700GB/Person entspräche. Berichten zufolge soll es genau dem Zweck der Zusammenführung von Daten aus verschiedenen Quellen dienen, um damit vorgeblich die Sicherheit des amerikanischen Staates zu erhöhen [8]. Was früher der Wunschtraum von Geheimdiensten war und von Science Fiction beschrieben wurde, nämlich die automatisierte totale Überwachung von Personen in Echtzeit, soll jetzt durch die Technologie Big Data Realität werden.

## Für Geheimdienste soll Big Data synonym stehen zu Big Brother, für Unternehmen zu Big Business

Die Technologie ist jedoch noch neu und der Kampf um sie noch nicht ausgefochten. Generell muss es zu einem kritischen Umgang mit der Technologie kommen – eine gründliche Reflexion über Big Data ist derzeit zu Gunsten eines puren Machbarkeitsfetisch komplett ausgeblendet. Es geht um die gesellschaftlichen Implikationen, die mit dieser Technologie einhergehen und höchst brisant sind, denn nicht ohne Weiteres würde ein staatliches bzw. geheimdienstliches Rechenzentrum in Utah genau für den Zweck Big Data entstehen.

Dass Big Data auch Big Chances bedeuten kann, zeigen mögliche Anwendungen im wissenschaftlichen Bereich, wie die optimale Positionierung von Windkraftwerken [3]. In Kanada wurde neuerdings ein Uni-Institut für Big Data gegründet, das nach eigener Aussage an der Technologie forschen will, um damit Erkenntnisse für den Menschen und zum Schutz seiner Privatsphäre zu gewinnen [9]. Es geht um Engagement in Big Data für den Menschen in einer kritischen Weise.

## Anmerkungen


[1] *http://www.google.com/trends/explore?q=big+data#q=big%20data%2C%20%20cloud%20computing&cmpt=q, Zugriff 30.7.2013*

[2] *http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf, Zugriff 30.7.2013*

[3] *i'X 5/2013*

[4] *http://en.wikipedia.org/wiki/Big_data, Zugriff 30.7.2013*

[5] *http://static.googleusercontent.com/external_content/untrusted_dlcp/research.google.com/en//archive/mapreduce-osdi04.pdf, Zugriff 30.7.2013*

[6] *http://hadoop.apache.org/, Zugriff 30.7.2013*

[7] *http://www.heise.de/tp/artikel/39/39623/1.html, Zugriff 1.8.2013*

[8] *http://en.wikipedia.org/wiki/Utah_Data_Center, Zugriff 30.7.2013*

[9] *http://www.heise.de/ct/meldung/Kanada-gruendet-Uni-Institut-fuer-Big-Data-Analyse-1920799.html, Zugriff 30.7.2013*




**Björn Schembera**

**Björn Schembera** ist Diplom-Informatiker und lebt in Stuttgart.

**Sylvia Johnigk, Kai Nothdurft**

# PRISM – Welche Rolle spielen US-IT-Firmen?

*Laut Guardian soll die NSA seit Jahren einen direkten Zugriff auf die Server und somit auf Kommunikations- und Internetdaten von Millionen KundInnen vieler wichtiger Internetdienstleister besitzen. Es sollen verdachtsunabhängig alle ausländischen KundInnen betroffen sein, US-BürgerInnen „nur", soweit sie mit AusländerInnen kommunizieren. Die US-Regierung wiegelt ab. Der Director of National Intelligence, James Clapper, gibt die Existenz von PRISM zu, spricht aber „nur" von Verkehrsdaten und ausschließlich von Fällen mit einem konkreten Verdacht. Die meisten der im Guardian erwähnten Firmen haben inzwischen ebenfalls dementiert, in der dargestellten Form mit der US Regierung zusammen zu arbeiten.*



Nehmen wir an, dass die Darstellung des Guardian korrekt ist und tatsächlich ein direkter Zugriff der NSA auf die KundInnendaten der genannten Firmen erfolgt. Die Dementis der Firmen können dann in zwei Varianten interpretiert werden:

**Variante 1:** Die Unternehmen kooperieren nicht in der dargestellten Form mit der NSA. Wie ist es der NSA gelungen, die Schnüffelkomponenten unbemerkt zu installieren? Es gab bereits Fälle, in denen IT-Systeme von größeren Organisationen über mehrere Jahre unbemerkt mit Schadsoftware kompromittiert waren. Allerdings war die Sachlage eine andere. In diesem Fall handelt sich es um Unternehmen, deren Kernkompetenz im Bereich Internet/IT liegt. Und dort soll es gelungen sein, fast alle Daten, die vom Unternehmen verarbeitet werden, über Jahre an externe Server zu übertragen, ohne dass es bemerkt wurde? Sämtliche Sicherheitsmechanismen und Systeme, Virenscanner, Netzwerkanalysetools und Monitoringsysteme etc. hätten völlig versagt. Keinem dieser Programme und der gesamten MitarbeiterInnen, die die Systeme betreuen, wäre aufgefallen, dass Ressourcen von einem hohen Ausmaß aufgewandt werden, ohne dass es eine Erklärung also einen dazugehörigen Geschäftsprozess dafür gibt. Das käme einem Offenbarungseid der IT-Sicherheitsabteilungen der Unternehmen gleich. In Zeiten von Kosteneinsparungen muss es auffallen, wenn Kosten entstehen, die keinen monetären Nutzen bringen. Jedes Jahr finden Konsolidierungsrunden statt, in denen unter anderem Serverkosten hinterfragt werden. Spätesten die Controller sollten hinterfragen, wie das höhere Datenvolumen zu erklären ist.

**Variante 2:** Die beteiligten Firmen haben mit der NSA kooperiert und zugelassen, dass die NSA PRISM installiert hat und dass fortan sämtliche Informationen direkt an die NSA in Echtzeit übermittelt wurden. Dies wirft andere Fragen auf: Zu wem ist die NSA gegangen? Warum hat der oder die Verantwortliche der Installation nicht widersprochen, zumal der Umfang selbst in den USA nicht legal wäre, wenn auch US-BürgerInnen überwacht wurden. Wie ist es dem Mitarbeiter oder der Mitarbeiterin gelungen, innerhalb der normalen Prozesse eines Unternehmens die Schnüffelprogramme „unauffällig" installieren zu lassen, ohne dass andere beteiligte MitarbeiterInnen Fragen stellen? In Unternehmen wie Google, Microsoft, YouTube, Apple, Facebook etc. ist eine Vielzahl von MitarbeiterInnen in Installations- und Changeprozesse involviert. Beteiligte MitarbeiterInnen werden informiert, selbst wenn ein Vorstandsmitglied Aktivitäten persönlich anordnet und höher priorisiert. Allen Menschen, die die Systeme betreuen, hätte man eine Story erzählen müssen: Warum oder weshalb gibt es eine Software, die relativ offensichtlich nicht von internen MitarbeiterInnen genutzt wird, dafür aber sehr viel Bandbreite benötigt und alle Informationen einer Anwendung an einen externen Server überträgt? Facebooks wichtigstes Asset sind z. B. die Daten ihrer Mitglieder und diese Daten werden an einen externen Server übermittelt.

Obwohl beide Varianten viele Fragen aufwerfen, ist leider die zweite die wahrscheinlichere. Die MacherInnen dieser Unternehmen sind nahezu fast ausschließlich von egomanischer Struktur, vielfach treten die Unternehmen nach außen liberaler auf, als sie es innen sind. Apple hat z. B. eine strikte Geheimhaltungskultur entwickelt. MitarbeiterInnen werden, wenn sie das Firmengelände betreten oder verlassen, kontrolliert und dürfen nur wenig mitbringen und noch weniger wieder herausbringen. Google kooperiert (zwangsweise) mit chinesischen Regierungsstellen, warum dann nicht auch mit der NSA? Es ist wahrscheinlich, dass diejenigen MitarbeiterInnen, die Fragen stellten, mit einer Geheimhaltungsklausel klein gehalten wurden, möglicherweise mit der Lüge, dass nur Daten von AusländerInnen übermittelt werden.


Sollten sich die Informationen des Guardian bewahrheiten, muss spätestens jetzt jedem europäischen Unternehmen klar sein, dass Daten, die es bei US-amerikanischen Unternehmen speichert, im Zugriff von amerikanischen Sicherheitsbehörden sind. Firmengeheimnisse sind dort direkt der Wirtschaftsspionage ausgesetzt. Auch datenschutzrechtlich hat dies Konsequenzen. Es dürfen keine personenbezogenen Daten von Dritten, etwa KundInnen- oder MitarbeiterInnen-Daten, mehr bei den kooperierenden Unternehmen verarbeitet werden. Die im Bericht genannten Unternehmen wären für Auftragsdatenverarbeitung nach §11 BDSG wegen nachgewiesener Unzuverlässigkeit ungeeignet. Wurden in den im Bericht genannten Zeiträumen bereits sensible KundInnendaten, etwa Kontoinformationen in den Clouddiensten der Firmen gespeichert, so müssen die KundInnen gemäß §42a BDSG über die Kompromittierung durch die Übertragung zur NSA informiert werden. Das *Safe-Harbor*-Abkommen ist nichts wert, wenn Firmen wie Apple, Facebook, Microsoft, Google, etc. zwar einen gewissen Schutz zusagen, aber nicht einhalten.

Selbst wenn sich die Vorwürfe nicht vollständig beweisen lassen, werden die Bedenken und Vorbehalte gegen die Unternehmen wachsen. Viele KundInnen und BenutzerInnen werden sich nach Alternativen umsehen oder sparsamer in der Weitergabe ihrer Daten werden.

**Sylvia Johnigk, Kai Nothdurft**

# Der NSA-Skandal, ein Déjà vu

*Ronald Pofalla erklärte am 12. August 2013 die aktuelle NSA-Affäre für beendet. Innenminister Hans-Peter Friedrich legte nach und behauptete am 16. August 2013, alle Vorwürfe seien ausgeräumt. Dabei stützen sich die Regierungsvertreter ausschließlich auf Aussagen der Geheimdienste.*



Es wurde dabei nur die einschränkende Aussage gemacht, dass deutsche Gesetze nicht verletzt würden.

Abgesehen davon, dass nur von den Verdächtigen behauptet wurde, dass Gesetze in Deutschland nicht verletzt würden, blieben dabei schwerwiegende Vorwürfe unwidersprochen:

1. US-amerikanische Internetunternehmen sollen im Rahmen des Programms *PRISM* massenweise Kundendaten an die NSA zur Auswertung weitergegeben haben.

2. Der britische Geheimdienst GHCQ soll im Rahmen des Programms *Tempora* den Internetverkehr an zentralen Glasfaserleitungen des Internetbackbone komplett abhören und über mehrere Tage speichern.

Der Verdacht der massiven Verletzung von Grundrechten ist damit nicht nur nicht ausgeräumt. Er wurde nicht einmal dementiert.

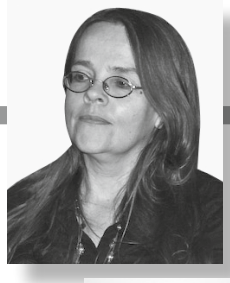
Ein weiterer Vorwurf, die NSA würde EU-Institutionen und Deutschland ausspionieren, wurde gar von Friedrich mit der Begründung als haltlos bezeichnet, dass die USA sich zur Verhandlung über ein No-Spy Abkommen bereit erklärt hätten.

Hier stellt sich zunächst die Frage, warum denn ein No-Spy-Abkommen nötig ist, wenn doch angeblich gar nicht spioniert wurde. Noch bemerkenswerter ist aber der Vertrauensvorschuss, der hier vom Innenminister den Geheimdiensten im Allgemeinen und der NSA im Besonderen entgegengebracht wird.

Wie kommt die Regierung in Anbetracht des Umfangs, der Komplexität und der Tragweite des Skandals dazu, die Affäre nach so kurzer Zeit als erledigt zu betrachten? Es ist nahezu unmöglich, in der kurzen Zeit die Vorwürfe selbst gewissenhaft zu untersuchen.

Durch die Enthüllungen von Edward Snowden gibt es zudem belastende Zeugenaussagen. Bereits im Zusammenhang mit dem Programm *Echelon* wurde bei einer Untersuchung durch die EU[1] 2001 festgestellt, dass Spionageaktivitäten durch US amerikanische Geheimdienste stattgefunden haben. Dies wurde sogar vom ehemaligen CIA-Chef James Woolsey öffentlich zugegeben[2]. Es besteht somit der dringende Verdacht der Wiederholungstäterschaft.

Gegenüber den US-amerikanischen Geheimdiensten scheint der Innenminister eine sehr großzügige Interpretation der Unschuldsvermutung zu vertreten, wie man sie sich im Zusammenhang mit der Vorratsdatenspeicherung und vielen anderen Gesetzen zur Inneren Sicherheit gerne einmal gegenüber dem eigenen Souverän, der deutschen Bevölkerung, wünschen würde. Völlig absurd wird dieser Vertrauensvorschuss gegenüber der NSA, wenn man bedenkt, dass die Behauptungen, man verstoße nicht gegen Gesetze, gegenüber ausländischen Regierungsvertretern getätigt wurden, denen die US-Behörden formal keinerlei Rechenschaft schuldig sind. Inzwischen wurde durch Snowden bekannt, dass sogar US-Bürger in großem Umfang ausgespäht und damit die US-amerikanische Verfassung gebrochen wurde. Dass der US-Geheimdienstchef James Clapper den amerikanischen Senat belogen hat, ist inzwischen ebenfalls nachgewiesen[3]. Enthüllungen von weiteren ehemaligen NSA-Mitarbeitern wie Thomas Drake und William Binney zeigen zudem, dass es sich auch beim Verletzen der US-amerikanischen Verfassung um Wiederholungstaten handelt[4]. Wie viel weniger mögen US-amerikanische Dienste da wohl deutsche Gesetze interessieren?



**Sylvia Johnigk und Kai Nothdurft**

**Sylvia Johnigk** studierte Informatik an der TU-Berlin und befasste sich schon im Studium mit Themen wie Datenschutz und Informationssicherheit, arbeitete fünf Jahre in der Forschung am Thema Informationssicherheit und acht Jahre bei einem Finanzdienstleister als IT-Security Consultant in Frankfurt am Main. Seit Mitte des Jahres 2009 ist sie selbständig und leitet ein kleines Unternehmen in München, das sich auf Beratung von Unternehmen zum Thema Informationssicherheitsmanagement mit dem Schwerpunkt Mitarbeitersensiblisierung spezialisiert hat.

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

Zur Bewertung der Rechtschaffenheit der NSA lohnt noch ein weiterer Blick in die Vergangenheit: auf die Affäre um den Einsatz der Data-Mining-Software PROMIS im Rahmen der *Inslaw-Verschwörung*. PROMIS – *Prosecutor's Management Information System* – ist eine Software, die in den 70er Jahren von Inslaw entwickelt wurde. In diesem Gebilde gibt es zwei Aspekte, die auch im Zusammhang mit PRISM Beachtung verdienen: Inslaw und PROMIS (siehe Kasten).

**Inslaw** *war* ein Unternehmen, das anfangs im staatlichen Auftrag für Behörden im Rechtsbereich, insbesondere für Staatsanwaltschaften, die Software PROMIS konzipierte. PROMIS konnte als elektronisches Schleppnetz ausgeworfen werden und Daten aus verschiedenen Datenbanken zusammenführen. Die Software fand ihren Einsatz bei der Aufklärung von Verbrechen. Die NSA war nicht davon begeistert, da es einer ihrer ehemaligen Mitarbeiter war, der zu Inslaw wechselte und NSA-Wissen in ein damals noch gemeinnütziges Unternehmen transferierte. Da PROMIS aus öffentlichen Mitteln finanziert war, handelte es sich zunächst um Public-Domain-Software. Anders als bei Open-Source-Software darf die Software grundsätzlich ohne Lizenzgebühr genutzt werden, der Sourcecode bleibt beim Unternehmen. Später, als unter US-Präsident Carter öffentliche Mittel ausblieben, wurde Inslaw in ein kommerzielles Unternehmen umgewandelt, das PROMIS auf eigene Kosten weiterentwickelte. Nach einem von außen absichtlich verursachten Bankrott verschwand das Unternehmen 1985 von der Bildfläche. Der Bankrott war die Folge mangelnder Kooperationsbereitschaft mit staatlichen Behörden seitens Inslaw. Bei diesem provozierten Bankrott spielte die NSA eine zwielichtige Rolle, die sich im Umfang und auf Grund der Vielzahl von Akteuren, die zur Verschleierung beigetragen haben nicht bemessen lässt. Mittlerweile scheint Inslaw wieder auferstanden zu sein und besitzt zumindest eine Webseite.

**PROMIS** funktioniert wie ein elektronisches Schleppnetz und kehrte als Konkursmasse zurück zur NSA. Es wurde weiterentwickelt, erhielt ein trojanisches Pferd in Form einer *Backdoor* und gelangte teilweise auf Umwegen an andere Geheimdienste bzw. Regierungen (Canada, Großbritanien, Israel, Libyen, Saudi-Arabien, Guatemala, Singapur, Deutschland). Nicht verwunderlich, dass auch CIA und FBI es einsetzten. Das Schleppnetz wurde fortan von allen genutzt, die ein hohes Interesse hatten, möglichst viele Informationen über vor allem unliebsame Personen zu sammeln und diese Informationen intelligent miteinander zu verknüpfen. Es war ein Verkaufsschlager und wurde ohne Rücksicht an Freund oder Feind aller politischen Couleur verkauft.

Versuche, diese Affäre im Ganzen aufzuklären, endeten unter anderem mit einem Journalisten, der „Selbstmord erlitt", einem Informanten, der nachweislich ermordet wurde, einem Richter, der nicht wiederberufen wurde, und scheiterten an mehreren US-Präsidenten wie Reagan, Bush sr. und Clinton, die alle an einer Aufklärung nicht interessiert waren.

Bei dem Text in diesem Rahmen handelt es sich um eine Zusammenfassung aus dem Buch: *Die Datenmafia von Egmont R. Koch und Jochen Sperber, Rowohlt Verlag 1995, ISBN 3 498 06304 9*

Bemerkenswert ist nicht nur die Namensähnlichkeit (PROMIS/PRISM), sondern vor allem die Ähnlichkeit der Funktionalität beider Programme und die vielen Lügen und Verschleierungen, die beide ummanteln. Zudem zeigt sich, dass die Regierungen und Geheimdienste keineswegs zimperlich sind, wenn es darum geht, Unternehmen unter Druck zu setzen, um sie zur Kooperation zu bewegen, eine weitere Facette auch von PRISM. In den USA haben zwei E-Mail-Dienstleister *Lavabit* und *Silent Circle* ihren Service aufgegeben, die ihren Kunden einen vertraulichen verschlüsselten E-Mail-Dienst angeboten haben. Ladar Levison, Gründer von Lavabit, bei dem wohl auch Edward Snowden Kunde war, begründete die Entscheidung sein Geschäft aufzugeben damit, dass „der E-Mail-Dienst durch das Vorgehen von US-Behörden nicht mehr so sicher gewesen wäre wie versprochen."[5] Silent Circle wollte durch Löschung der Verbindungsdaten des E-Mail-Dienstes einem potentiellen Zugriff der Behörden zuvor kommen.[6]

Die meisten Unternehmen wählen den einfacheren Weg und kooperieren. Die Zusammenarbeit von Unternehmen mit Geheimdiensten war schon in den 80er Jahren Usus. Auch in Deutschland kooperierten viele Unternehmen mit „ihren" Geheimdiensten, zum Beispiel Siemens, Rhode & Schwarz und AEG Telefunken.

Eine weitere Parallele zur Inslaw-Verschwörung ist, dass Präsident Obama genau wie die Kanzlerin und ihr Geheimdienstkoordinator Pofalla, oder Innenminister Friedrich, nicht an einer Aufklärung interessiert sind und stattdessen die Öffentlichkeit gezielt irreführen oder mit ignoranten Ausflüchten für dumm verkaufen wollen.

Mit der Art und Weise, wie unsere Regierungen unsere Geheimdienste mit unkontrollierbaren Befugnissen und Überwachungstechnik ausstatten, brechen sie ihren Amtseid, Schaden vom Volk abzuwenden und die Verfassung zu schützen. Sie untergraben die Demokratie und erschaffen den Überwachungsstaat.

## Anmerkungen

1 *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//DE*
2 *http://www.heise.de/tp/artikel/6/6663/1.html*
3 *http://www.theguardian.com/world/2013/jul/02/james-clapper-senate-erroneous*
4 *http://mirror.fem-net.de/CCC/29C3/mp4-h264-HQ/29c3-5338-en-enemies_of_the_state_h264.mp4*
5 *http://www.heise.de/newsticker/meldung/Lavabit-Schliessung-Sogar-meinem-Anwalt-darf-ich-nicht-alles-sagen-1935084.html*
6 *http://www.heise.de/security/meldung/Gruender-von-Silent-Circle-Verbindungsdaten-so-gefaehrlich-wie-Inhalte-1936525.html*

**Klaus Fuchs-Kittowski**

# Ethik und Informatik – Moralität und Historizität

## Zur notwendigen Solidarität mit den Whistleblowern



*Als ich in den 80er Jahren die Leitung der Arbeitsgruppe 1:* Computer and Work *des Technischen Komitees 9:* Wechselbeziehungen zwischen Computer und Gesellschaft *(TC9) der Internationalen Föderation für Informationsverarbeitung (IFIP) übernahm, hatten die Themen* Computer *und* Arbeit *Hochkonjunktur. Denn die Qualität des Arbeitslebens, arbeitsorganisatorische, arbeitspsychologische Probleme im Zusammenhang mit der Automatisierung der Arbeitsprozesse wurden in der Informatik und in der Politik weithin auf nationaler und internationaler Ebene diskutiert. Ein sichtbares Ergebnis dieser Debatten waren die in enger Zusammenarbeit mit den arbeitswissenschaftlichen Instituten (u. a. in Berlin, Zürich und Dresden) erarbeiteten Humankriterien der Arbeits- und Organisationsgestaltung sowie die für die Technikbewertung erarbeitete VDI-Richtlinie 3780.[1] Wir führten zwei internationale Workshops der Working Group 1 des TC9 in Berlin durch.[2, 3] Eine umfangreiche wissenschaftliche Literatur entstand zu den Problemen einer am Menschen orientierten Informationssystemgestaltung (z. B. [4, 5]).*

Unter der Leitung von *Jacques Berleur* war die Arbeitsgruppe 2: *Social Accountability* sehr aktiv. Hier ging es insbesondere um das auch heute besonders aktuelle Thema Datenschutz. Viele der dort entwickelten Ideen und Grundsätze fanden ihren Niederschlag in den nationalen Datenschutzgesetzen – bis hin zur Einführung des Rechts auf *informationelle Selbstbestimmung* in das Grundgesetz der Bundesrepublik. Damit wurde auch das Ausspähen privater Daten aus staatlichem Interesse geregelt und strengen Beschränkungen unterworfen. Nach bestimmter Frist müssen die Daten wieder gelöscht und dem Ausgespähten Kenntnis über den Vorgang gegeben werden. Der Hinweis *Wilhelm Steinmüllers*, der als Mitbegründer der Rechtsinformatik in Deutschland gilt[6] und aktiv in der WG 2 tätig war, dass die vom BND über den Briefverkehr zwischen Ost- und Westdeutschland gewonnen Daten nicht fristgemäß gelöscht wurden, brachten ihn schon damals in große Schwierigkeiten. Ihm wurde dadurch sehr geholfen, dass die IFIP zu ihm stand. Die Informatik hat also schon Erfahrung mit Whistleblowern aus den eigenen Reihen. Erinnert sei insbesondere auch an die große Tat von *David Lorge Parnas*, der aus der Beratergruppe des Starwars-Projekts mit der alarmierenden These austrat:

> *„Software muss getestet werden. Diese Software in den sogenannten Frühwarnsystemen ist nicht getestet. Ein Krieg aus Zufall wird immer wahrscheinlicher!"*

Natürlich war dies ein Affront gegenüber der amerikanischen Regierung, der Parnas sehr verübelt wurde. Für alle in der Friedensbewegung, für uns speziell in der Task-force der IFIP für *Peace and Disarmament*, war jedoch diese fachliche Stellungnahme eines international respektierten Informatikers von größter Bedeutung. Denn die Generalversammlung der IFIP hatte von uns immer wieder eine „nicht politische", „rein fachliche" Stellungnahme zu dem Wettrüsten gefordert, um selbst öffentlich Stellung beziehen zu können. So wie die Bewegung *Ärzte gegen den Atomtod* die fachlich unwiderlegbare These vertrat: „Nach einem Atomschlag gibt es keine Heilung mehr", konnten die InformatikerInnen in Bezug auf die installierten Frühwarnsysteme nun formulieren: „Es gibt keine fehlerfreie Software, eine zufällige Auslösung eines Krieges wird daher immer wahrscheinlicher." Auch hier stand die Frage, was wiegt mehr, die Förderung nationaler Machtinteressen oder das Wohl der Menschheit als Ganzes? Der Bewegung war dann doch der entscheidende Erfolg beschieden, dass die Raketen von der deutsch/deutschen Grenze abgezogen wurden.

Wie stellen wir uns nun heute persönlich, und auch unsere Fachorganisationen, zu den Computerspezialisten *Bradley Manning* und *Edward Snowden*? Es gilt für die Informatikerinnen, für jeden persönlich, und für die Fachorganisationen, Position zu Kriegsverbrechen und zur Ausspähung durch Geheimdienste und damit auch zu den Handlungen von Bradley Manning und Edward Snowden zu beziehen. Es ist doch paradox, wenn offensichtliche Kriegsverbrechen verurteilt und die Ausspähung durch den Geheimdienst NSA empört abgelehnt werden, diejenigen aber, die es auf sich nehmen, diese Geschehnisse aufzudecken, verfolgt und verurteilt werden.

Sie haben in der Tat Verrat gegenüber ihren Auftraggebern und ihrem Vaterland verübt. Verschärfend zum Geheimnisverrat kommt noch dazu, dass sie dies als Soldat bzw. als Geheim-

**Klaus Fuchs-Kittowski**

Prof. Dr. habil. **Klaus Fuchs-Kittowski** (Jahrgang 1934) ist Professor für Informationsverarbeitung. Er war Leiter des Bereichs Systemgestaltung und automatisierte Informationsverarbeitung der Sektion Wissenschaftstheorie und Wissenschaftsorganisation der Humboldt-Universität zu Berlin. Er war Mitglied des TC 9 (Wechselbeziehungen zwischen Computer und Gesellschaft) der Internationalen Föderation für Informationsverarbeitung (IFIP) und langjähriger Chairman der WG 9.1 (Computer und Arbeit) des TC 9 der IFIP und ist Mitglied der Leibniz-Sozietät der Wissenschaften.

dienstler begangen habe. Verräter oder Helden, dies mag für viele schwer zu beurteilen sein. Diese innere Zerrissenheit, in der sich sicher viele befinden, konnte kaum deutlicher werden, als in dem kürzlich in der *Berliner Zeitung* veröffentlichen Interview des Bundesdatenschutzbeauftragten *Peter Schaar*: *„Überwachung gehört ans Licht der Öffentlichkeit"*[7]. Dieses Interview ist ein engagiertes Plädoyer für den Datenschutz. Dem Enthüller Snowden kann er aber nur für kurze Zeit einen Schutzraum anbieten, nur damit er vom Generalbundesanwalt verhört werden kann. Snowden ist ein Verräter, obwohl die Geschichte vielleicht einmal zeigen wird, dass er ein Held ist. Müssen wir wirklich lange warten bis wir die historische Dimension der Enthüllungen Mannings und Snowdens einschätzen können? Die weltgeschichtliche Bedeutung ihrer Entscheidung sollte deutlich genug sein und ihr muss eine höhere Präferenz beigemessen werden, denn sie besaß für die getroffene Entscheidung offensichtlich größere Kraft, als die Verpflichtung zur individuellen Loyalität gegenüber den nationalen Institutionen.

Solange wir uns im Rahmen der gewöhnlichen Moralität bewegen, wird man kaum anders urteilen können, als den Verrat zu verurteilen. Denn es gibt in diesem Rahmen keine Möglichkeit zu seiner Legitimierung. Es gibt keine unmittelbaren moralischen Gründe, die die Weitergabe von hoch brisanten militärischen oder industriellen Geheimnissen an einen anderen Staat legitimieren würden. Und doch stehen viele mutige Amerikaner auf, wie z. B. *Daniel Elsberg*, der Friedensaktivist und ehemalige Whistleblower, durch dessen mutige Enthüllung der sog. *Pentagonpapers* die amerikanische Öffentlichkeit über die reale Situation im Vietnamkrieg informiert wurde. Sie rufen: *„Ich bin Bradley Manning! Lasst die Anklage gegen ihn fallen!"*

Woher kann man die Rechtfertigung für diese m.E. richtige und notwendige Haltung nehmen? Moralische Prinzipien können zwar, wie z. B. beim *kategorischen Imperativ* von *Immanuel Kant* mit dem Anspruch auf Allgemeingültigkeit verbunden werden. Es wird sich aber bald zeigen, dass uns ein solches formales Schema: *„Handle so, dass die Maxime deines Willens jederzeit zugleich als Prinzip einer allgemeinen Gesetzgebung gelten könne"*[8] schon bei einfachen Konflikten kaum weiter hilft. Denn die zunächst einleuchtende Regel muss auf die konkrete Situation bezogen werden, die eben nicht formal behandelt werden kann. Wer sollte dieses besser wissen als die (Rechts-) Informatiker. Wie ist es aber dann erst bei wirklich komplizierten Situationen, die die Welt erschüttern? Wissenschaftler mit entscheidenden Erkenntnissen, Ingenieure mit wichtigen Erfindungen, die für die Gesellschaftsentwicklung relevant werden, und wie wir sehen, auch Informatikspezialisten können offensichtlich in hoch komplizierte Konfliktsituationen geraten. Eine Antwort auf diese uns so bedrängende Frage finden wir bei dem weiteren großen Vertreter der deutschen klassischen Philosophie *Georg Wilhelm Friedrich Hegel*. Er schreibt:

> *„Denn Weltgeschichte bewegt sich auf einem höheren Boden, als der ist, auf dem die Moralität ihre eigentliche Stätte hat, welche die Privatinteressen, das Gewissen der Individuen, ihr eigentümlicher Wille und ihre Handlungsweise ist."*[9]

Hegel verdeutlicht damit, dass der Gesichtspunkt privater Moralität unvollständig und unzureichend ist. Unvollständig, weil er den Kontext der geschichtlichen Situation, von der der Handelnde ein konstitutives Glied ist, unberücksichtigt lässt, und unzureichend, weil die aus der historischen Sachlage entspringenden Entscheidungsgründe ein übergreifendes Allgemeines darstellen, das die ihnen entgegenstehenden moralischen Erwägungen in sich aufhebt.[10]

Der weltgeschichtlichen Bedeutung einer Entscheidung muss eine höhere Präferenz beigemessen werden. Die weltgeschichtliche Situation ist die Grundlage für die individuelle Entscheidung in der Humanitäts- und Freiheitsgewinn als ein für die Menschheit allgemeiner Wert gegenüber den individuellen Werten logisch zwingend die Priorität erhält. Jedes Festhalten an privater Moralität und Negieren des Einsatzes von Menschen (wie der Whistleblower) im Allgemeininteresse für die Gewährleistung der Bürger- und Menschenrechte könnte die Menschheit nur in die Katastrophe führen.

Die Anklage wegen Feindbegünstigung und damit die Todesstrafe für Bradley Manning ist zum Glück schon fallen gelassen worden. Aber ihn erwarten noch bis zu 35 Jahre Gefängnis. Daher muss sich ein Sturm der Entrüstung gegen die Verfolgung und Verurteilung erheben, Solidarität bekundet werde, mit dem Ruf: *„Ich bin Bradley Manning!"* Ständig erfahren wir neue Details zur NSA-Spionage, und auch die BND-Datenweitergabe ist zu klären, und doch muss Edward Snowden, der den bürger- und menschenrechtswidrigen Spähskandal aufgedeckt hat, in seinem Heimatland mit einer hohen Gefängnisstrafe rechnen. Auch für ihn müssen wir Solidarität bekunden, mit dem Ruf: *„Ich bin Edward Snowden!"*

## Anmerkungen

1 *Friedrich Rapp (Hrsg.): Normative Technikbewertung – Wertprobleme der Technik und die Erfahrungen mit der VDI-Richtlinie 3780*
2 *P. Docherty, K. Fuchs-Kittowski, P. Kolm, I. Mathiassen (Editors): System Design for Human Development and Productivity: Participation and Beyond, North-Holland, Amsterdam, 1986*
3 *P. Van Den Besselaar, A. Clement, P. Järvinen (Editors): Information System, Work and Organization Design, North-Holland, Amsterdam, 1991*
4 *Klaus Kornwachs, Information und Kommunikation – Zur menschengerechten Technikgestaltung, Springer-Verlag,, Berlin, New York, 1993*
5 *Peter Brödner, Der überlistete Odysseus – Über das zerrüttete Verhältnis von Mensch und Maschine, edition sigmar, Berlin, 1997*
6 *Wilhelm Steinmüller, Informationstechnologie und Gesellschaft – Einführung in die Angewandte Informatik, Wissenschaftliche Buchgesellschaft, Darmstadt, 1993*
7 *Peter Schaar, Überwachung gehört ans Licht der Öffentlichkeit, Berliner Zeitung, Freitag den 2. August 2013, S.6*
8 *Immanuel: Kant Kritik der praktischen Vernunft, Riga 1788, S. 54.*
9 *Georg Wilhelm Friedrich Hegel, Vorlesungen über die Philosophie der Geschichte, Werke, Suhrkamp Band 12, Frankfurt am Main 1970, S. 40 und 90f.*
10 *Hans Heinz Holz, Wissenschaft und Verantwortung – Historizität und Moralität, in: Ethik in der Wissenschaft – Die Verantwortung der Wissenschaftler – zum Gedenken an Klaus Fuchs, Abhandlungen der Leibniz-Sozietat, trafo Verlag der Wissenschaften, Berlin, S. 151-159*

**Die internationale Zivilgesellschaft**

# Brief an Präsident Obama

Präsident Barack Obama
Das Weiße Haus
Washington, D.C.
Vereinigte Staaten von Amerika

CC:
Generalstaatsanwalt Eric Holder
Außenminister John Kerry

**Sehr geehrter Präsident Obama,**

wir schreiben Ihnen als Organisationen, die sich weltweit für die Freiheit des Wortes und der Medien einsetzen, um unsere große Sorge auszudrücken, die wir im Hinblick auf die Reaktion der US-Regierung gegenüber den Handlungen des Whistleblowers Edward Snowden empfinden. Wir fordern Sie dazu auf, umgehend Maßnahmen zum Schutz von Whistleblowern und Journalisten zu ergreifen.

Edward Snowdens jüngste Enthüllungen haben eine dringend notwendige und längst überfällige öffentliche Debatte über die akzeptablen Grenzen der Überwachung in einem demokratischen Staat entfacht; eine Debatte, deren Aufkommen Sie am 5. Juni begrüßt haben. Die Enthüllungen stellten die Legitimation der geheimen Verfahren des *Foreign Intelligence Surveillance Court* und der geheimen *Congressional intelligence committees* als geeignete Foren, um die fundamentalen Menschenrechte von Amerikanern und Menschen auf der ganzen Welt zu bestimmen, in Frage. Die Enthüllungen dienen ohne Zweifel dem öffentlichen Interesse, einschließlich der Tatsache, dass sie den Anstoß für ähnliche Debatten in Ländern rund um den Globus liefern.

Wir sind deshalb darüber bestürzt, dass Anklage gegen Snowden erhoben wurde, die sich teilweise auf das vage und überholte Spionagegesetz von 1917 stützt.

Aussagen des Außenministeriums, dass Snowden schlicht aufgrund der Art der erhobenen Anklagepunkte kein Whistleblower sei, widersprechen eindeutig internationalen Standards der freien Information und Meinungsäußerung. Versuche, Snowdens Bewegungsfreiheit einzuschränken, sein Recht auf die Beantragung von Asyl zu behindern, einschließlich der Annullierung seines Reisepasses, und andere Formen von Vergeltungsmaßnahmen verletzen ebenfalls Pflichten der Vereinigten Staaten, die sich aus internationalem Recht ergeben.

Außerdem sind wir besorgt, dass die Anklage gegen Snowden keinen Einzelfall darstellt, sondern dass es in Ihrer Amtszeit eine beispiellose Zahl von Verfolgungen von Whistleblowern gibt, sowie intensive Untersuchungen, deren Ziel die Entlarvung der Quellen von Journalisten ist, die über Angelegenheiten von öffentlichem Interesse berichten. Diese Tendenz der US-Regierung, Informationsflüsse obsessiv zu kontrollieren, und die Aversion gegen öffentliche Diskurse sind undemokratisch und unhaltbar im digitalen Zeitalter.

Wir sind der Meinung, dass diese Handlungen einen gefährlichen Präzedenzfall in der Frage des Schutzes von Whistleblowern und Journalisten weltweit geschaffen haben. Wie Ihnen bewusst ist, sehen sich Whistleblower häufig Anklagen gegenüber, wenn sie Informationen an die Öffentlichkeit geben, die Regierungen in akute Verlegenheit bringen – wodurch vom aufgedeckten Fehlverhalten abgelenkt wird. In ähnlicher Weise werden Journalisten für die Veröffentlichung der enthüllten Informationen angegriffen. Wir sind in ernster Sorge, dass Regierungen sich auf das US-Beispiel berufen werden, um Angriffe auf Whistleblower und Journalisten zu rechtfertigen, die sich selbst einem erheblichen Risiko ausgesetzt haben, um das Fehlverhalten von Regierungen, Korruption und andere Gefahren für die Gesellschaft zu aufzudecken.

Die USA besitzen eine lange Tradition, die wichtige Rolle, die Whistleblower in Demokratien spielen, anzuerkennen, beginnend mit einem Gesetz Abraham Lincolns von 1863, dem *False Claims Act*. Obwohl der *Whistleblower Protection Act* von 2009 auf der Grundlage dieser Schutzmaßnahmen entwickelt wurde, schließt er Enthüllungen von Informationen der nationalen Sicherheit oder des Geheimdienstes aus diesem Schutz aus, selbst wenn diese von öffentlichem Interesse sind. Obschon die kürzlich veröffentlichte *Presidential Policy Directive/PPD-19* zum *„Schutz von Whistleblowern mit Zugang zu Geheiminformationen"* und Generalstaatsanwalt Eric Holders Anleitung zum Schutz der Privilegien von Reportern positiv

zu bewerten sind, stellen sie kein bindendes Gesetz und somit keinen juristischen Schutz dar für Whistleblower und Journalisten, die Enthüllung von Informationen zu verteidigen suchen. Stärkere juristische Schutzmaßnahmen werden daher in diesem Bereich benötigt.

Wir fordern Ihre Regierung dazu auf, folgende Schritte zu unternehmen:

- Lassen Sie alle Anklagepunkte gegen Edward Snowden rechtskräftig fallen.
- Stellen Sie die Gültigkeit von Edward Snowdens Reisepass unverzüglich wieder her und beenden Sie die Versuche, sein Recht auf die Beantragung von Asyl in einem Land seiner Wahl zu behindern.
- Initiieren Sie eine öffentliche Anhörung wegen der Aktivitäten der National Security Agency (NSA).
- Beauftragen Sie das Justizministerium, alle Anweisungen des Foreign Intelligence Surveillance Act freizugeben und zu veröffentlichen.
- Verpflichten Sie den Kongress, den Whistleblower Protection Act zu erweitern und eine Reform des Spionagegesetzes anzustreben, um sicherzustellen, dass es angemessene und juristisch bindende Schutzmaßnahmen für Whistleblower gibt, die Informationen der nationalen Sicherheit und des Geheimdienstes enthüllen.
- Unterstützen Sie weiterhin die Anpassung eines starken und robusten media shield law durch den Kongress mit engen Ausnahmeregelungen für Informationen, die die nationale Sicherheit betreffen.

August 2013

Mit freundlichen Grüßen,

***Rund 160 Organisationen aller Kontinente haben den offenen Brief an Präsident Obama unterzeichnet***

Quelle: http://www.article19.org/resources.php/resource/37194/en/#german

## Wissenschaft und Frieden 3-2013 – *Jugend unter Beschuss*


*Jugend unter Beschuss*. Unter diesem Oberbegriff befasst sich W&F in seiner August-Ausgabe mit dem Lebensalter von der Grundschulzeit bis zum jungen Erwachsenenalter. Kinder sind Krieg und Gewalt in der Regel als Opfer ausgesetzt, allerdings verschwimmen immer wieder die Täter-Opfer-Grenzen, wenn Kinder selbst gewalttätig werden oder als Kindersoldaten für Zwecke der Kriegsmaschinerie missbraucht werden. Die Chancen, sich aktiv und kreativ für ein friedlich(er)es Leben einzusetzen, wachsen mit fortschreitendem Alter – der Grundstein für solches Engagement wird aber ebenfalls oft in der Kindheit gelegt. Einige Aspekte davon beleuchten die Artikel im Schwerpunkt.

Joanna Schürkes: *Junge Männer und der Krieg – Youth Bulge im sicherheitspolitischen Diskurs*; Annika Henrizi: *Jugend in Bagdad – Handlungsmöglichkeiten in virtuellen und städtischen Räumen*; Sara Seifried: *Soziales leben guatemaltekischer Jugendlicher in Zeiten der Gewalt*; Rita Schäfer: *Jugendliche und Homophobie – Hassgewalt in Südafrika*; Simon Moses Schleimer: *Die Remigration kurdischer Jugendlicher in den Nordirak*; Kathin Jonkmann und Ingrid Bilstein: *Wie der Wehrdienst die Persönlichkeit beeinflusst*; Dieter Lünse: *Gewaltprävention in Schulen*.

Weitere AutorInnen wenden sich den Friedensverhandlungen im türkisch-kurdischen Konflikt, der Suche nach Friedenslösungen in Afghanistan, der (Nicht-) Korrelation von Antisemitismus und Israelkritik sowie friedenspolitischen Forderungen zur Bundestagswahl 2013 zu.

**Wissenschaft & Frieden**, Nr. 3/2013 **Jugend unter Beschuss**, € 7,50 plus Porto.

W&F erscheint vierteljährlich, dreimal im Jahr liegt W&F ein 12- bis 20-seitiges Dossier bei. Jahresabo 30 €, ermäßigt 20 €, Förderabo 60 €, Ausland 35 €, ermäßigt 25 €.

*Neu: W&F erscheint seit der 1-2013 nicht nur gedruckt, sondern auch in digitaler Form – als PDF und ePub. Das Abo kostet für Bezieher der Printausgabe zusätzlich 5 € jährlich – als elektronisches Abo ohne Printausgabe 20 € jährlich.*
Bezug: W&F, Beringstraße 14, 53113 Bonn,
E-Mail: *buero-bonn@wissenschaft-und-frieden.de*,
*www.wissenschaft-und-frieden.de*

# Schwerpunkt „Informatik und Bildung“



**Iris Bockermann, Nadine Dittert, Heidi Schelhowe**

## Akademische Medienkompetenz: Ein Beispiel aus der universitären Lehre

*Der anhaltende Hype um MOOCs (Massive Open Online Courses[1]) und damit einer Art Neuauflage der eLearning-Euphorie an deutschen Hochschulen ist interessant. MOOCs haben im Hinblick auf ihre Konzeption, Umsetzung und Qualität des Bildungsangebots im Hochschulbereich nicht nur Befürworter_innen (vgl. Schulmeister 2013)[2], dennoch erreichen sie mit ihrem Bildungsangebot zeit- und ortsunabhängig oft erstaunlich viele Menschen (in China gibt es z. B. gegenwärtig ein MOOC mit 500.000 Teilnehmer_innen, betreut von 12 Tutor_innen), die sich eigenständig, vermutlich nicht selten intrinsisch motiviert, bilden und bilden wollen, und dies unabhängig von formalen Abschlüssen und Zulassungsvoraussetzungen.*

In MOOCs wie im klassischen eLearning werden Digitale Medien eher instrumental für Bildungszwecke genutzt. Plattformen verstecken in der Regel hinter Benutzungsoberflächen den prozessualen, verarbeitenden Charakter und die Komplexität, die hinter (Hardware und) Software stecken, um eine einfache Benutzung und einen unkomplizierten Zugriff auf Inhalte zu ermöglichen. Das ‚Instrument‘ selbst ist ‚transparent‘, bleibt im Lernprozess im Hintergrund.

In unserem Beitrag möchten wir demgegenüber der Frage nachgehen, wie das Medium selbst sichtbar und verstehbar gemacht werden kann, wie ein auf das Medium selbst gerichtetes Interesse hergestellt und in diesem Sinne ‚akademische Medienkompetenz‘ zum Thema gemacht werden kann. Unser Anliegen ist es, die automatischen Prozesse und den Charakter technologischen Denkens begreifbar zu machen. Es stünde aus unserer Sicht einer akademischen Einrichtung gut an, Digitale Medien nicht nur zu nutzen, sondern auch Reflexionsprozesse über den Charakter und die Wirkungen neuer elektronischer ‚Werkzeuge‘ im wissenschaftlichen Prozess zu initiieren. Wir wollen dafür ein Beispiel aus einer Lehrveranstaltung zeigen, die sich an Studierende der Informatik, der Digitalen Medien und an Studierende mit dem Ziel Lehramt richtet.

### Ein Lehrkonzept „Digitale Medien in der Bildung“

Lehre an Universitäten und Hochschulen befindet sich in Bewegung. Nach einer Fokussierung auf Forschung und einer eher geringeren Reputation von Lehre in der deutschen Hochschullandschaft scheint heute doch wieder vermehrt nach einer Balance und einer stärkeren Gewichtung von Lernprozessen gesucht zu werden. An unserer Universität, der Universität Bremen, werden – nicht zuletzt auch befördert durch kritische Stimmen gegen eine reine Forschungsexzellenz sowie im Zuge des Qualitätspakts Lehre – wieder verstärkt Diskussionen um neue Konzepte für die Lehre geführt. Hochschuldidaktische Weiterbildungsangebote erfahren hohen Zuspruch, ein Magazin für Lehre und Studium wird im Herbst mit einer ersten Ausgabe starten und ein Leitbild für Lehre wird gegenwärtig diskutiert.

Digitale Medien sind nicht losgelöst von den generellen Vorstellungen und Leitbildern für Lehre und Studium an einer Universität zu sehen, vielmehr müssen sie sich in solche Zielvorstellungen einordnen. Im Folgenden möchten wir das Lehrkonzept für die Lehrveranstaltung *Digitale Medien in der Bildung* an der Universität Bremen vorstellen, in dem Informatik mit Bildungsanliegen verschränkt wird und mit dem die Rolle von IuK-Technologien als Bildungsmedien gezeigt werden soll.

Die interdisziplinäre Lehrveranstaltung richtet sich sowohl an Studierende aus der Informatik und aus den Digitalen Medien, die sich für Bildungsthemen interessieren, wie auch an Studierende mit dem Ziel Lehramt und Studierende anderer pädagogischer Fachrichtungen, die die Praxis und den Nutzen Digitaler Medien für Lernzusammenhänge kennen lernen wollen. Moderne Forschungskonzepte der Mensch-Maschine-Interaktion wie auch aktuelle pädagogische Konzepte spielen hier eine besondere Rolle und sollen von den Studierenden nicht nur theoretisch begriffen, sondern auch handelnd erfahren und angewandt werden. Didaktisch orientieren wir uns dabei im Rahmen des Kurses an Prinzipien des forschenden Lernens, das für die Profilbildung in der Lehre an der Universität Bremen eine besondere Rolle spielt (Huber et al. 2013). Im Rahmen der Lehrveranstaltung, die daneben eine zweistündige begleitende Vorlesung umfasst, werden, wenn möglich, interdisziplinäre Teams aus den drei Studienrichtungen gebildet, die dann ein Medienbildungsprojekt eigenständig konzipieren, prototypisch umsetzen und möglichst auch praktisch erproben.

Herangeführt werden die Studierenden an die theoretischen Grundlagen der *Digitalen Medien* im Hinblick auf ihre Gestaltung und Nutzung im Bildungskontext. Es wird beleuchtet, inwieweit *Digitale Medien* unsere Bildungsprozesse verändern und verändert haben, zudem wird eine Vorstellung von den Potenzialen der *Digitalen Medien* vermittelt. Das Design von Bildungsmedien spielt sowohl in den theoretischen wie auch methodischen Implikationen eine Rolle. Es werden Grundlagen zur Einbettung von *Digitalen Medien* in Bildungskontexte thematisiert, sowohl theoretisch wie praktisch-experimentell. Die Bedeutung von Lerntheorien für die Gestaltung von Software und von Lernarrangements soll verstanden werden. Moderne und

aktuelle Technologien wie Tangibles, Body Interaction, FabLab-Maschinen, Mobile Technologie oder Web 2.0 sind Gegenstand und sie werden von den Studierenden in ihren Potenzialen für das Lernen exploriert und bewertet.

Die projektorientierte und interdisziplinäre Zusammenarbeit in Arbeitsgruppen ist das Kernelement der Lehrveranstaltung. Die Kooperation zwischen unterschiedlichen Disziplinen, informatischer, gestalterischer und erziehungswissenschaftlicher Ausrichtung ist wesentlich, um der Komplexität der Aufgabe gerecht zu werden, um unterschiedliche Sicht- und Denkweisen sowie Methoden der jeweiligen Fachkulturen kennen zu lernen und zu erproben, um den gleichgewichtigen und teamorientierten Dialog miteinander führen zu können, um zu lernen einander in der jeweiligen Fachlichkeit zu verstehen bzw. sich verständlich machen zu können. Gerade die im Bologna-Prozess geforderte Orientierung auf Kompetenzen statt auf Lernstoff kann sich in der Projektarbeit und im forschenden Lernen entwickeln.

## Die Rolle digitaler Medien und von Medienbildung

Schon seit einigen Jahren sehen die Bildungspläne für die allgemeinbildenden Schulen in den verschiedenen Bundesländern vor, dass Medienbildung und kritische Medienkompetenzförderung fächerübergreifend und altersangemessen unterrichtet wird. Trotz des Bildungsauftrages der Kultusministerkonferenz (Kultusministerkonferenz 1995: 2012), der in den Ländern konzeptionell unterschiedlich angelegt ist und umgesetzt wird, lässt der Status quo der Medienbildung in allen Schulformen zu wünschen übrig. Medien werden von Lehrkräften zwar zunehmend eingesetzt, aber die Reflexion über die Medien, wie sie zur Medienbildung gehört, bleibt unzureichend oder rein belehrend und theoretisch. Insbesondere fehlt es aber auch häufig am Bezug zu aktuellen Technologien, wie sie von Kindern und Jugendlichen als ‚Early Adopters' im Alltag genutzt werden unter einer medienbildenden Perspektive. Die Hoffnung, dass sich dies mit jüngeren Lehrergenerationen deutlich verändert, hat sich (noch) nicht erfüllt. Vielmehr scheint auch für jüngere Lehrerinnen und Lehrer zweifelhaft, ob und inwiefern digitale Medien einen Bildungswert besitzen können (Bockermann 2012).

Der Universität kommt als Einrichtung, an der angehende Lehrkräfte ausgebildet werden, im Hinblick auf Medienbildung eine Schlüsselrolle zu. Dies wird für die Lehramtsausbildung heute in der Regel zwar gefordert (z. B. BMBF 2009), findet jedoch oft keinen Platz im übervollen Pflicht-Curriculum. Kammerl und Ostermann (Kammerl und Ostermann 2010) bezeichnen die geringe Rolle und Präsenz der digitalen Medien in der Schule, die eher distanzierte Haltung der Lehramtsstudierenden zu digitalen Medien und die geringe Bedeutung der Medienbildung in der Ausbildung von Studierenden als Teufelskreis der Medienbildung, den es zu durchbrechen gilt. Noch deutlich weniger im Bewusstsein und noch weniger präsent in den Lehrangeboten ist jedoch bis heute die ‚akademische Medienkompetenz' als Schlüsselkompetenz generell für akademisch gebildete Bürgerinnen und Bürger wie auch hochqualifizierte Arbeitskräfte der sogenannten Wissensgesellschaft, auch wenn hier die Hochschulrektorenkonferenz vor Kurzem einen Anfang gemacht hat (HRK 2012).

**Iris Bockermann, Nadine Dittert, Heidi Schelhowe**

**Iris Bockermann** ist Lektorin an der Universität Bremen und bildet insbesondere Lehramtsstudierende aller Schulstufen und Fächer, aber auch Studierende der digitalen Medien und der Informatik in der Entwicklung und im Einsatz digitaler Medien im Bildungskontext aus. Zudem ist sie externe Evaluatorin im Forschungsprojekt „Perspektive 2.0 – Beruflich einsteigen mit kritischen Medienkompetenzen", gefördert durch das BMBF. Ihre Dissertation „Wo verläuft der Digital Divide im Klassenraum? Lehrerhandeln und digitale Medien" (2012) befasst sich mit dem besonderen Verhältnis von Lehrkräften zu digitalen Medien im Bildungskontext.

**Nadine Dittert** ist wissenschaftliche Mitarbeiterin in der AG *Digitale Medien in der Bildung* an der Universität Bremen. Ihr Hauptforschungsgebiet sind Bildungsanwendungen mit be-greifbaren Technologien. Die Diplom-Informatikerin entwirft, plant und konzipiert Technologie-Workshops und setzt diese mit verschiedenen Zielgruppen um. Ihr besonderes Forschungsinteresse bezieht sich auf Tangibles für Sportanwendungen mit Kindern und Jugendlichen.

**Heidi Schelhowe** ist Professorin für digitale Medien in der Bildung in der Informatik und Konrektorin für Lehre und Studium an der Universität Bremen. Mit ihrer interdisziplinär zusammengesetzten Arbeitsgruppe *dimeb* entwickelt sie Hardware und Software für Bildungskontexte, gestaltet Lernumgebungen aus pädagogisch-didaktischer Sicht und betreibt empirische Forschung im Bereich Bildung und digitale Medien. Ein weiterer Schwerpunkt ist Medienkompetenz.

Wir sind an der Universität Bremen in der glücklichen Lage, dass wir aus einer interdisziplinär zusammengesetzten, sich über Informatik- und Erziehungswissenschaft erstreckende Arbeitsgruppe heraus ein Angebot entwickeln können, das sich sowohl aus der Informatik als auch aus den Erziehungswissenschaften speist. Angesichts der tiefgreifenden Durchdringung und Einschreibung digitaler Medien in alle gesellschaftlichen Bereiche kommt der Technologieentwicklung, aber auch der Medienbildungsarbeit eine besondere Rolle zu, die weit über die intuitive Bedienbarkeit und Nutzung der digitalen Medien als Werkzeug zur Erleichterung bzw. Übernahme von Routinearbeiten hinausgeht. Digitale Medien sind gesellschaftlicher Handlungsraum und haben sich eingeschrieben in unsere Sichtweisen auf die Welt, strukturieren unser Denken und Handeln, berühren unsere Orientierung in der Welt.

Die Studierenden lernen in unserer Lehrveranstaltung neuartige, innovative Technologien und Bereiche der digitalen Medien kennen, die wir in der Forschung gerade erst erproben und entwickeln. Diese können und sollen sie dann selbst in aktiver Aneignung auf ihre Eignung in Bildungszusammenhängen hin experimentell erproben und bewerten. Die Studierenden lernen, die Entwicklung und den Einsatz von Software sinnvoll auf Lernen zu beziehen, diese Technologien aber auch im Hinblick auf ein Bildungsanliegen zu prüfen und die Technologien darauf zu beziehen.

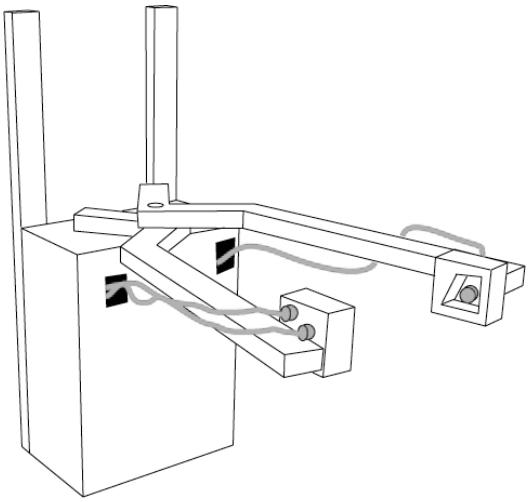
In Workshops werden zum Beispiel innovative *Tangibles* in ein didaktisches Konzept eingebunden (Dittert et al. 2008). Der handlungsorientierte Ansatz baut auf konstruktionistischen Lerntheorien (Papert 1980) auf und lässt Studierende zu Entwickler_innen und Designer_innen einer persönlich als relevant empfundenen Anwendung werden. Dabei werden zugrunde liegende technische Funktionsweisen und Programmierung begreifbar. Wir verwenden dafür sogenannte *Construction Kits* – Baukästen, die klassische Konstruktionsmaterialien und technische Komponenten miteinander verbinden. Bekannte Stoffe wie Holz, Styropor, Pappe, Stoffe, Wolle etc. werden mit Sensoren, Aktuatoren und Mikrokontrollern verbunden, programmiert und es entstehen so „lebendige" Artefakte. Auf diese Weise entwickeln Studierende beispielsweise zum Lernen anregende Stofftiere, interaktive Erste-Hilfe-Kästen oder Musik-Lerntische.

*Construction Kits* lassen sich als be-greifbare Interfaces in Lernszenarien einbetten. Die Herausforderung besteht darin, Raum und Möglichkeiten so zu gestalten, dass der pädagogisch-didaktische Wert dieser Medien entfaltet wird. Dies ermöglicht es zunächst, die Entwicklungssicht einzunehmen und dabei grundlegende informatische Prozesse zu durchlaufen und zu verstehen. Mittels einer einfach zugänglichen Programmierumgebung wird auch Studierenden außerhalb der digitalen Medien und der Informatik ein Zugang zur Programmierung eröffnet. Damit werden Prozesse formal abgebildet und erhalten wiederum im Objekt eine konkrete Form. Sie lassen sich verifizieren und wenn nötig verändern und anpassen. Neben der Formalisierung bietet die Entwicklungsperspektive Einblick in die grundlegende Funktionsweise von digitalen Medien mit dem Computer als Kern. Das eigenständige Konstruieren mit Sensoren, Aktuatoren und Mikrokontrollern erlaubt einen aktiven Einblick im Unterschied zur schlichten Nutzung solcher Systeme. Im begleitenden didaktischen Konzept legen wir Wert darauf, Parallelen zu Systemen zu ziehen, die die Studierenden aus ihrem Alltag kennen. Im Konstruktionsprozess nehmen die Studierenden die Design- und

*Ein von Studierenden entwickelter Sprachlernpanda*

*Ein von Studierenden entwickelter Sprachlernpanda mit Vokabelelementen*


*Vokabelelemente für den Panda*



*Skizze des Inneren des Pandas*

Entwicklungssicht wie aber auch die Perspektive des Lernens ein. Sie erleben die Verantwortung, die die Konstruktion mit sich bringt, und erfahren etwas über die Möglichkeiten der Technologiegestaltung. Dies verstehen wir als eine wesentliche Komponente von Medienkompetenz (BMBF 2009): Wer hat welches Produkt zu welchem Zweck entwickelt? Was lässt sich damit machen? Welche Daten gebe ich preis, wenn ich das Produkt benutze? Um Fragen dieser Art zu evozieren, ist ein didaktischer Rahmen nötig, den wir in der Lehrveranstaltung schaffen. Wir laden Studierende dazu ein, Entwickler_innen zu werden und einen kritischen Blick auf die digitalen Medien zu werfen.

Durch MOOCs steht das Wissen, das an Universitäten und Bildungseinrichtungen vermittelt wird, für neue Zielgruppen jenseits formaler Abschlüsse offen; es können unterschiedliche Bevölkerungsgruppen an akademischen Bildungsangeboten teilnehmen. Die Quote derjenigen, die solche Kurse erfolgreich abschließen, ist mit 5-10 % sehr gering und trotzdem nicht zu vernachlässigen. Auf der anderen Seite sind die Abbruchquoten so hoch, dass gemeinsames Arbeiten in der Regel schwierig ist und wenig stabile Diskussions- und Arbeitsprozesse verspricht.

Für die Organisation von Lernprozessen an Hochschulen genügt es aus unserer Sicht nicht, das Medium bereitzustellen. Es kommt darauf an, das Medium selbst in den Blick zu nehmen und dieses als ein zu ‚Öffnendes' zu betrachten. Dazu bedarf es geeigneter Rahmungen, die Anwender_innen in die Lage versetzen, mit diesem Medium kritisch umzugehen, es durch aktives Mitgestalten in seinem Potential für die eigenen Bedürfnisse auszuschöpfen und die Eigenverantwortung wahrzunehmen. So sind ‚Citizenship' (neben der Employability auch ein wichtiges Ziel der Bologna-Reform), Autonomie und selbstbestimmtes Handeln auch gegenüber den Computermedien, die unsere Gesellschaft prägen, zu erreichen. Sich *nur* neuen Trends anzupassen und sich in mediale Wellen hineinziehen zu lassen, ist einer akademischen Einrichtung und ihren Lehrkonzepten nicht angemessen. Ihre Absolvent_innen sollen Verantwortung in der Gesellschaft auch für die Einführung und Bewertung digitaler Medien übernehmen. Gerade die neueren Entwicklungen im Zuge der Diskussion um PRISM und die durch viele Bevölkerungsschichten von unten getragene Crypto-Bewegung zeigen eindrücklich, dass Menschen sehr wohl bereit sind, sich auf den Weg zu machen, um z. B. auch die Kontrolle über die eigenen Daten wieder zu gewinnen oder zu behalten.

## Referenzen


*BMBF (2009): Bericht der Expertenkommission des BMBF zur Medienbildung. Kompetenzen in einer digital geprägten Kultur. Medienbildung für die Persönlichkeitsentwicklung für die gesellschaftliche Teilhabe und für die Entwicklung von Ausbildungs- und Erwerbsfähigkeit. Unter Mitarbeit von Heidi Schelhowe, Silke Grafe, Bardo Herzig, Jochen Koubek, Horst Niesyto et al., 12.03.2009. Online verfügbar unter http://www.bmbf.de/pub/kompetenzen_in_digitaler_kultur.pdf*

*Bockermann, Iris (2012): Wo verläuft der Digital Divide im Klassenraum? Lehrerhandeln und Digitale Medien. Bremen. Online verfügbar unter http://elib.suub.uni-bremen.de/edocs/00102499-1.pdf, zuletzt aktualisiert am 01.03.2012, zuletzt geprüft am 10.01.2013.*

*Dittert, Nadine; Dittmann, Katharina; Grüter, Torsten; Kümmel, Anja; Osterloh, Anja; Reichel, Milena; Schelhowe, Heidi; Volkmann, Gerald & Zorn, Isabel (2008): Understanding Digital Media byconstructing intelligent artefacts. In Proceedings of ED-MEDIA'08.*

*HRK 2012 Hochschule im digitalen Zeitalter: Informationskompetenz neu begreifen – Prozesse anders steuern. Göttingen. Online verfügbar unter http://www.hrk.de/uploads/media/Entschliessung_Informationskompetenz_20112012.pdf*

*Huber, Ludwig; Kröger, Margot; Schelhowe, Heidi (Hg.) (2013): Forschendes Lernen als Profilmerkmal einer Universität. Beispiele aus der Universität Bremen. Bielefeld: UVW Univ.-Verl (Motivierendes Lehren und Lernen in Hochschulen, 16).*

*Kammerl, Rudolf; Ostermann, Sandra (2010): Medienbildung – (k)ein Unterrichtsfach? Eine Expertise zum Stellenwert der Medienkompetenzförderung in Schulen. Unter Mitarbeit von Sandra Ostermann und Rudolf Kammerl. Hamburg. Online verfügbar unter http://www.ma-hsh.de/cms/upload/downloads/Medienkompetenz/ma_hsh_studie_medienbildung_web.pdf*

*Kultusministerkonferenz (1995): Erklärung zum Thema Medienpädagogik in der Schule. Düsseldorf. Online verfügbar unter http://www.nibis.de/nli1/chaplin/portal%20neu/portal_start/start_grundsaetze/materialien_grundsaetze/3kmk95.pdf*

*Kultusministerkonferenz (2012): Medienbildung in der Schule. Beschluss der Kultusministerkonferenz vom 8. März 2012. Online unter: http://www.kmk.org/fileadmin/veroeffentlichungen_beschluesse/2012/2012_03_08_Medienbildung.pdf*

*Papert, Seymour (1980): Mindstorms: Children, Computers, and Powerful Ideas. Basic Books. New York*

*Schulmeister, Rolf: Der Computer enthält in sich ein Versprechen auf die Zukunft. In: Ullrich Dittler, Jakob Krameritsch, Nicolae Nistor, Christine Schwarz, Anne Thillosen (Hrsg.): E-Learning: eine Zwischenbilanz : kritischer Rückblick als Basis eines Aufbruchs (2009). Münster [u. a.]: Waxmann.*

*Schulmeister, Rolf (2013): As Undercover Student in MOOCs. http://lecture2go.uni-hamburg.de/konferenzen/-/k/14447*


## Anmerkungen

1 MOOC-Ausschreibung und Bekanntgabe der Gewinner_innen von Diversity und dem Stifterverband für die Deutsche Wissenschaft: https://moocfellowship.org/, weitere in Deutschland und international bekannte MOOCs sind Coursera: https://www.coursera.org; Udacity: https://www.udacity.com/; edX: https://www.edx.org

2 Neben vielen Befürworter_innen gibt es zu bestehenden MOOCs auch kritische Untersuchungen und Einordnungen, hier exemplarisch Schulmeister: http://lecture2go.uni-hamburg.de/konferenzen/-/k/14447

*Der Panda fordert auf Chinesisch auf: „Gib mir bitte einen Apfel" und wartet auf das passende Element. Bei richtiger Zuordnung sagt er „ja" auf Chinesisch, sonst wiederholt er seine Bitte.*

**Berthold Hoffmann**

# Wie studiert man im Norden von Kamerun Informatik?

*Ein Erfahrungsbericht über Lehraufenthalte an einer neu gegründeten Universität im äußersten Norden Kameruns.*



Das zentralafrikanische Land Kamerun ist mit 475.000 km² so groß wie Deutschland, die Schweiz und Österreich zusammen. Die Bevölkerung von ca. 20 Mio. wächst jährlich um 2 %; 60 % der Einwohner sind jünger als 25 Jahre. Offiziell ist das Land eine parlamentarische Demokratie, de facto regiert der Präsident Paul Biya es seit 30 Jahren ohne nennenswerte Opposition. Trotz seiner ca. 250 Ethnien und der religiösen Vielfalt (70 % Christen, 20 % Muslime und 10 % Animisten) gilt das nach französischem Muster zentralistisch regierte Land als weitgehend stabil, wenn auch korrupt. Dank eines ausgebauten Bildungssystems wird eine Alphabetisierungsrate von 76 % erreicht [1]. An acht Universitäten wird eine Hochschulausbildung angeboten – das ist in Zentralafrika keine Selbstverständlichkeit.

Die *Région Extrème Nord* ist etwa so groß wie Nordrhein-Westfalen und hat ca. drei Mio. Einwohner. Sie liegt am Rand der Sahelzone, und die Bevölkerung ist hier noch ärmer als im Landesdurchschnitt; außerhalb der wenigen Städte herrscht Subsistenzwirtschaft. Der Anteil der Muslime ist größer als im Rest des Landes (ca. ein Drittel), und der Islam ist im öffentlichen Leben sehr präsent.

Die Hauptstadt Maroua ist ein Zentrum für Handwerk und Handel bis in den Tschad und den Norden Nigerias. Die Universität Maroua wurde 2008 mit dem ausdrücklichen Ziel gegründet, in Forschung und Lehre regionale Schwerpunkte zu setzen. Sie ist noch im Aufbau begriffen. Derzeit existieren erst zwei Fakultäten: In der *Ecole Normale Supérieure* (ENS) für Lehrerausbildung gibt es ca. 5.000 Studierende, und ca. 2.000 am *Institut Supérieur du Sahel* (ISS), an dem Ingenieure ausgebildet werden sollen. Später sollen noch weitere Fakultäten folgen, z. B. für Geisteswissenschaften, Recht und Medizin. Im Endausbau soll die Universität 50.000 Studierende haben.

Die Studienprogramme gliedern sich in drei Zyklen, in Anlehnung an das französische Hochschulsystem: Sie beginnen mit einer dreijährige *Licence* (Bachelor), darauf folgt ein zweijähriges Master-Programm und ggf. eine dreijährige Promotionsphase.

Die Namen der Fachbereiche im ISS künden vom Anspruch, sich mit den Belangen der Region zu beschäftigen. Neben Ackerbau und Viehzucht gibt es Umweltwissenschaften, Stadtplanung, Textilien und Bekleidung, Wasserkraft und eben auch Informatik und Telekommunikation. Die regionale Bedeutung dieses Fachbereichs wird darin gesehen, dass Funknetze für Telefonie und Internet für die Infrastruktur eher realisierbar sind als kabelgebundene (das gilt in vielen ländlichen Gebieten Afrikas), während die Informatik als Hilfsdisziplin für andere Fächer des ISS gebraucht wird.

Im Fachbereich werden drei Studienrichtungen angeboten: Telekommunikation sowie Informatik mit den Schwerpunkten Systemanalyse und Netze. Die gemeinsame Basis umfasst in vier Semestern Inhalte der Informatik und der Elektrotechnik zu etwa gleichen Teilen – dazu kommt noch Mathematik (Analysis 1-3). In den letzten zwei Semestern verschieben sich dann die Anteile an Elektrotechnik und Informatik je nach Schwerpunkt. Auf die *Licence* bauen Master-Programme in Telekommunikation und Informatik auf, wobei in der Informatik im dritten (insgesamt neunten) Semester zwischen den Schwerpunkten Rechnernetze und Softwaretechnik gewählt werden kann. Danach kann sich ein Graduiertenstudium von drei Jahren mit dem Ziel der Promotion anschließen [2].

Die ca. 300 Studierenden werden betreut von einem Professor, der gleichzeitig Direktor des gesamten ISS ist und an der ENS auch noch Kurse für Lehramtsstudenten halten muss, einem fest angestellten promovierten Dozenten (dem Dekan) und einer Handvoll weiterer Dozenten, von denen die meisten frisch gebackene Absolventen des Master-Programms sind, die an ihren Dissertationen arbeiten. Im Vergleich dazu erscheint die Ausstattung deutscher Universitäten wirklich luxuriös. Der Dekan ist der einzige Dozent für das Master-Programm Telekommunikation und sagt über die Situation der Studierenden: „Es ist wie in der Grundschule – sie haben mich in allen Fächern!“ Dabei ist die Situation in den anderen, schon länger etablierten Universitäten in Kamerun nicht viel besser; auch dort sind Informatik-Fachbereiche meist nur mit einem Hochschullehrer und einigen wenigen Dozenten ausgestattet, von denen nur wenige promoviert sind. Die Studienprogramme können nur durch eine rege Reisetätigkeit aufrecht erhalten werden: Entsprechend qualifizierte Dozenten, die für Ministerien, Behörden oder andere Hochschulen arbeiten, bieten Lehrveranstaltungen zu bestimmten Themen als Blockkurse an.

**Berthold Hoffmann**

Dr. **Berthold Hoffmann** ist wissenschaftlicher Mitarbeiter an der Universität Bremen. Er studierte und promovierte an der Technischen Universität Berlin und lehrt und forscht an der Universität Bremen im Fachgebiet Programmiersprachen und Übersetzer.
*hof@informatik.uni-bremen.de*

Forschung ist bei der enormen Lehrbelastung extrem schwierig. Auch interdisziplinäre Zusammenarbeit mit anderen Fachbereichen scheitert oft an der Arbeitsbelastung und auch der fehlenden Erfahrung mit interdisziplinärer Arbeit.

## Die Situation der Studierenden

Die Studierenden kommen vorwiegend aus dem Norden Kameruns und aus dem Tschad. Sie müssen pro Semester ca. 40 Euro Studiengebühren bezahlen. Das ist kein Pappenstiel bei einem durchschnittlichen Verdienst von 2.400 Euro im Jahr! Wegen der Personalknappheit an den Universitäten dominiert bei den Lehrformen der Frontalunterricht, so dass die Studierenden Schwierigkeiten haben, sich praktisch zu qualifizieren – Programmieren und Softwareentwicklung steht nur in geringem Umfang auf dem Stundenplan. Die Personalknappheit hat darüber hinaus zur Folge, dass viele Lehrveranstaltungen nur als Blockkurse angeboten werden können, wodurch die Semesterplanung für die Studierenden erschwert wird.

Die Berufsaussichten für Absolventen sind ungewiss: Von den Arbeitsplätzen liegen landesweit derzeit 70 % in der Landwirtschaft, 13 % in der Produktion und 17 % in Dienstleistungssektor (mit öffentlicher Verwaltung) [1]. Softwarefirmen gibt es kaum, und auch die Industrie bietet wenige Arbeitsplätze für Informatiker. Am Ehesten gibt es Stellen in der Verwaltung. Nur die Besten können als Dozenten an die Universitäten gehen. Entsprechend begehrt sind bei den Studierenden in Maroua (und anderswo in Kamerun) Gelegenheiten, ihre Berufsaussichten durch einen Aufenthalt und möglichst einen Abschluss in Europa oder Nordamerika zu verbessern. Die Hochschulen versuchen, ihren Dozenten die Möglichkeit zu Auslandsaufenthalten und auch zur Promotion im Ausland einzuräumen, solange sie ihren Lehrverpflichtungen daheim nachkommen. So soll erreicht werden, dass die Dozenten nach der Promotion an ihre Hochschulen zurückkehren.

## Meine persönlichen Erfahrungen

Im Februar 2012 und Januar 2013 habe ich im Fachbereich *Informatik und Telekommunikation* zweiwöchige Kurse zum Thema *Formal Languages and Compiler Construction* gehalten. Die Aufenthalte wurden vom DAAD als Kurzzeitdozenturen gefördert. Jeweils rund zwanzig Studierende im *Licence*-Programm haben daran teilgenommen. Der Kurs fand an zehn Tagen vormittags von 7:30 bis 12:30 Uhr statt. Nachmittags haben die Studierenden kleinere Übungsaufgaben bearbeitet, die am nächsten Tag gemeinsam besprochen wurden. So in etwa sind auch die dortigen Veranstaltungen organisiert. Allerdings ist Frontalunterricht dort wohl immer noch die Regel. So wurde ich zu Anfang gefragt: „*Sir, will you dictate?*“ Manche Dozenten diktieren ihren Studierenden, was sie in ihre Hefte schreiben sollen. Dennoch beteiligten sich die Studierenden lebhaft, trotz der ungewohnten Unterrichtssprache – in Maroua wird vorwiegend in Französisch gelehrt, nicht in Englisch. Die Studierenden zeigen großen Lerneifer und Wissensdurst und sind begeistert, dass jemand aus dem fernen Europa zu ihnen kommt, um sie zu unterrichten.

Der Versuch, das Bearbeiten dieser Übungsaufgaben als Prüfungsleistung zu verwenden, schlug fehl, weil unter den Studierenden eine Kultur des Teilens besteht: Es wird trotz Ermahnungen viel voneinander abgeschrieben. Deshalb gab es doch eine schriftliche Klausur, die einige Wochen nach meinem Aufenthalt von Dozenten vor Ort durchgeführt und anhand von mir vorbereiteter Lösungen korrigiert und bewertet wurde. Diese Prüfung haben alle Studierenden bestanden, einige allerdings erst im zweiten Versuch.

Erst beim zweiten Aufenthalt (2013) habe ich dann erfahren, dass Lehrveranstaltungen normalerweise aus drei Teilen bestehen: neben Vorlesung und Übungen gehört dazu auch *individuelle praktische Arbeit*, bei der die Studierenden einzeln oder in kleinen Gruppen selbstständig eine Aufgabe bearbeiten. Daraufhin habe ich nach meiner Rückkehr das Compilerbau-Praktikum, das Kollegen mit mir gemeinsam an der Universität Bremen anbieten, ins Englische übersetzt und den Studierenden als Aufgabe gestellt. Das „Fernstudium“ hat sich – vorerst – als zu schwierig erwiesen. Sei es, weil den Studierenden die Programmiererfahrung fehlt, sei es, weil das Material (Präsentationen und vorgegebene Software) doch ohne intensive Betreuung nicht zu verstehen waren, jedenfalls ist keine Gruppe über minimale Lösungsansätze hinausgekommen, wobei es auch hier Plagiate gab.

## Wie kam es überhaupt zu diesen Aktivitäten?

Kolyang, der nahe Maroua geboren wurde, hat in Bremen Informatik studiert und in unserer Arbeitsgruppe promoviert, bevor er 1999 als Dozent an die Universität Ngaoundéré zurückkehrte. Dort hat er eine Zusammenarbeit zwischen den Universitäten Ngaoundéré und Bremen initiiert, in der gemeinsame Studienprogramme in den Fächern Ökologie und Informatik entwickelt wurden. Dies wird vom DAAD seit 2009 im Rahmen des Programms für *themenzentrierte Zusammenarbeit mit Entwicklungsländern* gefördert. Nachdem Kolyang 2008 an der Universität Bremen habilitierte, wurde er als Professor an die *Ecole Normale Supérieure* der gerade gegründeten Universität Maroua berufen und 2009 zum Gründungsdirektor des ISS ernannt. Er hat dessen Ausrichtung stark geprägt. Dabei geht es ihm um praxisbezogene Inhalte und Lehrformen wie Projekte, die er in Bremen kennen gelernt hat, während im französisch inspirierten System die systematische Grundlagenforschung im Vordergrund steht. Solche Veränderungen sind schwierig durchzusetzen, zumal die Dekane der Fachbereiche nicht von den Mitarbeitern gewählt werden, sondern unter Einflussnahme der Politik ernannt werden, wobei nicht unbedingt nach Qualifikation entschieden wird, sondern auch der religiöse und ethnische Proporz eine Rolle spielt.

Neben seinen beruflichen Aktivitäten engagiert Kolyang sich gesellschaftlich: Er hat das *Zentrum für endogene Entwicklung SAARE* gegründet, in dem er unabhängig von staatlichen Strukturen Projekte zur Bewahrung der einheimischen Kultur, Erwachsenenbildung und nachhaltigen Entwicklung ansiedeln kann [3]. Unser Kontakt zu Kolyang war nie abgebrochen, und nach einem Besuch unseres Sohnes in Maroua wurde klar, dass Hilfe bei der Weiterentwicklung der Lehrangebots dort bitter nötig ist, und unsere Lehrangebote höchst willkommen sind.

## Wie geht es weiter?

Im nächsten Schritt werde ich das Übersetzer-Praktikum so aufarbeiten, dass es mit Erfolg in Maroua durchgeführt werden kann. Daneben arbeite ich daran, das Material meines Kurses für die E-Learning-Plattform *Moodle* vorzubereiten. *Moodle* wird bereits in einem Projekt eingesetzt, in dem *E-Learning*-Kurse zur Softwaretechnik und Entwicklung mobiler Anwendungen an der Universität Ngaoundéré entwickelt wurden [4]. Genauer strebt man dort *blended learning* an: die selbstständige Arbeit der Studierenden mit dem *E-Learning*-Material der Kurse wird ergänzt um Tutorien und praktische Projektarbeit. Die in Ngaoundéré entwickelten Kurse werden allen Universitäten in Kamerun zur Verfügung gestellt, um die Lehrsituation zu entspannen.

Wir wollen unsere Lehraufenthalte in Maroua sehr gern fortführen. Es ist derzeit leider ungewiss, wann wir erneut dorthin reisen können. Denn im Februar 2012 wurden fünf französische Touristen in der Nähe Marouas von Anhängern der islamistischen Boko Haram nach Nigeria entführt und erst im April 2013 freigelassen. Daraufhin hat das Auswärtige Amt eine Reisewarnung für diese Region ausgesprochen, so dass derzeit keine DAAD-Aufenthalte in diesem Teil Kameruns genehmigt werden.

Auch die Zukunft der Universität in Maroua ist nicht gesichert. Wie auch in Deutschland verringern sich die finanziellen Zuwendungen des Staates eher als dass sie steigen, wie dies angesichts der zu leistenden Aufgaben bei steigenden Studierendenzahlen nötig wäre. Kolyang sagt dazu: „*C'est compliqué!*". Von diesem Ausspruch gibt es auch noch die Steigerungen „*C'est très compliqué!*" und „*C'est trop compliqué!*" Da hilft nur, was Menschen in Maroua einem oft wünschen: „*Du courage*!"

## Anmerkungen


[1] *Central Intelligence Agency (CIA): The World Factbook (www.cia.gov/library/publications/the-world-factbook/)*

[2] *Institut Supérieur du Sahel, Université de Maroua: Programme d'Enseignement. Januar 2011.*

[3] *Centre de Développement Engogène (CDE) SAARE, Maroua (cde-saare.de, Zugriff 29. Juli 2013)*

[4] *Karl-Heinz Rödiger (Universität Bremen) und David Békollé (Universität Ngaoundéré): Qualifizierung für die berufliche Perspektive als Software-Entwickler. Ein Beitrag zur Verbesserung der Lehrsituation in Informatik in Kamerun. BMBF-Projekt, 2011-2013. Ergebnisse unter elms.informatik.uni-bremen.de.*






**Lutz Frommberger**

# ICT for Development – ein Ansatz für Forschung und Lehre

## Erfahrungen mit dem studentischen Projekt *Mobile4D* an der Universität Bremen

*ICT for Development – kurz ICT4D – beschreibt den Einsatz an Informations- und Kommunikationstechnologie (ICT) für nachhaltige Entwicklung, insbesondere in Entwicklungsländern. Das trägt der Einsicht Rechnung, dass Entwicklungspolitik nicht bedeutet, mit dem Helikopter ein paar Sack Hirse abzuwerfen, um den Hunger in der Welt zu bekämpfen. Vielmehr heißt es, die betroffenen Regionen in die Lage zu versetzen, ihre Entwicklungsziele aus eigener Kraft zu erreichen. Für das englische Wort* Capacity Building *gibt es keine befriedigende deutsche Übersetzung – Hilfe zur Selbsthilfe trifft es noch am ehesten. Dabei sind der Zugang zu Kommunikationsmitteln und die Möglichkeit des Wissenstransfers bedeutende Elemente, die mit ICT-Systemen stark befördert werden können.*

Während sich ICT4D weltweit als eigenes Forschungsfeld etabliert, gibt es in Deutschland bislang nur wenige Arbeitsgruppen, die sich mit diesem Thema befassen. An der Universität Bremen haben wir 2011 das *International Lab for Local Capacity Building* (Capacity Lab, siehe *www.capacitylab.org*) gegründet, ein Forschungszusammenschluss der Arbeitsgruppe *Cognitive Systems* und des *Institute for Software Technology* der United Nations University in Macau (UNU-IIST). Ziel des Capacity Lab ist es, lokale Strukturen in Entwicklungsländern durch Einsatz von ICT-Systemen zu stärken. Die Ziele des Capacity Lab passen perfekt zu den Leitzielen der Universität Bremen (u. a. gesellschaftliche Verantwortung und Praxisbezug, fachübergreifende Orientierung, Internationalisierung von Lehre und Forschung, umweltgerechtes Handeln), so dass die Universität den Aufbau des Labs durch Finanzierung einer Postdoc-Stelle für zwei Jahre unterstützte.


*Kickoff-Workshop in Bremen: Savanh Hanephom vom MAF mit Studierenden von Mobile4D*

### ICT-Systeme und Naturkatastrophen

Eines der ersten Projekte des Capacity Lab ist die WWW-basierte Kommunikationsplattform PRAM KSN (siehe *www.capacitylab.org/project/pramksn*) für die landwirtschaftliche Entwicklung in Laos. Sie hat zum Ziel, über das WWW einen direkten Kommunikationsweg zwischen sogenannten „Extension Workers" (Angestellte der Regierung, die in dörflichen Strukturen landwirtschaftliche Entwicklung unterstützen) bereit zu

*Entwicklung und Bugfixing auf der Terrasse des Hotels in Vientiane*

stellen und direkten Austausch zwischen ihnen zu ermöglichen. PRAM KSN wird in direkter Zusammenarbeit mit dem Ministerium für Land- und Forstwirtschaft in Laos (MAF) von Beginn an in Workshops mit den Beteiligten selbst entwickelt und geplant. Seit Anfang 2012 ist ein Prototyp im Einsatz. Als Ergebnis eines gemeinsamen Workshops im Sommer 2012 in Luang Prabang wird als weitere Komponente von PRAM KSN ein Vorhersage- und Meldesystem für Naturkatastrophen gewünscht. Die Verantwortung für die Entwicklung dieser Komponente übernehmen wir an der Universität Bremen. Innerhalb eines Jahres soll ein Prototyp fertig sein und in Laos getestet werden – ein ambitionierter Plan.

Bedingt durch den Klimawandel, das Bevölkerungswachstum und durch soziale Veränderungen haben Naturkatastrophen einen immer größeren Effekt auf die Lebensverhältnisse der Menschen, insbesondere auf die Nahrungsstabilität. So sind in Laos vor allem die verheerenden Überschwemmungen des Mekong und seiner Nebenflüsse in den letzten Jahren zu einem immer gravierenderen Problem geworden. Allein die Flut des Mekong im Jahr 2011 betraf über 420.000 der sechs Millionen Einwohner von Laos. Aber insbesondere auch vergleichbar kleinere Vorfälle, wie die Ausbreitung von Pflanzen- und Tierkrankheiten, können massive Folgen für die Einzelnen haben. Viele der entstehenden Probleme könnten dabei leichter und wirksamer gelöst werden, wenn die Kommunikationsstrukturen im Lande verlässlicher funktionieren würden. Vielfach wird die Verwaltung der Probleme vor Ort überhaupt nicht gewahr, und Warnungen vor Katastrophen erreichen die Betroffenen zu spät. Hier soll nun unser System ansetzen.

Geplant ist ein System, das einen bidirektionalen Kommunikationsfluss ermöglicht. Einerseits sollen Warnungen vor Naturkatastrophen von der Administration direkt an die zuständigen lokalen Behörden, aber vor allem auch an die unmittelbar Betroffenen geleitet werden. Andererseits sollen die Menschen vor Ort in die Lage versetzt werden, ihrerseits Katastrophen zu melden. Als Location-based-Service sollen die Beteiligten direkt verortet werden können und so soll gewährleistet sein, dass immer genau die Betroffenen informiert werden können. Als Plattform haben wir Android-Smartphones gewählt. Diese stellen ein verhältnismäßig preiswertes System mit breiter Sensorik zur Verfügung, insbesondere die Lokalisierbarkeit per GPS ist für den geplanten Location-based-Service relevant. Zudem ist die großflächige Abdeckung mit mobilem Internet in Laos überraschend gut – besser als mancherorts in der deutschen Provinz.

Aus Sicht der Wissenschaft ist ein solches System überaus interessant. ICT-Systeme zum Katastrophenmanagement sind Gegenstand aktueller Forschung. Auch der Einsatz partizipativer Methoden, insbesondere VGI (Volunteered Geographic Information), hat noch großen Forschungsbedarf. Zudem ist der Entwurf von Benutzerschnittstellen für vergleichbar technikferne Zielgruppen ein herausforderndes Thema.

## Ein studentisches Projekt in der ICT4D-Forschung

Die Planung und Realisierung eines solchen komplexen Systems ist allerdings relativ zeit- und ressourcenaufwändig und mit der einen vorhandenen Stelle und freiwillig mitarbeitenden WissenschaftlerInnen nicht zu bewältigen. Wir haben uns daher entschieden, eine der spezifischen Stärken der Universität Bremen zu nutzen: das Projektstudium. Studentische Projekte sind ein zentraler Bestandteil des Informatik-Studiums. Hier kommt eine Gruppe von üblicherweise 10-20 Studierenden für 8 bis 12 Monate zusammen, um gemeinsam fokussiert an einer Fragestellung zu arbeiten. Handlungsorientierung, Selbstorganisation und Selbstverantwortung, kooperatives Lernen im Team, Interdisziplinarität sowie die Einbindung von Forschungsinhalten in den Lehrkontext sind hier die Ziele – somit ein perfekter Rahmen für die Entwicklung des geplanten Systems. Im Oktober 2012 startete das Projekt *Mobile4D* mit 21 Studierenden.

Studentische Projekte agieren sehr autonom und organisieren ihre Arbeit weitestgehend selbst. Das beinhaltet theoretisch auch stets die Möglichkeit des Scheiterns – mitunter mal die falsche Entscheidung zu treffen, sich in eine Sackgasse zu verrennen und sich in unmöglichen Planungen zu verheddern, gehört für das selbstständige Erlernen von Projektarbeit selbstverständlich dazu. Gehen wir ein Risiko ein, die Systementwicklung ganz in die Hände des studentischen Projekts zu geben?

Nicht wirklich. Natürlich, man hat schon das eine oder andere Projekt mit eher zweifelhaftem Ergebnis gesehen. Nicht immer wird das gesteckte Ziel erreicht, mitunter funktioniert das erstellte Produkt doch nicht wie gewünscht. Jedoch hat das Projekt Mobile4D einige Vorteile, die nicht jedes studentische Projekt mitbringt: Das zu entwickelnde Produkt ist nicht für die akademische Schublade oder eine einzige Präsentation nach Projektende gedacht, sondern soll produktiv in großem Rahmen genutzt werden. Zudem verfolgt es ein konkretes Ziel: im Katastrophenfall zur Verminderung von Armut beizutragen. Die Verantwortung für dieses Projekt mit einzugehen, sorgt für die notwendige Motivation und zielgerichtetes Vorgehen im Projektverlauf.

Zu Beginn des Projekts konnten wir mit Unterstützung des Bundesministeriums für Bildung und Forschung zwei zuständige Mitarbeiter des Ministeriums für Land- und Forstwirtschaft in Laos für einen zweitägigen Kickoff-Workshop mit dem Mobile4D-Projekt nach Bremen holen. Das sollte absichern, dass wir nicht am Bedarf vorbei planen, sondern die Belange und An-

forderungen der Menschen vor Ort verstehen und berücksichtigen. Auch die Organisation des Workshops war weitestgehend den Studierenden überlassen – und er war ein Erfolg. Am Ende stand eine konkrete, detaillierte Anforderungspezifikation und ein ambitionierter Zeitplan: Bereits fünf Monate später sollte das System in einem Feldtest in Laos getestet werden.

Die Projektarbeit läuft rund, alle Meilensteine werden eingehalten, das System steht wie geplant. Als Projektbetreuer müssen wir kaum steuernd eingreifen – ein musterhafter Verlauf. Bleibt nur noch der Praxistest vor Ort. Hier sind wir darauf angewiesen, dass auch Studierende mit nach Laos reisen – schließlich sind sie die Experten für das System. Da der Feldtest über mehrere Distrikte verteilt stattfinden muss, brauchen wir auch ausreichend Leute. Für zwei Studierende können die Reisen aus Universitätsmitteln finanziert werden. Das Geld für zwei weitere Studierende kommt aus Spenden zusammen: Eine lokale Firma finanziert einen Flug, einen weiteren wirbt das Projekt u. a. durch Einrichtung einer temporären Caféteria im Informatik-Gebäude der Universität durch den Verkauf von Kaffee und Kuchen ein. So können wir Mitte April mit einer sechsköpfigen Delegation starten.

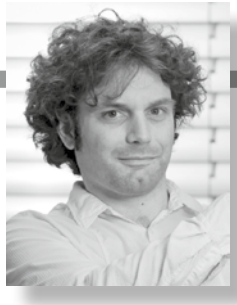
## Der Praxistest vor Ort

Vor Ort in Laos werden dann zunächst Kompetenzen gefordert, die zur Arbeit in Entwicklungsländern zwingend dazugehören: Flexibilität und Improvisationsfähigkeit. Durch Missverständnisse in der Terminplanung mit den Partnern in Laos landen wir mitten im laotischen Neujahrsfest. Faszinierend – allerdings ist Lao New Year vergleichbar mit Weihnachten in Deutschland: Geschäfte und Behörden haben tagelang geschlossen, man fährt heim zur Familie, das Alltagsleben steht quasi still. Das geplante Auftaktreffen im Ministerium müssen wir genau wie die geplanten Tests um einige Tage nach hinten verschieben, das Büro von UNU-IIST können wir entgegen der Planung nicht benutzen, Kontaktpersonen sind nicht erreichbar. Zudem gibt es Unklarheiten über den Ort des Feldtests: statt wie erwartet in der Hauptstadt Vientiane zu testen, muss nun die ganze Delegation nach Luang Prabang weiterfliegen. Und es gibt genug zu tun: Die Smartphones müssen mit Datentarifen der wichtigsten lokalen Provider ausgerüstet werden, letzte Bugs werden gefixt und die lokalen Eigenheiten der Ortungsdienste umschifft, der Feldtest wird konkret geplant – bei 40 Grad im Schatten, drückender Luftfeuchtigkeit, den unausweichlichen Verdauungsproblemen, zeitweise ohne fließend Wasser und mit einer Internetanbindung, deren Qualität für das entwickelte System vollends ausreicht, aber für die eigene Entwicklung mit unserer Infrastruktur in Deutschland zum Flaschenhals wird.

*Schulung von Mitarbeitern im Provinzbüro in Luang Prabang, Laos*

Dennoch können wir eine Woche nach unserer Ankunft in Luang Prabang zuständige Mitarbeiter aus Provinz- und Distriktbehörden in der Verwendung des Systems schulen, und am Tag darauf den ersten Feldtest erfolgreich bestreiten. Im Test in drei verschiedenen Distrikten funktioniert Mobile4D wie gewünscht. Dabei können wir die Probleme vor Ort ganz direkt begutachten. Den Test im Distrikt Chompet müssen wir vorzeitig abbrechen: Durch ein heranziehendes Gewitter droht die Straße unpassierbar zu werden – was wir dann direkt per Smartphone-App melden können. Kleinere Auffälligkeiten werden behoben. Ein Beispiel: Die Internetanbindung im Distriktbüro in Pak-Ou ist noch deutlich langsamer als erwartet, so dass allein das erste Laden der Administrations-Webseite fast 15 Minuten benötigt – hier wird noch einmal deutlich Code reduziert. Zwei Tage später nutzen wir Mobile4D, um in den Dörfern in den verschiedenen Distrikten reale Katastrophen der letzten Wochen aufzunehmen und das System für den Gebrauch wirklicher Daten zu testen. Auch hier muss wieder improvisiert werden: In Chompet treffen wir niemanden mehr in den Behörden an – dort feiert man immer noch Neujahr. Insgesamt ist der Test ein voller Erfolg: Das System funktioniert, und die beteiligten Mitarbeiter zeigen sich begeistert und geben uns noch etliche Verbesserungsvorschläge und Feature-Wünsche mit. Zurück in Vientiane vereinbaren wir mit dem Ministerium eine weitere Zusammenarbeit und eine längere produktive Pilotphase – sofern wir eine Finanzierung finden.

Die zweiwöchige intensive Zusammenarbeit mit den Studierenden war auch für uns als Betreuer eine intensive und erfreuliche Erfahrung. Es war gut zu sehen, dass so professionell gearbeitet wird, dass man den Studierenden problemlos Präsentatio-



**Lutz Frommberger**

**Lutz Frommberger** ist Senior Researcher in der Arbeitsgruppe *Cognitive Systems* an der Universität Bremen. Seit 2011 ist er Lab Manager des International Lab for Local Capacity Building (Capacity Lab).

*Erster Feldtest des Mobile4D-Systems in einem Dorf im Distrikt Chompet*

nen in einem Ministerium anvertrauen oder sie zur Testdurchführung in ferne Distriktverwaltungen schicken kann. Zudem konnten wir uns auf die zeitnahe Unterstützung der in Deutschland verbliebenen Projektmitglieder und die Funktionalität der dort betriebenen Server-Infrastruktur stets verlassen. Und für einen tagesaktuellen Bericht über Feldtest und Vorbereitungen auf Facebook wurde auch gesorgt (siehe *www.facebook.com/mobile4d*).

## Ausblick

Insgesamt eröffnet der Bereich ICT4D faszinierende Optionen für Forschung und Lehre in der Informatik. Ein Hürde in der ICT4D-Forschung, nämlich dass die interessanten Forschungstätigkeiten oft erst ein laufendes System und somit recht viel Arbeit im Vorfeld erfordern, kann durch die Mitarbeit von Studierenden wirksam angegangen werden. Zudem sind Projekte mit ICT4D-Hintergrund gut geeignet, den eigenen Horizont zu erweitern, für uns selbstverständliche Technologien und Mechanismen zu hinterfragen und das Themenfeld *Informatik und Verantwortung* mit sehr praktischen Inhalten zu füllen. Natürlich müssen erst geeignete Partner vor Ort gefunden werden. Hier bietet sich gegebenenfalls an, auf die expandierenden US-Universitäten zu schauen, die verstärkt Dependancen in Entwicklungsländern aufbauen und dort gern kooperieren. So wird auch das Capacity Lab demnächst mit einem Studierendenprojekt an der CMU Rwanda zusammenarbeiten, und einen Studenten aus dem Mobile4D-Projekt konnten wir in ein Praktikum an der New York University in Abu Dhabi vermitteln.

Wie geht es weiter mit Mobile4D? Im Oktober 2013 startet das Nachfolge-Studierendenprojekt, jetzt mit Master-Studierenden. Wenn die erhoffte Finanzierung gesichert werden kann, werden wir mit diesen Studierenden die Pilotphase des Systems in Laos begleiten – sicherlich auch wieder vor Ort und wahrscheinlich mit nicht weniger guten Ergebnissen und Erfahrungen für alle Beteiligten.

*Zweiter Feldtest: Aufnahme einer Pflanzenkrankheit auf einem Reisfeld in Muangkhay*

**Klaus Fuchs-Kittowski**

# Umweltinformatik und Gesellschaft

## Vorlesung und Projektarbeit[1] an der Hochschule für Technik und Wirtschaft im Studiengang Umweltinformatik

*Das Fachgebiet* Informatik und Gesellschaft *war von Anbeginn keine Ansammlung verschiedener Themen, wenn auch im konkreten Vorlesungsbetrieb immer nur eine Auswahl an aktuellen Problemen vorgenommen werden kann. Es ging und geht um viel mehr! Im Sinne des Humboldtschen Bildungsideals geht es um die Vermittlung von Orientierungswissen, um die Herausbildung einer Grundhaltung zu den durch die Gestaltung und den Einsatz der modernen Informations- und Kommunikationstechnologien (IKT) hervorgerufenen sozialen und gesellschaftlichen Veränderungen. Die Informatikerinnen sollen damit in der Lage sein, den Konflikt zwischen Technokratie und Soziokratie[2], zwischen Rationalität und Humanität, durch eine am Menschen orientierte (sozio-technische) Informationssystemgestaltung und Softwareentwicklung, durch eine auch sozialwissenschaftlich und ethisch fundierte Theorie und Methodologie der Informatik, in der praktischen Arbeit zu überwinden.*

### Umweltinformatik und Gesellschaft – Notwendiges Orientierungswissen

Entsprechendes Orientierungswissen hat für die Umweltinformatikerinnen besondere Bedeutung. Die Erfahrung zeigt, dass Technologien recht schnell einem veränderten Weltbild, neuen Orientierungen, folgen, während sich unser Weltbild, unser Verhältnis zur Natur und Gesellschaft auch bei schnellem technologischen Wandel kaum verändert. Der Streit um den richtigen Weg in die Zukunft wird in den Köpfen und Herzen von Men-

schen entschieden, die sich der Tatsache bewusst werden, dass man sich auch gegenüber der Natur in ihrer Mannigfaltigkeit so wie gegenüber den Mitmenschen moralisch verhalten sollte. Hier fehlt es nicht an Angeboten zur Entwicklung einer Naturethik, einer Bioethik oder auch Umweltethik[3]. Die Verhaltensänderung, die in der Umweltinformatik verlangt wird, damit das Leben auf unserem Planeten nicht weiterhin immer stärker gefährdet wird, muss jedoch noch tiefer gehen. Verlangt wird ein Wissen von der Natur und den technisch-technologischen Eingriffen in die Natur sowie den Möglichkeiten der informationstechnologischen Unterstützung und Kontrolle dieser erforderlichen Eingriffe, die von der Achtung gegenüber den Naturwesen, der Teilnahme an ihrem Dasein ausgeht und den Menschen als Teil der Natur und vorrangig soziales und gesellschaftliches Wesen versteht.

Angesichts der Steigerung der technischen Verfügbarkeit über die Natur, die speziell mit den Ergebnissen der Entschlüsselung des Humangenoms[4] und der modernen Forschungen zur künstlichen Intelligenz auch unseren eigenen Körper und den menschlichen Geist einschließt, entzündet sich die Diskussion um das Selbstverständnis des Menschen. Die entscheidende Erfahrung ist, dass auf Grund der technologischen Entwicklungen, speziell der Bio- und Informationstechnologien, die Menschen fast nichts mehr als Gewordenes, als schon Gegebenes akzeptieren können. Wollen wir uns nicht einfach dem spontanen Geschehen überlassen, kann die entscheidende Konsequenz nur sein, dass auch unser Natursein in den bewussten Entwurf von Humanität einbezogen sein muss.

## Zur Umweltinformatik und zur Ambivalenz der Wirkungen moderner IKT

Die besondere Stärke der Umweltinformatik liegt in ihrer Interdisziplinarität. Im Zusammenwirken von Natur-, Struktur- und Technikwissenschaften sowie Human-, Sozial- und Wirtschaftswissenschaften wird sie einen wichtigen Beitrag zur Bewältigung der globalen Herausforderung für das 21. Jahrhundert, zur nachhaltigen Entwicklung leisten können[5].

Die Umweltinformatik und damit auch die betriebliche Umweltinformatik stellen sich als Teilgebiet der angewandten Informatik bzw. der Wirtschaftsinformatik die Aufgabe, die Methoden der Informatik zur Entwicklung einer nachhaltigen Informationsgesellschaft zum Einsatz zu bringen[6]. Ziel ist die Nachhaltigkeit in ihrer umweltorientierten, ökonomischen und sozialen Dimension durch Entwicklung und Einsatz moderner Informations- und Kommunikationstechnologien zu fördern. Bei den vorausschauenden Einschätzungen der bisher noch ungenügend ausgeschöpften Potenzen der modernen IKT für die Entwicklung einer nachhaltigen Informationsgesellschaft, aber auch der deutlich werdenden Grenzen z. B. durch Bumerangeffekte und elektronische Abfälle, zeigt sich immer deutlicher, dass man bei diesen Einschätzungen von vornherein von der Ambivalenz der Wirkungen moderner IKT ausgehen muss, und dies auch getan wird[7]. Die Ambivalenz, wie an Beispielen zu zeigen ist, sagt zunächst, dass nicht immer nur das Gewünschte erreicht wird, sondern dass mit der wissenschaftlich-technischen Entwicklung auch unerwünschte Ergebnisse verbunden sein können, wobei es die positiven Wirkungen zu fördern und die negativen zu vermeiden oder zu kompensieren gilt. Der Gedanke des „Verlusts im Vorwärtsschreiten“ von Ernst Bloch[8] führt jedoch in einem wesentlichen Punkt noch weiter. Hier wird z. B. deutlich, dass wir zugunsten höherer Rationalität durchaus bereit sind, etwas aufzugeben, was gut war in der Vergangenheit, die Aufgabe also einen Verlust darstellt, so z. B. der persönlichere Einkauf im kleinen Laden gegenüber dem Supermarkt. Die elektronische Kommunikation führt zum Verlust an sogenannter face-to-face-Kommunikation usw.

Durch die Zurückführung der menschlichen (semantischen) Informationsverarbeitung auf maschinelle (syntaktische) Informationsverarbeitung erhält die Information neue Gebrauchswerte, die entsprechend den herrschenden Produktions- und Organisationsverhältnissen, den gewünschten Leistungs- und Persönlichkeitsentwicklung fördernden Arbeitsbedingungen und -inhalten sowie auch entsprechend den persönlichen Bedürfnissen zur Entfaltung der Individualität, selektiert werden können[9]. In der Informatik erfolgt die Auswahl zunächst unter dem Gesichtspunkt des technisch Machbaren. Dies muss ergänzt werden durch den fachlich, sozial und ethisch verantwortbaren Computereinsatz. Eine Richtschnur dafür ist die These von der Schaffung einer „Informationsgesellschaft für alle“[10], eng verbunden mit der Vision der „nachhaltigen Entwicklung“ im Sinne der Brundtland Commission. Die (betriebliche) Umweltinformatik ist eine junge, interdisziplinäre Wissenschaft, die dieser Vision verpflichtet ist[11]. Ihre Entwicklung ist eng verbunden mit der Entwicklung des Umweltbewusstseins und der Erkenntnis, dass mit dem dezentralen und vernetzten Einsatz der Computer besonders positive, aber auch negative Wirkungen auf die Individuen, die soziale Organisationen sowie die Gesellschaft und die Natur verbunden sind. Hiermit müssen sich die Studierenden der Umweltinformatik auseinandersetzen, wollen sie erfolgreich Umweltinformationssysteme gestalten.

Das Gebiet Umweltinformatik und Gesellschaft analysiert die Wirkungen des Einsatzes moderner Informations- und Kommunikationstechnologien in unterschiedlichen Bereichen, speziell in der Wirtschaft und der Umwelt, in Einrichtungen des Umweltschutzes und des Gesundheitswesens und entwickelt Kriterien und Methoden einer am Menschen orientierten Gestaltung von IKT-Anwendungssystemen in betrieblicher und zwischenbetrieblicher sozialer Organisation. Damit wird der Weg aufgezeigt, den die Disziplin *Informatik/Wirtschaftsinformatik/Umweltinformatik und Gesellschaft* gehen muss – von der Wirkungsforschung über ein tieferes Verständnis des Wesens informationeller Systeme zur sozial und ökologisch orientierten Gestaltung automatenunterstützter Informationssysteme. Es geht dabei um erforderliche rechtliche Regelungen des Computereinsatzes und um ethische Konsequenzen möglichen Missbrauchs des Einsatzes des Computers sowie der weltweiten digitalen Netze. Es geht um grundlegende Anwendungsprobleme in den verschiedenen Bereichen des sozialen und gesellschaftlichen Lebens, um deren natur-, informations- und sozialwissenschaftlichen sowie philosophischen, erkenntnistheoretischen und methodologischen Fundierung[12].

## Zielstellung des Projektes: Umwelt – Informatik – Gesellschaft

Das Projekt *Umwelt–Informatik–Gesellschaft* wurde im Wintersemester 2012/2013 mit folgender Zielstellung begonnen: Die Studierenden sind in der Lage, die Disziplin der Umweltinformatik in einen übergeordneten wissenschaftlichen Kontext einzuordnen und wissen, welche gesellschaftlichen Konsequenzen und Implikationen mit den Ergebnissen der Informatik verbunden sind. Der Begriff der Nachhaltigkeit mit seinen sozialen, ökonomischen und ökologischen Facetten ist den Studierenden geläufig. Insbesondere das hohe Maß an Interdependenz sowie die umfassende Entwicklungsmöglichkeit der Umweltinformatik gehören zum gesicherten Kenntnisstand der Studierenden. Die theoretischen und praktischen Erkenntnisse aus dem Literaturstudium und die Erfahrungen aus den Gesprächen mit den Experten oder Befragungen (und eventuell auch aus Exkursionen) werden in dem rund 20 Seiten umfassenden Abschlussbericht der Projektgruppe zusammengefasst. Aus dem Abschlussbericht wird gegen Ende des Semesters von jeder Projektgruppe vorgetragen. Der Bericht ist bis zum Vortrag als Heft und in elektronischer Form abzuliefern. Dauer der Präsentation ist pro Gruppe mindestens 25 Minuten. Weiterhin erfolgt eine mündliche Prüfung.

Gegenüber den vorangegangenen Jahren wurde mit der Projektveranstaltung der Umfang der Lehre auf dem Gebiet Umweltinformatik und Gesellschaft im Bachelor-Studium noch erweitert. Zuvor gab es nur eine Vorlesung ohne Seminar in einem Semester. Jetzt ist mit einer zeitlich etwas verkürzten Vorlesung mehr Zeit für eigenständige Projektarbeit der Studenten vorgesehen. Aus der Vielzahl möglicher Themen für die Vorlesung wurden solche Themen gewählt, die einerseits in Grundprobleme von Informatik/Umweltinformatik und Gesellschaft einführen, aber zugleich auch mit dem Fach (betriebliche) Umweltinformatik verbunden sind, damit eine echte Fundierung des Fachs durch entsprechendes Orientierungswissen erfolgt.

Die Vorlesungsthemen waren:

- Zur Ambivalenz der Wirkungen moderner Informations- und Kommunikationstechnologien auf Individuum, Gesellschaft und Natur.
- Umweltinformatik und Umweltforschung in ihrer Interdisziplinarität – Aufgaben der betrieblichen Umweltinformatik bei der Unterstützung der drei Säulen der Nachhaltigkeit.
- Umweltinformatik und Umweltforschung zur Bewältigung der Herausforderungen des Klimawandels und der Energiewende.
- Zur (informatischen) Modellbildung im Methodengefüge der Wissenschaft – Zur revolutionären Rolle der Methoden in der Wissenschaft.
- Künstliche Intelligenz im Umweltbereich – KI-Kritik – der lange Weg der Informatik zum Menschen Paradoxie der Sicherheit – Werden Kapitäne, Operateure in Zukunft Menschen oder Computer sein?
- Information, Selbstorganisation und Evolution – Zum evolutionären Stufenkonzept der Information[13].
- Informatik und Ethik – zum fachlich, sozial und ethisch verantwortbaren Computereinsatz.
- Umweltmanagement – die Vision der Nachhaltigkeit als Leitmotiv der Umweltinformatikerinnen.
- Stoffstrommanagement – Methodologie der Umweltinformatik und der Technologiefolgenbewertung.

Mit den hier realisierten zehn Vorlesungen kann natürlich nur eine Einführung in einige der Grundprobleme gegeben werden. Der Grundgedanke ist: Durch die Entwicklung der modernen Technologien ist der Mensch von einem relativ hilflosen Wesen zum Gestalter natürlicher und gesellschaftlicher Strukturen und Prozesse auf der Erde geworden, der heute nach den Sternen greift. Der Mensch als ein Teil der Natur und vorrangig gesellschaftliches Wesen ist weder physikalisch vollständig zu erklären noch durch den technischen Automaten vollständig zu ersetzen; er muss, insbesondere in riskanten Systemen, höchste Autorität sein und bleiben. Weitere durchgehende Gedanken beziehen sich auf die spezifische Verantwortung der Umweltinformatikerinnen gegenüber den gesellschaftlichen Entwicklungen und der Umweltbewegung. Die Umweltinformatik kann in dem aufrüttelnden Buch: *Die Grenzen des Wachstums*[14], welches durch Modellstudien die entscheidende Debatte über die Zukunft der Menschheit angestoßen hat, ihre Geburtsurkunde sehen. Damit und mit den weiteren Veröffentlichungen des *Club of Rome* zur Umweltproblematik, wie die von Ernst Ulrich von Weizsäcker[15,16], Franz Josef Radermacher[17] u. a. sind die Grundprobleme für die Vorlesung Umweltinformatik und Gesellschaft und eine entsprechende Projektarbeit der Studenten vorgezeichnet. In der Tat ist die globale Erwärmung unseres Planeten durch die Treibhauseffekte, der vom Menschen induzierte Klimawandel, die größte Herausforderung der Menschheit im 21. Jahrhundert.[18, 19]

Die selbständige Bearbeitung der vorgeschlagenen Projektthemen durch die Studierenden in verschiedenen Projektgruppen bildet den Kern der Projektveranstaltung. In diesem Jahr haben wir dazu folgende Themen, mit entsprechender Literatur, den Studenten vorgeschlagen:

- Zur Verantwortung der Wissenschaft und der Wissenschaftler für eine effektive, effiziente und sozial verantwortbare Energiewende
- Ambivalenz der Wirkungen moderner IKT auf Natur, Mensch und Gesellschaft
- Technik – Sicherheit – Techniksicherheit
- Für und Wider einer automatisierten Kriegsführung (der Kriegsroboter)
- Medium Computer – Digitalisierung und Rationalisierung einer Welt
- Kognitionswissenschaft und Kognitionstechnologie – Josef Weizenbaum – Informatik- (KI-)Kritik als Gesellschaftskritik

- Diskussion um Grundbegriffe der Informatik/Umweltinformatik und zur Anwendung von Informatikmethoden in der (betrieblichen) Umweltinformatik
- Zu Problemen der Informationssystemgestaltung: am Menschen orientierte Gestaltung von (betrieblichen Umwelt-) Informationssystemen in sozialer Organisation
- Diskussion um Leitbilder und Einsatzstrategien der Informatik
- Computergestütztes Stoffstrommanagement – Entwicklung der Methodologie der Umweltinformatik
- Wie kann man Schüler und andere Interessierte für ein Studium der (betrieblichen) Umweltinformatik an der HTW begeistern?
- Informationstechnologie (IT) und der Klimawandel

Die Tragweite der Themen kann noch besser erfasst werden, wenn die dazu angegebene Untergliederung und Literatur zur Kenntnis genommen werden kann. Dies würde aber den hier gegebenen Rahmen sprengen. Auf der Grundlage der angegebenen Literatur konnten die Studenten relativ schnell zur eigenständigen Arbeit in der Gruppe kommen.

## Aktuelle Probleme und Herausforderungen an Informatik und Gesellschaft

Es ist in diesem Rahmen nicht möglich, auf die Ergebnisse der einzelnen Projektarbeiten einzugehen. Daher soll im Folgenden über einige generelle Probleme und Herausforderungen an das Fachgebiet *Informatik/Umweltinformatik und Gesellschaft*, wie sie sich auch in den Projektarbeiten niedergeschlagen haben, gesprochen werden.

Die Informatiker, Wirtschaftsinformatiker und Umweltinformatiker sind sich heute sehr wohl bewusst, dass mit der Informationssystemgestaltung und Softwareentwicklung, mit der damit verbundenen Arbeits- und Organisationsgestaltung soziale Realität verändert, ja neu geschaffen wird. Sie müssen sich entsprechenden Fragen stellen[20] und Lösungswege für die sich ergebenden gravierenden Probleme suchen. Solche zentralen Fragen und damit gegebenen Probleme sind u. a.:

1. Die Studierenden der Informatik und speziell auch der Umweltinformatik sollen sich ein selbständiges Urteil darüber bilden können, welchen Beitrag die Informatik und speziell die Umweltinformatik zur Lösung der gegenwärtigen Weltkrisen leisten kann:
   - zur Umweltkrise, zur Verminderung des durch den Menschen induzierten Klimawandels,
   - zur Entwicklung der sogenannten 3. Welt, zur Überwindung von Armut und Überbevölkerung,
   - zur globalen Finanz- und Wirtschaftskrise, zur Überwindung krasser sozialer Ungleichheit,
   - zur Entwicklung einer gerechteren Gesellschaft als Voraussetzung für Frieden,
   - zur Gewährleistung der individuellen, sozialen und internationalen Menschenrechte,
   - zur Entwicklung einer nachhaltigen Informationsgesellschaft, einer sozialen Kommunikationsgesellschaft, die zur Wertschaffung die Kreativität der Menschen umfassend einzusetzen vermag, die sich auf die Entwicklung ihrer Intelligenz und Bewusstheit ihres Menschseins – Menschen unter Menschen zu sein – gründet.
2. Die Studierenden sollen Klarheit darüber gewinnen, ob die Idee einer sich auf die modernen Informations- und Kommunikationstechnologien gründenden Informations- bzw. Wissensgesellschaft, einer post-industriellen Gesellschaft ein Mythos oder sich herausbildende Realität ist? Inwieweit muss und kann diese Idee der Informations- bzw. Wissensgesellschaft mit der Vision der Nachhaltigkeit verbunden werden und was kann die Umweltinformatik zur Entwicklung einer nachhaltigen Informationsgesellschaft beitragen? Modifiziert die Informations- und Kommunikationstechnologie wirklich die Strukturen der Industriegesellschaft und inwiefern kann sie real zur Dezentralisierung von Organisationsstrukturen und zur Nachhaltigkeit beitragen?
3. Die Studierenden sollen beurteilen können, ob die von manchem Theoretiker aufgestellte These der Neutralität des Werkzeugs wirklich hält oder ob es politisch-organisatorische Implikationen gibt. Welche Konsequenzen ergeben sich daraus für die Informationssystemgestaltung und Softwareentwicklung? Schon bei der frühen Technikentwicklung wird man feststellen können, dass hier nicht nur Mittel für einen gegebenen Zweck zur Verfügung gestellt wurden, sondern mit ihnen zugleich neue Ziele erschlossen wurden. Diese Entwicklung gipfelt in der Universaltechnik der Informatik. Informatikerinnen und Informatiker müssen lernen mit der Frage umzugehen, dass es keine wertfreie Wissenschaft und noch weniger eine wertfreie Anwendung von Technologie gibt. Die Softwaretechnik erlaubt, wie kaum eine andere Technik, die Anpassung an neue Zwecke für neue Anwendungen.
4. Die Studierenden der Umweltinformatik sollten sich ein selbständiges Urteil darüber bilden können, in welchem Maß Umweltmodelle, Umweltinformationssysteme mit ihrer Modellwahrheit die realen sachlichen, technisch-organisatorischen Bedingungen erfassen und in welchem Maß sie möglicherweise Sichtweisen überholter Managementtheorien (Taylorismus) bzw. scientistisch-technokratische Ideologie bewusst oder unbewusst mit aufnehmen. Für kaum eine andere Wissenschaft hat die Modellmethode ein solches Gewicht, wie für die Klima- und Umweltforschung sowie für die Umweltinformatik, die für ihre sachgerechte Einordnung ins Gesamtgefüge der Methodologie der Wissenschaften Sorge tragen muss.
5. Die Studierenden werden mit der Diskussion des Geist-Gehirn-Problems, der philosophischen Frage: „Können Maschinen denken?“, der Darstellung der Entwicklung der

Forschung zur Künstlichen Intelligenz und der Kritik an dieser Forschung mit einer Reihe theoretischer und praktischer Grundfragen der Informatik konfrontiert. Durch die Diskussion dieser Fragen gewinnt der Studierende der Informatik bzw. Umweltinformatik das erforderliche Verständnis für das Verhältnis von Automat und Mensch, von maschineller (syntaktischer) und menschlicher (semantischer) Informationsverarbeitung, um deren sinnvolle Kombination es bei allen konkreten Fragen eines rationalen und menschengerechten Computereinsatz geht.

6. Die Studierenden haben sich mit sozial-psychologischen Problemen des Einsatzes moderner IKT auseinanderzusetzen. Widerstand gegen technisch-technologische Innovation gründet sich oftmals auf eine irrationale Angst vor Neuerungen, oftmals aber auch auf sensitive Reaktionen auf mögliche Dehumanisierung des Arbeitslebens, Gefahren hinsichtlich des Datenschutzes und der Datensicherheit u. a. Der mit dem Einsatz der modernen Technologien beschäftigte Informatiker muss daher die möglichen berechtigten und unberechtigten Befürchtungen der Betroffenen kennen, um ihnen sachgerecht begegnen zu können. Er muss daher die Methodologie einer sozio-technischen Informationssystemgestaltung gründlich kennen und über die sozialen Aspekte der Einführung der modernen Informations- und Kommunikationstechnologien systematisch unterrichtet sein.

7. Die Studierenden der Informatik und Umweltinformatik sind insbesondere über die Wirkungen der IKT auf die Arbeitswelt, auf das politische und private Leben gründlich zu informieren, so z. B. über die Besonderheiten der technisierten Kommunikation gegenüber der face-to-face-Kommunikation. Sie müssen sich ein Urteil darüber bilden können, mit welcher Radikalität eine globale Digitalisierung aller unserer Lebensbereiche voranzutreiben ist. Die sich hieraus ergebenden moralischen und ethischen Fragen sind keine Fragen der Naturwissenschaft und Technik selbst, auch nicht der Grundlagenforschung, sondern Gegenstand übergeordneter Bewertung der Anwendung von Wissenschaft und Technik.

8. Die Studierenden sollten sich darüber im Klaren sein, dass angesichts fragwürdiger militär-technischer Projekte, wie die Entwicklung von Killer-Robotern, für die Informatikerinnen, nicht erst heute, schwerwiegende moralische und ethische Fragen entstehen. Sie müssen die wirkliche Leistungsfähigkeit solcher Systeme beurteilen können, um falschen Erwartungen in eine automatisierte Kriegsführung zu begegnen. Sie sollten fachkundig vor den realen Gefahren der immer stärker angestrebten Automatisierung der Kriegsführung warnen können. Es ist ein Bann dieser neuen Waffensysteme zu erreichen, um ein erneutes sinnloses Wettrüsten zu verhindern.

9. Die so stark gewachsene Betroffenheit und Abhängigkeit des Einzelnen wie der Gesellschaft von der Informations- und Kommunikationstechnik verlangt nach einem tieferen Nachdenken über die reale Situation. Eine Gewohnheitsethik, die vor allem den engeren Wirkungskreis Familie, Beruf im Auge hat, reicht nicht mehr aus im Zeitalter globaler Verflechtungen. Auch wenn sich die humanistischen Grundlagen nicht verändert haben, so haben sich doch die Anwendungsbedingungen der Ethik in einer global arbeitsteiligen und kooperativen Welt wesentlich geändert. Es gilt also das „minimal moral principle", wie es von Joseph Weizenbaum formuliert wurde: „Don`t use computers to do what people ought not do."[21] Um Solidarität mit den Whistleblowern unser Gegenwart zu üben, ist auch die Unterscheidung von Moralität und Historizität im Sinne Hegels[22] zu berücksichtigen.

10. Wir wollen und können den wissenschaftlich-technischen Fortschritt nicht aufhalten. Die gesundheitliche Versorgung der wachsenden Bevölkerung muss gesichert und ständig verbessert werden, die Wettbewerbsfähigkeit der Wirtschaft, der Lebensstandard der Bevölkerung muss erhalten und wenn möglich erhöht werden. Gerade deshalb ist es die entscheidende Aufgabe der Wissenschaftler und Ingenieure zu gewährleisten, dass der wissenschaftlich-technische Fortschritt dem Leben, dem Wohl des Menschen dient. Das ist der humanistische Auftrag der Wissenschaft.

Dies erfolgt jedoch nicht im Selbstlauf, sondern speziell auch die Informatikerinnen müssen lernen, wie dies durch bewusste, am realen Humanismus orientierte, sozio-technische Gestaltung der automatenunterstützten Informationssysteme in sozialer Organisation zu gewährleisten ist.

Die eigentlich zu lösende Aufgabe ist, auf der Grundlage einer progressiven Gesellschaftskonzeption, die sich herausbildenden realen Entwicklungsmöglichkeiten im Horizont konkreter Utopien zu erfassen, getragen von einer konkreten humanistischen Vision, wie der einer nachhaltigen Informationsgesellschaft, die moderne Informations- und Kommunikationstechnologie so in den individuellen und gesellschaftlichen Entwicklungsprozesse zu integrieren, dass der Mensch Subjekt aller Entwicklung ist und bleibt[23].

Das sind Fragen, die sich jeder Studierende der Umweltinformatik stellen muss, will er wirklich für das Studium motiviert sein und gute Informationssysteme im Rahmen der betrieblichen Umweltinformatik und für den Umweltbereich schaffen.

Es gibt aber sicher noch weitere Fragen, die im Rahmen der Lehrveranstaltung *Umweltinformatik und Gesellschaft* zu stellen und zu beantworten sind. Dies sind nicht nur fachspezifische Probleme, die fachintern zu lösen sind. Es sind auch nicht nur soziale oder ökonomische oder ökologische Probleme, die man an andere Disziplinen delegieren kann. Es sind Probleme, die interdisziplinär oder besser noch transdisziplinär zu lösen sind. Aber gerade deshalb muss der Informatiker auf diese interdisziplinäre und transdisziplinäre Zusammenarbeit in Lehre und Forschung vorbereitet werden.

Neu sind die Probleme nicht. Wissenschaftlich-technische Entwicklungen hatten immer schon nicht vorhersehbare Nebenwirkungen und konnten auch immer schon missbraucht werden. Aber die Reichweite der ambivalenten sozialen und gesellschaftlichen Wirkungen speziell der modernen IKT, der nicht vorhersehbaren Nebenwirkungen, die Größe des mit einem fehlerhaften Funktionieren verbundenen Risikos haben sich in hohem Maße potenziert, so dass eine Einführung in diese Problemkreise durch Vorlesungen und Seminare sowie eigenständige Projektarbeiten der Studenten in der Disziplin *Informatik und Gesellschaft*[24, 25, 26] unabdingbar ist.

## Anmerkungen

1 *Seit Gründung der Hochschule für Technik und Wirtschaft Berlin und der Gründung des Studienganges Wirtschaftsinformatik und dann des Studiengangs (betriebliche) Umweltinformatik wurde das Fachgebiet Wirtschaftsinformatik und Gesellschaft und dann auch Umweltinformatik und Gesellschaft an dieser Institution gelehrt und von Klaus Fuchs-Kittowski vertreten. Im Wintersemester 2011/12 wurde diese Lehrveranstaltung zeitlich und inhaltlich sowie durch eigenständige Projektarbeit der Studenten noch erweitert. Im Wintersemester 2012/13 wurde sie aufgrund der erhöhten Studentenzahlen von Volker Wohlgemuth und Klaus Fuchs-Kittowski gemeinsam durchgeführt und wird im Wintersemester 2013/14 gemeinsam mit Frank Fuchs-Kittowski fortgeführt. Der hier gegebene Bericht bezieht sich auf die in besonders guter Zusammenarbeit mit V. Wohlgemuth durchgeführte Projektveranstaltung.*

2 *Informationssystem-, Arbeits- und Organisationsgestaltung – Informatik zwischen Technokratie und Soziokratie. 6. FIfF-Jahrestagung 1990.*

3 *Julian Nida-Rümelin (Hrsg.), Angewandte Ethik, Die Bereichsethiken und ihre theoretische Fundierung, Alfred Kröner Verlag Stuttgart, 1996*

4 *Klaus Fuchs-Kittowski, Hans A. Rosenthal und André Rosenthal: Die Entschlüsselung des Humangenoms – ambivalente Auswirkungen auf Gesellschaft und Wissenschaft, in: Erwägen Wissen Ethik, Deliberation Knowledge Ethics, EWE 16 (2005), Issue 2, S. 149- 162 (Hauptartikel), Geistes- und Naturwissenschaften im Dialog 219- 234 (Replik)*

5 *Klaus Fuchs-Kittowski, Volker Wohlgemuth, Umweltinformatik und Umweltforschung in ihrer Institionalisierung und Interdisziplinarität, in: Klaus Fischer, Hubert Laitko, Heinrich Parthey Hsrg.): Wissenschaftsforschung, Jahrbuch 2010. Wissenschaftlicher Verlag, Berlin, 2011*

6 *Andreas Möller, Arno Rolf, Nachhaltige Geschäftsmodelle, Universität Hamburg, Fachbereich Informatik, Vogt-Kölln-Str. 30, Universität Hamburg, 2003.*

7 *Mario Dompke et al (Hrsg.): Memorandum Nachhaltige Informationsgesellschaft, Freihofer IRB Verlag, Stuttgart, 2004.*

8 *Ernst Bloch, Differenzierung im Begriff Fortschritt, , Sitzungsberichte der Deutschen Akademie der Wissenschaften zu Berlin, Berlin, 1956*

9 *Klaus Fuchs-Kittowski, Horst Kaiser, Rainer Tschischwitz, Bodo Wenzlaff, Informatik und Automatisierung, Akademie-Verlag Berlin, 1976*

10 *Christiane Floyd, Christian Fuchs, Wolfgang Hofkirchner (Hrsg.): Stufen zur Informationsgesellschaft – Festschrift zum 65. Geburtstag von Klaus Fuchs-Kittowski, Peter Lang Verlag, Frankfurt a.M. 2000.*

11 *Lorenz M. Hilty. Information Technology and Sustainability – Essays on the Relationship between ICT and Sustainable Development, Books on Demand, Norderstedt, 2008*

12 *Klaus Fuchs-Kittowski, Zur Ambivalenz der Wirkungen moderner Informations- und Kommunikationstechnologien auf Individuum, Gesellschaft und Natur – Wo liegen die Potentiale und Risiken der allgegenwärtigen Datenverarbeitung?, in: FIfF- Kommunikation, transparenz, arbeit, kontrolle, 2/201, S. 36-45*

13 *Christian Fuchs, Wolfgang Hofkirchner, Studienbuch Informatik und Gesellschaft, Books on Demand, Norderstedt, 2003, S. 120 ff.*

14 *Donella H. Meadows, Dennis l. Meadows, Jorgen Randers, William W. Behrens: „Die Grenzen des Wachstums, Stuttgart, DVA, 1972*

15 *Ernst Ulrich von Weizsäcker, Amory B. Lovins, L. Hunter Lovins, Faktor vier: Doppelter Wohlstand – halbierter Naturverbrauch, Der neue Bericht an den Club of Rome, Droener Knaur, 1995*

16 *Ernst Ulrich von Weizsäcker, Das Jahrhundert der Umwelt – Vision: Ökoeffizient leben und arbeiten, Campus Verlag, Frankfurt/New York, 1999*

17 *Franz Josef Radermacher & Bert Beyers, Welt Mit Zukunft – Die Ökosoziale Perspektive, Muhrmann (überarbeitete Auflage) 2011*

18 *Klaus Fuchs-Kittowski, IT-Support of International Collektive Scientific Research to Limit the Human – induced Climate Change – The Impact of Computer (-Networks) on the Organization of Science and the Culture of Scientific Work, in: Volker Wohlgemuth (Ed): Information Technology and the Climate Change, trafo Wissenschaftsverlag, Berlin, 2009, S. 107-132*

19 *Robert Barling, Volker Wohlgemuth, Carbon Footprinting – enabeling the ecological supply chain of the future, in: Volker Wohlgemuth (Ed): Information Technology and the Climate Change, trafo Wissenschaftsverlag, Berlin, 2009, S. 77-85*

20 *Hans-Jörg Kreowski (Hg.): Informatik und Gesellschaft – Verpflichtungen und Perspektiven, Lit Verlag, Berlin 2008*

21 *siehe Klaus Fuchs-Kittowski, Report of Working Group: Computer And Ethics, in: Abbe Mowshowitz (Editor): Human Choicnd Computers,2, North-Holland, Amsterdam, 1979, S. 279*

22 *Georg Wilhelm Friedrich Hegel, Vorlesungen über die Philosophie der Geschichte, Werke, Suhrkamp, Band 12, Frankfurt am Main 1970, S. 40 und 90f*

23 *Klaus Fuchs-Kittowski, Strategies of the Effective Integration of ICT into Social Organization – Organization of Information Processing and the Necessity of Social Informatics. In: Jacques Berleur, Markku I. Nurminen, John Impagliazzo (eds): Social Informatics: An Information Society for All? In Remembrance of Rob Kling, Proceedings of the Seventh International Conference on Human Choice and Computers (HCC7), IFIP TC9, Springer Verlag, 2006, S. 431-444.*

24 *Jürgen Friedrich, Thomas Herrmann, Max Peschke, Arno Rolf (Hrsg.): Informatik und Gesellschaft. Berlin, Oxford, 1995*

25 *Christian Fuchs, Wolfgang Hofkirchner, Studienbuch Informatik und Gesellschaft, Books on Demand, Norderstedt, 2003*

26 *Hans-Jörg Kreowski (Hg.): Informatik und Gesellschaft – Verpflichtungen und Perspektiven, Lit Verlag, Berlin 2008*

Autoreninfo siehe Seite 41

**Antonia Wagner**

# Absolventenrede Sommersemester 2013[1]

Liebe Absolventinnen und Absolventen, liebe Eltern, verehrte Professoren, verehrte Gäste!

Mein Name ist Antonia Wagner. Ich habe im Bachelor *Angewandte Informatik* mit dem Schwerpunkt *Embedded Systems* studiert und darf heute zu Ihnen sprechen.

Ich weiß noch genau, wie sehr ich auf meine Zulassung für das Studium hier in Fulda gewartet habe. Zwar hatte ich das Glück und wollte in das zulassungsfreie Studium der Angewandten Informatik, dennoch hatte das offizielle Zulassungsschreiben eine Bedeutung. Endlich eintauchen in die faszinierende Welt der Technik, das „dahinter" verstehen … und dann ging es los zur Einschreibung, es war ein Donnerstagnachmittag mitten im August und der bis dato heißeste Tag des Jahres. Und so warteten wir angehenden Studenten schwitzend und uns Luft zufächelnd auf unseren ersten Studentenausweis.

Als die Einschreibung geschafft war, kam – nach dem Mathe-Vorkurs – schließlich das erste Semester. Dort lernten wir vor allem mathematische und technische Grundlagen. Aber wir hatten auch das Modul *Informatik und Gesellschaft*, das im neuen Curriculum und auch in den Studiengängen Wirtschaftsinformatik und digitale Medien nicht enthalten ist. Meiner Ansicht nach ist das schade, denn vielen Informatikern und Informatikerinnen ist es gar nicht bewusst, wie hoch ihre gesellschaftliche Verantwortung ist.

Immer mehr Lebensbereiche werden von technischen Geräten bestimmt. Allein die fast explosive Zunahme an Smartphones, deren Anzahl sich in Deutschland zwischen 2009 und 2012 auf 31 Millionen Geräte verfünffacht hat, spricht eine deutliche Sprache. Viele Endanwender nutzen ihre Smartphones ganz selbstverständlich und haben keine Ahnung, wie die Technik des Geräts funktioniert. Während den meisten Benutzern von Standrechnern noch klar war, dass es zwischen Unix und Windows einen Unterschied gibt, fehlt dieses Verständnis bei Smartphones fast vollständig. Dass iOS und Android etwas völlig anderes sind, ist vielen Besitzern von telefonierenden Minicomputern nicht mehr klar. Das Verständnis für die Technik scheint also bei einem großen Teil der Anwender immer weiter abzunehmen. Und damit wächst die Verantwortung der Entwickler. Während Schadsoftware das Mikrofon und die Kamera am Smartphone einschaltet, ahnt der betroffene Anwender vielleicht nicht einmal, dass das überhaupt möglich ist. Jeder von uns sollte sich also darüber im Klaren sein, dass wir mit unseren Kenntnissen großen Schaden anrichten können, und dass unsere Verantwortung dementsprechend hoch ist.

Das Thema Informatik und Ethik ist nicht neu, denn die Gesellschaft für Informatik hat bereits vor fast zwanzig Jahren Leitlinien zur Ethik aufgestellt und veröffentlicht. Jeder Mediziner leistet den hippokratischen Eid und bekommt erst anschließend seine medizinische Approbation. Ärzte dürfen also erst praktizieren, wenn sie ihre Arbeit der medizinischen Ethik unterworfen haben. Bei Informatikern sieht die Sache anders aus, denn ich bin sicher, dass es genug Studenten der Informatik gibt, die nicht einmal wissen, dass es ethische Leitlinien für die Arbeit in und mit der Informationstechnologie gibt. Wir sind also weit davon entfernt, unsere Arbeit der technischen Ethik zu unterwerfen. Ärzten wird ihre medizinische Approbation entzogen, und sie dürfen nicht mehr als Arzt praktizieren, wenn sie grob gegen den hippokratischen Eid verstoßen haben. Der Missbrauch von technischen Kenntnissen hat hingegen allenfalls straf- oder zivilrechtliche Konsequenzen und zieht kein Berufsverbot nach sich. Oftmals haben zweifelhafte Handlungen im Zusammenhang mit Technik aber gar keine Konsequenzen, da sie zwar unter moralischen Gesichtspunkten fragwürdig, aber nicht strafbar sind. „Weil ich es kann" oder „weil es geht" kann also weiterhin als Begründung für jemanden herhalten, der sein Projekt unbedingt durchziehen möchte. Ich hoffe, es ist allen klar, dass es deutlich bessere Argumente für ein Projekt gibt.

Aber nicht nur für unsere Projekte selbst sind wir verantwortlich. Wir sind auch verantwortlich für die Verarbeitung von unzähligen Informationen. Schlagworte wie *Big Data* verdeutlichen die sprunghafte Zunahme von digitalen Daten und deren Nutzung. Wir als Informatikerinnen und Informatiker sind dafür verantwortlich, was mit den Daten geschieht, wie diese verarbeitet werden und wie mit gefundenen Querverbindungen umgegangen wird. Wir können mit diesen Informationen enormen Schaden anrichten, denn heutzutage bedeutet Information Macht. Manch einer handelt die Information gar als den Rohstoff des 21. Jahrhunderts. Und wie viel Macht die Kontrolle der Infor-

**Antonia Wagner**

**Antonia Wagner**, Jahrgang 1986, ist Master-Studentin im Studiengang Informatik an der Technischen Hochschule Mittelhessen in Gießen. Im März 2013 schloss sie den Bachelor-Studiengang *Angewandte Informatik* an der Hochschule Fulda ab. Ihr Schwerpunkt liegt in der Technischen Informatik an der Schnittstelle zur Elektrotechnik. Darüber hinaus interessiert sie sich für wirtschaftliche und politische Themen. Aus diesem Grund ist ihr sehr daran gelegen, technische Themen auch aus der Perspektive der gesellschaftlichen Auswirkungen zu betrachten.

mation bedeutet, konnten wir zuletzt im letzten Monat in der Presse verfolgen. Google streitet sich seit Jahren mit der EU in kartellrechtlichen Fragen. Denn der Suchriese entscheidet, welche Information an welcher Position der Suchanfrage erscheint. Dienste von Google werden bei entsprechender Sucheingabe bevorzugt angezeigt, ohne dass der Benutzer dies erkennen kann. So innovativ Google auch sein mag, dieses Informationsmonopol ist gefährlich und öffnet der Beeinflussung der öffentlichen Meinung Tür und Tor. Wir sollten in unserer täglichen Arbeit also sehr darauf achten, wie wir mit den uns anvertrauten Daten umgehen und das Recht zur informationellen Selbstbestimmung stets beachten.

Zu Information gehören aber nicht nur die Daten der Benutzer, sondern auch das Wissen über die Fähigkeiten und die Funktionsweise unserer Software oder unseres Geräts. Um den Anwendern das Gefühl geben zu können, dass die Funktionalität unserer Software transparent ist, sollten wir dazu bereit sein, ihnen jederzeit zu erklären, was die Software macht und wie dies geschieht.

Ebenso ist es unsere Aufgabe, die Anwender für die Gefahren der technischen Geräte zu sensibilisieren. Bei der Installation von Software auf Smartphones ist der Glaube, dass „alles schon seine Richtigkeit hat", weit verbreitet. Wir sollten unsere Freunde und Kollegen aber auch einmal fragen, wozu die Kalender-App die Erlaubnis braucht, Kurznachrichten versenden zu dürfen. Als Absolventen aus dem in aller Munde liegenden MINT-Bereich ist es unsere Aufgabe, auch kritisch zu hinterfragen und die Antworten an die Anwender heranzutragen.

Unsere Aufgaben im Berufsleben sind vielfältig. Von der Pflege technischer Infrastruktur, über Softwareentwicklung zu Beratung, von Wissenschaft über Lehre zu Politik. Genauso vielfältig ist unsere Verantwortung, die wir bei der Ausübung unseres Berufs haben. Ich hoffe und wünsche mir, dass diese Verantwortung uns allen bewusst ist. Und dass wir alle dazu bereit sind, diese Verantwortung zu übernehmen. Dass die Bereitschaft, die uns gegebenen und erlernten Fähigkeiten sinnvoll und gewissenhaft einzusetzen, bei uns allen vorhanden ist.

In diesem Sinne wünsche ich allen, vor allem aber uns Absolventen, dass wir vor schwierigen beruflichen Entscheidungen in uns gehen und uns fragen, ob wir eine Entscheidung ethisch tragen können und wollen. Im Zweifelsfall heißt es dann, „Nein" zu sagen.

Vielen Dank.

## Anmerkung

1 *Diese Rede wurde anlässlich der Absolventenverabschiedung des Fachbereichs Angewandte Informatik der Hochschule Fulda am 7. Juni 2013 von Antonia Wagner gehalten. Es gilt das gesprochene Wort.*



**Reinhard Keil, Harald Selke, Felix Winkelnkemper**

# Informatik und Bildung – Ein Kampf um die Gestaltungshoheit in der Gesellschaft?

*Der Computer verändert die Gesellschaft! Wohl niemand würde diese Binsenweisheit inzwischen noch bestreiten. Die Konsequenzen aus der Nutzung der Technologie sind vielseitig und werden mittlerweile teils auch in einer breiten Öffentlichkeit diskutiert. Grund genug für die Forderung, sich als Fachdisziplin mit Nutzung und Gefahren der Technologie auseinanderzusetzen. Grund genug auch zu fordern, schon in der Schule verpflichtend mit der Beschäftigung mit der ja offenbar gesellschaftsrelevanten Informatik zu beginnen.*

Wenn man ein wissenschaftliches Fachgebiet wie die Informatik mit solch fundamentalen Kategorien wie Gesellschaft oder Bildung verbindet und fordert, diese möge die entstehenden Probleme analysieren und lösen, schwingt immer ein wenig Imperialismus mit. Das gilt im Hinblick auf eine beanspruchte allumfassende Gestaltungskompetenz, die offenbar alle gesellschaftlichen Bereiche durchdringt und sogar beansprucht, in absehbarer Zeit den Menschen durch künstlich intelligente Systeme ersetzen zu können. Das gilt zum anderen aber auch für eine kritisch reflektierende Informatik, die meint, nur weil man in allen gesellschaftlichen Bereichen mit Problemen mit der Informationstechnik konfrontiert wird, hier auch eine entsprechende Lösungskompetenz beanspruchen zu können bzw. gar zu müssen. Es geht um die universelle und unverzichtbare Kompetenz der Informatik für die Gesellschaft, denn nichts anderes spiegelt sich letztlich in den Verknüpfungen wider, in denen das Fachgebiet über das Wörtchen „und" mit Kategorien wie Bildung oder Gesellschaft verknüpft wird.

Dabei ist nicht entscheidend, ob die Informatik bedeutsam ist – sie ist unverzichtbar für unsere gesellschaftliche Entwicklung. Es geht auch nicht darum, ob die Probleme, die mit der Kommunikations- und Informationstechnik verbunden sind, unbedeutend sind – sie sind es nicht, denn ihre Beherrschung entscheidet über Fluch und Segen dieser Technik. Es stellt sich jedoch die Frage, welchen kompetenten und verantwortlichen Beitrag die Informatik hierbei leisten kann.

Kritiker wie Befürworter innerhalb der Informatik müssen sich in Zurückhaltung üben, wenn es um ihre Problemlösungskompetenzen geht, wenn es um die vielfältigen Wechselwirkungen zwischen der technologischen und der gesellschaftlichen Ent-

wicklung geht. Für diese kann nicht allein die Informatik zuständig sein. Unterschiedliche Disziplinen wie z. B. Soziologie, Politologie, Recht, Wirtschaftswissenschaften oder auch (Technik-) Philosophie müssen einbezogen sein. Warum sollte ausgerechnet die Informatik mit ihrem spezifischen, aber zugleich auch beschränkten mathematisch-technischen Methodenrepertoire die Disziplin sein, der es gelingen könnte, solche Wechselwirkungen wissenschaftlich zu durchdringen? Unabhängig davon, ob die Informatik als Verursacherin dieser Probleme angesehen wird, kann man ihr noch lange nicht die Kompetenz attestieren, auch allein angemessene Lösungen entwickeln zu können. Wenn andere Disziplinen an der Bearbeitung der Probleme mitarbeiten sollen – und das müssen sie –, dann kann das kaum unter der Fachhoheit der Informatik erfolgen.

Die Informatik muss sich zweifelsohne den aktuellen gesellschaftlichen Herausforderungen stellen und sich aus ihrer Sicht und mit ihrer Kompetenz am gesellschaftlichen Diskurs beteiligen. Soweit sie sich dabei als wissenschaftliche Disziplin versteht, muss sie aber auch mit den Beschränkungen einer wissenschaftlichen Herangehensweise umgehen und sich entsprechend in Bescheidenheit üben. Diese Bescheidenheit betrifft auch den Alltag von Hochschulbildung und Allgemeinbildung, der nicht allein durch hehre Absichten geprägt sein darf, sondern auch Kompetenz, Verantwortung und interdisziplinäre Anknüpfung berücksichtigen muss. Welche Konsequenzen das neben dem kritischen Blick auf grundlegende Begriffe und fundamentale Kategorien mit sich bringt, wollen wir nachfolgend am Beispiel unserer eigenen Praxis skizzieren.

## Kompetenz und Verantwortung

Das folgende Beispiel aus der Ausbildungspraxis an der Universität soll zeigen, wie wichtig Kompetenz in Bezug auf Verantwortung ist. Es soll verdeutlichen, dass man, wenn man sich bewusst mit einer Kompetenz in einen Diskurs einbringt, auch für diese Kompetenz geradestehen (können) muss. Anders ausgedrückt: Das was zu verantworten ist, muss auch mit den vorhandenen Kompetenzen gestaltbar sein.

In einem Softwarepraktikum an der Universität übernahm eine Gruppe von Mitarbeitern, die nicht zum Lehrteam gehörte, die Rolle der Benutzer, für die ein System entwickelt werden sollte. Den Studierenden wurde gesagt, dass sie mit diesen Benutzern die Anforderungen absprechen müssten und dass es letztlich die Abnahme des Systems durch diese Nutzer sei, die über Erfolg oder Misserfolg ihrer Arbeit entscheide. Normalerweise sollte man annehmen, dass die Studierenden, also die Entwickler der Software, versuchen, die Anforderungen in einem überschaubaren bzw. „verantwortbaren" Rahmen zu halten, auch, um den eigenen Erfolg am Ende der Veranstaltung nicht zu gefährden. Genau dies passierte jedoch nicht. Die „Benutzer", die die Aufgabe hatten, ihre Wünsche möglichst weitgehend zu artikulieren, setzten in der Frühphase des Projekts eine Anforderung nach der anderen durch, ohne dass die Entwickler wirklich kritisch analysierten, ob sie denn in der vorhandenen Zeit und mit den vorhandenen Ressourcen diese Anforderungen umsetzen konnten. Auch der nochmalige Hinweis durch die Lehrenden, dass der beschlossene Anforderungskatalog das Kriterium für die Abnahme des Projekts darstelle, führte zu keinerlei Revisionen. Das Ende war vorhersehbar: Alle Projektteams blieben in diversen Schwierigkeiten stecken und konnten bei weitem nicht das von den Nutzern Gewünschte umsetzen. Daraufhin erhob sich ein Protest, in dem alle Beteiligten wortreich darlegten, dass die vereinbarten Anforderungen eigentlich überhaupt nicht in der Zeit und mit den vorhandenen Ressourcen hätten erledigt werden können, es somit selbstverständlich sei, dass die Nutzer am Ende nicht das hätten erhalten können, was sie am Anfang gefordert haben.

Nun kann man den Mangel an Verantwortung für die eigenen Versprechen in diesem Falle mit der Unerfahrenheit der beteiligten Studierenden erklären und letztlich geschädigt wurde hier ja auch niemand. Übertragen lässt sich dieses Beispiel aber auch auf die Versprechungen eines Fachgebiets wie Informatik und Gesellschaft, das verspricht, die gestellten Anforderungen zu erfüllen, und dabei gar nicht merkt, dass viele der notwendigen Kompetenzen ja gar nicht in einem Themenfeld liegen, das in dieser Allgemeinheit mit den Kompetenzen, die Informatiker üblicherweise mitbringen, wissenschaftlich zu bearbeiten wäre. Schlimmstenfalls geraten dann auch die Aspekte aus dem Blickfeld, in denen die Informatik eben doch kompetente Beiträge zum Diskurs liefern kann. Als Beispiel für solche Aspekte sei hier auf den Kollegen Christoph Sorge verwiesen, der im Rahmen der Arbeitsgruppe *Codes und Kryptographie* unter der Bezeichnung *Sicherheit in Netzwerken* viele Themenstellungen bearbeitet, die nach einem breiten Verständnis auch unter dem Stichwort Informatik und Gesellschaft verzeichnet werden könnten[1].

All dies bedeutet nicht, dass es keine wichtigen oder gar wegweisenden Arbeiten und Projekte im Bereich *Informatik und Gesellschaft* gegeben hätte, aber es bedeutet schon, dass die Zusammenfassung unter diesem Oberbegriff keine klare Perspektive verkörpert und damit auch keine forschungsstrategischen Positionen in der Informatik eröffnet[2]. Möglicherweise ist dies einer der Gründe, warum die Fachgebietsbezeichnung *Informatik und Gesellschaft* zunehmend aus den Fachgebietsübersichten der Informatik an den deutschen Hochschulen verschwindet. Auch unser eigenes Fachgebiet haben wir schon vor einiger Zeit in *Kontextuelle Informatik*[3] umbenannt[4]. Denn unsere Forschung und Lehre drehen sich nicht um grundlegende gesellschaftliche Fragestellungen, sondern um die Identifikation von Bereichen, in denen unter Berücksichtigung des Kontextes des Einsatzes von Informatiksystemen Gestaltungsoptionen und ihre Konsequenzen frühzeitig erkannt, Entwicklungsmethoden verbessert, neue Lösungsansätze gefunden und negative Folgen eingeschränkt werden können. Die von uns identifizierten Probleme können nur unter Zuhilfenahme von Informatikkompetenz gelöst werden; die Informatik allein reicht für ihre Lösung aber in der Regel nicht. Wir sehen es also als unsere Aufgabe, Ansätze und Konzepte zu entwickeln, die die Anschlussfähigkeit der Informatik für den interdisziplinären Diskurs in den jeweiligen Problembereichen sichern[5]. Wir verstehen uns somit weder als die besseren Informatiker, noch übernehmen wir stellvertretend für die Kolleginnen und Kollegen die Verantwortung für die Informatik, sondern wir steuern einen kleinen, aber relevanten Teil zur Weiterentwicklung der Informatik bei. Und das erfordert auch Bescheidenheit in der Namensgebung und damit in der beanspruchten Gestaltungskompetenz.

## Informatik und Gesellschaft in der Hochschulbildung

Ungeachtet der genannten Probleme von *Informatik und Gesellschaft* als Forschungsgebiet wird im Rahmen der Hochschulbildung in der Informatik immer wieder die Forderung laut, Inhalte von gesellschaftlicher Relevanz im Curriculum zu verankern. Das angestrebte Themenspektrum ist dabei sehr breit. Allein das Themenspektrum einschlägiger Lehrbücher[6] oder auch das Curriculum für ein *Fernstudium Informatik und Gesellschaft*[7] sind beeindruckend umfangreich und vielfältig. So vielfältig, dass man sich schon die Frage stellen muss, ob ein solches Themenspektrum jemals an einer Institution oder in einem Studiengang lehrbar sein kann. Für ein Fachgebiet ebenso wie für einzelne Lehrveranstaltungen ist eine solche Vielfalt interdisziplinärer und komplexer Fragestellungen zu umfangreich und letztlich unseriös.

Gewiss kann man argumentieren, dass es nicht darum geht, jeweils alles abzudecken, doch stellt sich dann die Frage, wie denn eine Auswahl erfolgen kann und wie diese Auswahl belegen kann, dass sie exemplarisch und unverzichtbar ist. Genau hier liegt die Crux: Wenn bestimmte Inhalte als unverzichtbar angesehen werden, sie gleichzeitig aber nicht genauer eingegrenzt oder definiert werden können, dann stellt sich die Frage, welche Art von Kompetenz damit eigentlich vermittelt werden soll. Noch schwieriger ist zu beantworten, über welche Kompetenz die Vermittler verfügen sollten. Selbstverständlich gehört zu einem ordentlichen Studium die Notwendigkeit, die Kompetenzen zu erweitern und über den Tellerrand hinausschauen zu können. In vielen Studiengängen und Universitäten erfolgt genau dieses unter dem Begriff *Studium Generale*. In einigen Studiengängen gibt es zudem auch Lehrveranstaltungen zum Thema *Informatik und Gesellschaft*. Doch stellt sich natürlich auch für die Lehre die Frage, warum es sinnvoll sein sollte, alle auftretenden Grenzüberschreitungen nur aus dem Blickwinkel der Informatik heraus zu betrachten.

Zwar kann man in der Lehre auch in Veranstaltungen zum Thema *Informatik und Gesellschaft* die Auseinandersetzung der Studierenden mit den Wechselwirkungen zwischen Informatik und Gesellschaft unter Rückgriff auf entsprechende (dann oft fachfremde) Literatur fördern – allerdings um den Preis, dass das Humboldtsche Ideal der Verbindung von Forschung und Lehre nicht mehr umsetzbar ist, da es den Universalgelehrten vergangener Jahrhunderte erforderte. Letztlich bleibt auch hier ein Sammelgebiet, das als Ausdruck eines schlechten Gewissens zwar nachvollziehbar, in seiner Essenz aber nahezu nicht erschließbar ist. Die Unfähigkeit oder Unwilligkeit, sich hier auf für Informatiker beherrschbare und damit auch verantwortbare Problemstellungen einzuschränken – d.h. zu wollen, ohne das Können belegen zu können –, ist letztlich nicht verantwortbar.

Die Informatik grenzt sich als Fachdisziplin von anderen ab. Dass die von ihr benutzten Begriffe, Kategorien und Metaphern wie z. B. *Informationsverarbeitung*, *virtuelle Realität* oder *intelli-*






**Reinhard Keil, Harald Selke, Felix Winkelnkemper**

Prof. Dr.-Ing. **Reinhard Keil** ist seit 1992 Professor für Kontextuelle Informatik am Heinz Nixdorf Institut der Universität Paderborn. Promotion (1985) und Habilitation (1991) an der TU Berlin im Fachbereich Informatik. Über 170 Veröffentlichungen, Herausgeber von 15 Büchern und der Zeitschrift „Erwägen Wissen Ethik". Forschungsschwerpunkte: E-Learning, Kooperationsunterstützende Systeme, Gestaltung digitaler Medien, verteilte Wissensorganisation, Software-Ergonomie.

**Harald Selke** ist wissenschaftlicher Mitarbeiter in der Fachgruppe Kontextuelle Informatik im Heinz Nixdorf Institut der Universtität Paderborn und bietet dort unter anderem die Vorlesung *Informatik und Gesellschaft* an. Er studierte in Paderborn Mathematik und Informatik und promovierte 2009 im Bereich E-Learning. Seine Forschungsschwerpunkte sind die Unterstützung von Lehr- und Lernprozessen durch digitale Medien, die Entwicklung ko-aktiver Systeme und die Gebrauchstauglichkeit von Web-Applikationen.

**Felix Winkelnkemper** studierte Informatik an der Universität Paderborn und ist wissenschaftlicher Mitarbeiter in der Fachgruppe Kontextuelle Informatik des Heinz Nixdorf Instituts. Er arbeitet dort unter anderem zu den Themen visuelle Wissensorganisation, technische Potenziale digitaler Medien, Lernunterstützung und Software-Ergonomie.

Kontaktinformationen: Prof. Dr.-Ing. Reinhard Keil, Dr. Harald Selke, Felix Winkelnkemper, Kontextuelle Informatik, Heinz Nixdorf Institut, Universität Paderborn, Fürstenallee 11, 33102 Paderborn *(reinhard.keil@hni.uni-paderborn.de, hase@uni-paderborn.de, winfel@uni-paderborn.de; koi.uni-paderborn.de).*

*gentes System* diese Grenzen vielfach überschreiten, ist nicht nur ein terminologisches Problem, sondern auch eins in Bezug auf geweckte Erwartungen (Redlichkeit) und adäquate Lösungsansätze (Angemessenheit). Solch überzogene Erwartungen kann man aber auch wecken, wenn man unter dem Stichwort *Informatik und Gesellschaft* eine zu große gesellschaftliche Gestaltungskompetenz nicht nur für die universitäre, sondern auch für die Allgemeinbildung beansprucht.

## Informatik und Allgemeinbildung

Die weitreichende Bedeutung der Informations- und Kommunikationstechniken könnte jedoch zumindest die Notwendigkeit eines Schulfachs Informatik begründen. Derzeit ist Informatik nur in wenigen Bundesländern ein Pflichtfach und, so wird verschiedentlich beklagt, nicht gleichberechtigt zu anderen Fächern wie beispielsweise den naturwissenschaftlichen. Hier soll nicht hinterfragt werden, ob diese Forderung generell sinnvoll ist. Interessant ist jedoch, welche Begründungen für ein Pflichtfach Informatik angeführt und welche Inhalte vorgeschlagen werden. In den Empfehlungen *Grundsätze und Standards für die Informatik in der Schule* der Gesellschaft für Informatik aus dem Jahr 2008 wird u. a. dargelegt, welche Bedeutung nach Auffassung der GI der Informatik in der Sekundarstufe I zukommt. In einem Rückgriff auf Klafki zur Rechtfertigung von Informatik bzw. Technik in allgemein bildenden Schulen, dass Bildung insbesondere als Auseinandersetzung mit aktuellen und sich abzeichnenden Frage- und Problemstellungen von gesellschaftlicher Relevanz zu verstehen sei, folgern die Autoren, dass Informatikunterricht eine Chance biete, einer nicht näher bezeichneten Fehlentwicklung entgegenzuwirken, die einen „Mangel an … technisch orientierten Fachkräften“ zur Folge habe. (Gesellschaft für Informatik, 2008, S. 9f.) Dabei wird betont, dass die Auseinandersetzung mit der Nutzung und den Anwendungsmöglichkeiten im Vordergrund zu stehen habe: „Dies erfordert die Kompetenz, die Einsatzbereiche der Informatik einschließlich der Auswirkungen zu analysieren und einzuschätzen.“ (ebd., S. 10)

Gerade für diese Fragestellungen stellt jedoch die Fachwissenschaft Informatik weder die fachlichen Grundlagen noch die Methoden bereit. Nach Auffassung der GI müssen für den Erwerb „informatischer Kompetenzen“ tatsächlich eben gerade die Grenzen des Fachs verlassen werden. Dass die demzufolge notwendige Interdisziplinarität innerhalb des Fachs Informatik erfolgen soll (ebd.), ist durchaus problematisch, denn ein interdisziplinäres Fach ist ein Oxymoron. Das zeigt sich auch in den vorgeschlagenen Inhalten: Neben der Forderung, dass in der Unterstufe die Grundbegriffe der Objektorientierung erlernt werden sollen, findet sich auch, dass in der Mittelstufe die Auswirkungen der Automatisierung auf die Arbeitswelt bewertet werden sollen. Eine wahrlich nicht triviale Aufgabe, mit der sich wissenschaftlich ausschließlich andere Disziplinen befassen!

Im Gegensatz zu den Auswirkungen des Einsatzes von Informatik-Technologien ist die Modellierung (wie auch viele andere der in den Empfehlungen genannten Inhalte) sicherlich ein Gegenstand der Informatik; jedoch stellt sich gerade hier die Frage, in wie weit diese Inhalte zur Allgemeinbildung beitragen. Die Autoren postulieren: „Die Bedeutung der Informatik liegt darin, dass sie die Strukturen und Methoden des Denkens und Arbeitens nahezu aller Disziplinen und damit den beruflichen und privaten Alltag jedes Einzelnen betrifft und permanent verändert.“ Eine ernsthafte kritische Auseinandersetzung mit solchen Aussagen scheint uns nicht nur lohnend, sondern unverzichtbar, wenn man fachliche Inhalte jenseits aktueller politischer Wellen nachhaltig in der Allgemeinbildung verankern will.

Aus unserer Sicht stellt sich die Frage, ob es sinnvoll ist, die Thematisierung der Auswirkungen der Informations- und Kommunikationstechniken an der Informatik oder anderen wissenschaftlichen Fächern zu orientieren. Könnte es nicht gerade unter allgemeinbildenden Gesichtspunkten generell sinnvoller und nützlicher sein, sich verstärkt (fächer-)übergreifenden Fragestellungen zu widmen – was allerdings ein stark verändertes Schul- bzw. Fachkonzept erfordern würde. Das ist jedoch nicht so einfach umzusetzen, denn dafür müsste auch die Lehrerausbildung grundlegend geändert werden. In den meisten Bundesländern wird sie seit der Auflösung der Pädagogischen Hochschulen als Teil der wissenschaftlichen Bildung konzipiert und bewegt sich damit im universitären Kontext entlang des Fächerkanons der Fachdisziplinen.

Die Ausbildung von Pädagogen für die o. a. Fragestellungen ist aber nicht gegeben. Nach Paech & Poetzsch-Heffter (2013, S. 248) finden sich nur in „deutlich weniger als 50 %“ der Informatikstudiengänge wenigstens ein Modul, das sich mit der Thematik im weitesten Sinne befasst. Wenn es dennoch existiert, dann in einer Vielzahl von sehr individuellen Ausprägungen. Das wäre für sich allein genommen auch nicht problematisch, aber es ist problematisch im Hinblick auf einen Allgemeinbildungsansatz, in dem von einem Informatiklehrenden erwartet wird, die Auswirkungen der Automation auf die Gesellschaft mit den Schülern und Schülerinnen zu erarbeiten. Kann man das angesichts der Überforderung und der Alltagssituation an unseren Schulen wirklich ernst meinen oder reduziert es nicht sehr auf einen Cartoon aus der Zeit der Studentenbewegungen, wo der Mathematikdozent vor seiner Tafel stehend sagt: „Die Studenten haben mich aufgefordert zu lehren, dass der bürgerliche Staat korrupt sei. Nun gut: der bürgerliche Staat ist korrupt. Kehren wir nun zum Problem der deckungsgleichen Dreiecke zurück.“

## Zusammenfassung

Die Auswirkungen der Informatik betreffen uns alle. Ein gesellschaftlicher Diskurs über Chancen und Probleme des Einsatzes von Informationstechnik ist wichtig und muss auf jeder Ebene unterstützt werden, also speziell natürlich auch in Schule und Hochschule. Ein Fehler liegt aber u.E. darin begründet, dass man in der Diskussion zu wenig Wollen und Können zusammenbringt.

Wenn ein Schulfach Informatik sich auch mit grundlegenden gesellschaftlichen Problemen befassen soll, dann muss das auch einen seriösen Niederschlag in den Informatik-Studiengängen und damit auch der Lehrerbildung finden. Dies war und ist nicht der Fall und es ist gegenwärtig auch nicht absehbar.

Ein weiterer Gesichtspunkt ist die Frage, für welche Problemstellungen man tatsächlich eine fachliche Kompetenz beanspruchen

und vor allem auch glaubhaft umsetzen kann. Ein Schulfach in der hier angesprochenen Breite zu fordern, ohne sicherstellen zu können, dass man dafür auch die notwendigen Kompetenzen und die erforderlichen Ressourcen besitzt, dürfte ähnlich ausgehen wie das weiter oben beschriebene Projektbeispiel.

Der in der Konsequenz vielleicht wichtigste Gedanke aber wäre: Wenn man wirklich Verantwortung übernehmen will, darf man nicht alle Probleme der Welt auf sich laden, sondern muss sich auch hier bescheiden. Andernfalls läuft man Gefahr, dass man nicht halten kann, was man verspricht. Die Informatik leistet einen wichtigen Beitrag für die Gesellschaft, ist vielleicht sogar unverzichtbar, aber es ist und bleibt ein Beitrag unter vielen. Je genauer und präziser dieser benannt werden kann, desto wirksamer und nachhaltiger kann er auch in der Bildung verankert werden.

## Referenzen


Gesellschaft für Informatik e. V.: Grundsätze und Standards für die Informatik in der Schule – Bildungsstandards Informatik für die Sekundarstufe I, 2008

Keil, R.: Hypothesengeleitete Technikgestaltung als Grundlage einer kontextuellen Informatik. In: Breiter, A., Wind, M. (Hrsg.): Informationstechnik und ihre Organisationslücken. Soziale, politische und rechtliche Dimensionen aus der Sicht von Wissenschaft und Praxis. Berlin: LIT-Verlag, 2011

Keil-Slawik, R.: Von Informatik und Gesellschaft zum Kontext der Informatik. FIfF-Kommunikation 18 (4), Dezember 2001, S. 39-45

Paech, B., Poetzsch-Heffter, A.: Informatik und Gesellschaft: Ansätze zur Verbesserung einer schwierigen Beziehung. Informatik Spektrum 36 (3) 2013, S. 242-250

Rohde, M., Wulf, V.: Sozio-Informatik. Informatik Spektrum 34 (2) 2011, S. 210-213

Tübingen 1999: Tübinger Studientexte Informatik und Gesellschaft. 10 Hefte. Herausgegeben von H. Klaeren und anderen. Wilhelm-Schickard-Institut für Infomatik, Universität Tübingen,1999


## Anmerkungen

1 *Siehe http://www.cs.uni-paderborn.de/?csorge.*

2 *Vgl. zur Vielfalt der Ansätze und Inhalte u. a. die Beiträge in der FIfF-Kommunikation Heft 4/2001, Heft 2/2009 und Heft 3/2009.*

3 *Siehe https://www.hni.uni-paderborn.de/koi/.*

4 *Eine ausführlichere Begründung hierzu findet sich in Keil-Slawik (2001).*

5 *z. B. im Rahmen der Sozio-Informatik (Rohde, Wulf 2011) oder einer hypothesengeleiteten Technikgestaltung (Keil 2011)*

6 *Siehe z. B. Friedrich, Herrmann, Peschek, Rolf (1995).*

7 *Tübingen (1999)*

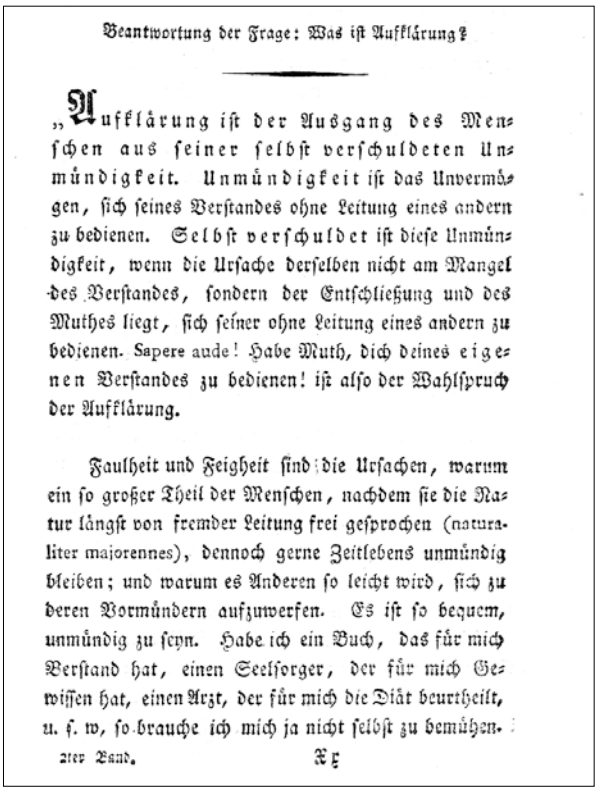


**Bernd Robben**

# Zu Bernard Stieglers pharmakologischer Medientheorie

## *Denken bis an die Grenzen der Maschine, Die Logik der Sorge. Verlust der Aufklärung durch Technik und Medien* und *Von der Biomacht zur Psychomacht*

Die berühmte Frage von Immanuel Kant, „Was ist Aufklärung", ist einer der zentralen Ausgangspunkte für Bernard Stieglers pharmakologische Medientheorie. Er analysiert, wie Medien zur Formierung unseres Wollens und Denkens beitragen. Medien fasst er als *Pharmaka* auf, die gemäß der griechischen Wortbedeutung gleichzeitig Gifte und Heilmittel sein können. Stiegler klagt den möglichen Verlust der Aufklärung durch Technik und Medien an, die in einer „Zerstörung der Sorge als Aufmerksamkeit, Achtsamkeit und Anerkennung" mündet. Kant hat gezeigt, dass die Epoche der Aufklärung die Mündigkeit „als Stadium der kollektiven Individuation" hervorgebracht hat. Für diese Entwicklung hat das Buch als „kritikfähige Unterstützung der Wissensformen" (LS 32) eine zentrale Funktion. Stiegler fragt, welche Lehren sich für die heutige Situation aus dem Zeitalter der Aufklärung ziehen lassen. Er entwickelt seine Medientheorie also von einem ethischen Anspruch aus, formuliert das *Prinzip Verantwortung* neu. Explizit bezieht er sich dabei auf Hans Jonas, der die „Frage der Verantwortung, die wir den kommenden Generationen im spezifischen Kontext der industriellen Welt schulden" (LS 70) gestellt hat. „Handle so, daß die Wirkungen deiner Handlung verträglich sind mit der Permanenz echten menschlichen Lebens auf Erden" (Jonas 2003, S. 36), so hatte dieser den Kantschen kategorischen Imperativ umformuliert. Mit Jonas hat Stiegler außerdem gemeinsam, dass ihr Denken sehr viel Martin Heidegger schuldet.[1]



Beantwortung der Frage: Was ist Aufklärung?

„Aufklärung ist der Ausgang des Menschen aus seiner selbst verschuldeten Unmündigkeit. Unmündigkeit ist das Unvermögen, sich seines Verstandes ohne Leitung eines andern zu bedienen. Selbst verschuldet ist diese Unmündigkeit, wenn die Ursache derselben nicht am Mangel des Verstandes, sondern der Entschließung und des Muthes liegt, sich seiner ohne Leitung eines andern zu bedienen. Sapere aude! Habe Muth, dich deines eigenen Verstandes zu bedienen! ist also der Wahlspruch der Aufklärung.

Faulheit und Feigheit sind die Ursachen, warum ein so großer Theil der Menschen, nachdem sie die Natur längst von fremder Leitung frei gesprochen (naturaliter majorennes), dennoch gerne Zeitlebens unmündig bleiben; und warum es Anderen so leicht wird, sich zu deren Vormündern aufzuwerfen. Es ist so bequem, unmündig zu seyn. Habe ich ein Buch, das für mich Verstand hat, einen Seelsorger, der für mich Gewissen hat, einen Arzt, der für mich die Diät beurtheilt, u. s. w, so brauche ich mich ja nicht selbst zu bemühen.

ater Band. Xx

Jonas geht davon aus, dass es eine neue Dimension der Verantwortung gibt, seitdem die moderne Technologie eine derartige Größenordnung angenommen hat, dass es zu einer globalen Verletzlichkeit der Natur gekommen ist (Jonas 2003, S. 26ff). 1979 – beim Erscheinen des Buches von Jonas – ist die Welt gekennzeichnet von der atomaren Bedrohung der Supermächte USA und UdSSR, die sich im Kalten Krieg befinden und ihre Atomraketentechnik immer stärker hochrüsten. Die Katastrophe im sowjetischen Atomreaktor von Tschernobyl steht kurz bevor. Auf die Frage, was in einer solch bedrohlichen Situation als Kompass für ethisches Handeln dienen kann, antwortet Jonas mit einer *Heuristik der Furcht*. Da wir erst wissen, „was auf dem Spiele steht, wenn wir wissen, *dass* es auf dem Spiele steht", muss die Ethik eine der *Ehrfurcht* sein (Jonas 2003, S. 8). Weil Menschen viel eher wissen, was sie nicht wollen, als das, was sie wollen, kann die Furcht ein relativ zuverlässiger Wegweiser sein, „muss die Moralphilosophie unser Fürchten vor unseren Wünschen konsultieren" (Jonas 2003, S. 64). Das so konzeptualisierte *Prinzip Verantwortung* begründet maßgeblich die Ethik der Friedensbewegung, der Ökologie sowie der Bewegung gegen Gentechnik und hat auch die ethischen Leitlinien des FIfF beeinflusst.

Stiegler formuliert seine Theorie dagegen nicht vor dem Hintergrund der Gefahren industrieller Großtechnologien und atomarer Katastrophen, sondern vor der Folie der zunehmenden Mediatisierung der Welt. Deshalb spricht er sich gegen einen Diskurs aus, der auf einer *Heuristik der Furcht* gründet, weil diese nicht fähig sei, „eine neue soziale Organisation der Aufmerksamkeit und der Sorge hervorzubringen" (LS 70). Denn das auf das Fürchten basierte Prinzip der Sorge ignoriert das Wünschen gänzlich. Weil aber „der *Gegenstand der Aufmerksamkeit* zunächst ein *Objekt des Begehrens* ist" (LS 70), muss eine vom Medium aus gedachte Ethik sich auf andere Prinzipien berufen.

Dafür macht Stiegler Anleihen bei Michel Foucault, einem anderen Denker über Aufklärung (Foucault 2005a und 2005b). Kants kritisches Denken hat die Begründung für eine Metaphysik und Transzendentalphilosophie zum Ziel; Foucault radikalisiert diese Kantsche Kritik derart, „dass die Kritik nicht mehr in der Suche nach formalen Strukturen von universalem Wert praktiziert wird, sondern als historische Untersuchung, welche die Ereignisse durchläuft, die uns dazu veranlasst haben, uns als Subjekt dessen, was wir tun, denken und sagen, zu konstituieren und zu erkennen" (Foucault 2005a, S. 702). Das philosophische Arbeiten von Foucault befasst sich sein ganzes Leben lang – immer wieder neu ansetzend – mit den *Technologien des Selbst* (Martin et al 1993). Um das Werden von Subjekten zu begreifen, gilt es, vier Typen von Technologien zu erfassen – die Technologien der Produktion, die Technologien der Zeichensysteme, die Technologien der Macht und die Technologien des Selbst (Foucault 2005c, S. 968) – und die Praktiken des Zusammenwirkens von Menschen, Objekten und Maschinen zu beschreiben.

In diesem Sinnzusammenhang wird die Technikfrage zu *dem* zentralen philosophischen Thema: Das technische Objekt figuriert darin nicht mehr als an sich bedeutungsloses Werkzeug, Instrument und bloßes Mittel zum Zweck, sondern taucht unübersehbar im Innersten der Sinnkultur auf. Über die *Existenzweise technischer Objekte* hat in den 1950er Jahren Gilbert Simondon nachgedacht, ein heute fast vergessener Theoretiker. Aufbauend auf dessen Theorie, dass technische Objekte „Mediateure zwischen der Natur und dem Menschen sind" (Simondon 2012, S. 9) beabsichtigt Stiegler, die Technikfrage von Grund auf neu zu stellen. Simondons Denken hat sich sowohl gegen die seinerzeit aufkommende Kybernetik gewandt, die Robotern den Status von Lebewesen zuspricht, als auch gegen eine technikfeindliche Kulturauffassung, die davon ausgeht, dass technische Objekte keine menschliche Wirklichkeit beinhalten. Einen Gegensatz zwischen Kultur und Technik, Mensch und Maschine aufzustellen, hält Simondon für grundfalsch. Im Mittelpunkt seines Denkens steht nicht die Frage, *was* denn Technik ist, sondern *wie* sie funktioniert. Dabei gibt es einen *unmündigen* Umgang mit Technik, wobei diese nur zweckgebunden benutzt wird, man sich nie reflexiv die Frage nach ihrem Funktionieren stellt. Ein *mündiger*, quasi ingenieursmäßiger Umgang mit Technik dagegen sucht immer zu ergründen, wie ihr Funktionieren zustande kommt. Dazu gehört die Erkenntnis, dass sich im technischen Objekt menschliches Wissen inkarniert hat. Ein Kind, das ein solches technisches Objekt noch unmündig benutzt, kann davon nichts wissen. Aber will es erwachsen und mündig werden, muss es sich reflektierend auf solch reflexive Technologie beziehen. „Das technische Objekt ist nicht diese oder jene, *hic et nunc* gegebene Sache, sondern das, was eine Genese durchläuft. Die Einheit des technischen Objekts, seine Individualität, seine Artzugehörigkeit, sind die Konsistenz- und Konvergenzeigenschaften seiner Genese" (Simondon 2012, S. 14).

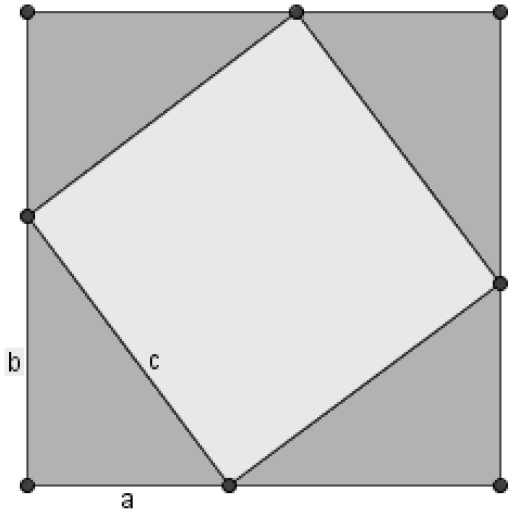
Bernard Stieglers an Medien orientierte Verantwortungsethik stellt sich in einen derartigen Prozess der Zeitlichkeit der Medien. Ein mündiger Umgang verlangt die Einsicht in das eigene Verwobensein mit solchem Zeitwerden der Medien. Anstatt wie Jonas eine *Heuristik der Furcht* gegen die aktuelle Bedrohung versucht er eine *Logik der Sorge* zu konzipieren. Zu erklären ist zunächst, wie solches Verwobensein in den Prozess des Werdens funktioniert, in einen Prozess des Werdens, der von den Menschen weder autonom gesteuert noch völlig durchschaut werden kann. Es geht um einen Diskurs über Bildung, der nicht nur vom Menschen ausgeht, sondern sich reflektierend auf reflexive Technologien bezieht. Stiegler versucht ihn in einer weiten historischen Perspektive zu beschreiben. Dabei beginnt er mit einer eigenen Variante der Erzählung des Mythos vom Ursprung als Grundlage der Technikfrage.

## Der Ursprungsfehler als Potenzial

Für Stiegler ist die Frage nach der Technik zu verstehen „als der *vergessene* Ursprung aller Fragen, aber auch als die Frage des von mir so genannten *fehlenden Ursprungs, Ursprungsfehls bzw. Ursprungsfehlers*" (DM 33). Dafür erzählt er den griechischen Schöpfungsmythos über die Titanen Prometheus und Epimetheus. Aber entgegen der Tradition stellt er nicht Prometheus, der die Menschen aus Lehm schuf, in den Mittelpunkt, sondern seinen zerstreuten Zwillingsbruder Epimetheus. Auf dessen Bitte hin lässt ihn Prometheus die von Zeus verliehenen „*dynameis*, die ‚Qualitäten', ‚Eigenschaften' oder wörtlicher ‚Kräfte', die dem Ton Form geben verteilen" (DM 47). Der Naivling Epimetheus vergisst dabei die Menschen, so dass wir Sterblichen durch den Fehler des Epimetheus ohne festgelegte Eigenschaften bleiben. Prometheus stiehlt daraufhin dem Schmied Hephaistos und der Göttin Athene die *technai* und gibt sie den Sterblichen, de-

ren Schicksal deshalb ist, ohne festgelegte Eigenschaften und *prothetisch* zu sein. „Damit zeigt der Mythos, dass die Zeit […] einer ursprünglichen Technizität oder Prothezität entspringt" (DM 49). Menschen sind deshalb künstlich und technisch, da sie „ihr Sein nicht in sich selbst finden. […] Die Menschen müssen ihr Sein, ihre Existenz, *erfinden*" (DM 49f). Wir Sterblichen bedürfen der Bildung.

Wissen ist uns nicht einfach gegeben, sondern wir erlangen es nur, wenn wir es begehren, wenn wir es in einem zeitlichen Prozess quasi durch die Einverleibung von außerhalb von uns liegenden Dingen erfahren. Um einen Gegenstand zu denken, müssen wir ihn veräußerlichen. In der Auseinandersetzung mit der Schrifttheorie Platos analysiert Stiegler insbesondere den berühmten Menon-Dialog, in dem es zunächst um die Tugend und dann um die Einsicht des Satzes von Pythagoras geht. Sokrates stellt hier in seiner berühmten Art die Fragen, die den Befragten zur Einsicht bringen, dass er den Beweis schon gekannt hat, ihn nur erst wieder erinnern muss (anamnésis). Von Frage zu Frage fortschreitend, führt Sokrates die geometrische Argumentation vor Augen, die der Befragte erst langsam begreifend nachvollzieht. Die Quintessenz ist: „Eine Idee darf niemals *rezipiert* werden, sondern muss immer *konzipiert* werden, und zwar durch denjenigen, den sie bewohnt" (DM, S. 44). Notwendig für solche Konzept- oder Begriffsbildung – so erkennt Stiegler frappiert beim Lesen des Menon-Dialogs – ist die Zeichnung.




Für die nötigen geometrischen Schlussfolgerungen muss man eine Figur zeichnen, das Problem entäußern. Plato spricht davon an keiner Stelle. Aber es ist als selbstverständlich vorausgesetzt. Die Zeichnung stellt quasi eine Krücke des Verstandes dar. Mit der Zeichenbewegung wird ein Anschauungsraum gebildet, in dem sich der geometrische Schluss vollziehen kann. „Die *anamnésis* (Wiedererinnerung) beinhaltet immer eine *hypomnésis* (eine Mnemotechnik oder Gedächtnistechnik), von der sie getragen und beseelt wird" (DM, S. 44). Gemeint ist damit jenseits der Zeichnung vor allem die Technik der Schrift. Plato kritisiert und analysiert völlig richtig deren Grenzen und Verfälschungen gegenüber einem wirklichen Dialog, bei dem Dialogpartner im selben Raum gegenwärtig sind. Aber seine Ablehnung der Schrift ist trotzdem falsch; denn insgesamt betrachtet stellt die Schrift keine Gefahr für die Erkenntnis dar, sondern konstituiert im Gegenteil erst die westliche Wissenschaft, indem sie einmal ausgesprochene Argumente an einem anderen Ort und einer anderen Zeit als dem ursprünglichen Kontext verfügbar und kritisierbar macht. Nur mit einem „organologischen Entwurf" von Psychotechniken wie dem Schriftsystem ist es möglich, für sich und andere Sorge zu tragen. Deshalb kritisiert Stiegler die geisteswissenschaftliche Tradition, die Fragen nach der Erkenntnis des Selbst die Priorität über die Erforschung der Sorge um sich selbst gibt (LS 71f). Wer die Technik der Wissenschaft entgegensetzt, versteht deren Genese nicht. Das technische Medium, in dem sich die Wissenschaft darstellen muss, bildet den blinden Fleck des platonischen Intellektuellen.

## Bildung als Formierung der Aufmerksamkeit

Bildung, die Kultur und Aufklärung umfasst, bedarf nicht nur der wissenschaftlichen Anstrengung des Begriffs, sondern einer Pflege der Psychotechniken. Eine ihrer vornehmsten ist eben genau die Schrift, die eine Stütze „der Gelehrtenrepublik ist, welche die Öffentlichkeit im Zeitalter der Aufklärung bildete" (LS 34). Das Buch als Psychotechnik führt zu einer Aufmerksamkeitsformierung. „Die Formierung von Aufmerksamkeit, die Moses Mendelssohn – nach der Bedeutung von Aufklärung befragt – als Bildung bezeichnete […], ist eine grundlegende Voraussetzung für jede menschliche Gemeinschaft. […] Die Formierung der Aufmerksamkeit, der At-tention, besteht in der Verknüpfung von Re-tentionen und Pro-tentionen durch Psychotechniken" (LS, S. 34f). Stiegler bedient sich hier der phänomenologischen Kategorien von Edmund Husserl zur Erklärung der Entstehung des Zeitbewusstseins (Husserl 1980). Zeit wird dabei nicht als homogene Uhrzeit im Sinne einer naturwissenschaftlichen Physik verstanden, sondern als sich bildende Zeitlichkeit, als Zeitbewusstsein, das erst entstehen kann, wenn im Gedächtnis Abgelagertes (Re-tentionen), sich mit unseren immer auf die Zukunft gerichteten Intentionen (Pro-tentionen) verbindet. Aufmerksamkeit ist ein solcher zeitlicher Bewusstseinsstrom. Husserl unterscheidet primäre Retentionen, quasi die Wahrnehmung, in der sich ein erscheinendes Objekt in Umrissen konstituiert, von sekundären Retentionen, in die das Objekt quasi durch die Vergangenheit des aufmerkenden Bewusstseins, durch seine Erfahrungen verpackt wird. Dadurch bildet das Bewusstsein Erwartungen, Protentionen. Husserl verdeutlicht diese Theorie am Hören einer Melodie, die wir nur als solche wahrnehmen, wenn im Bewusstsein nicht einfach eine Sequenz von Tönen abläuft, sondern wenn dem Zusammenspiel von Retention und Protention Aufmerksamkeit geschenkt wird. Deshalb wird die Melodie beim erneuten Hören immer anders wahrgenommen.

Stiegler erweitert diese Theorie um die Dimension externalisierter Ablagerungen des Gedächtnisses, welche er als *tertiäre Retentionen* bezeichnet. Tertiäre Retentionen werden geformt durch künstlich hergestellte Sedimentierungen, die sich über die Generationen hinweg in einem kollektiven Individuationsprozess, wie Simondon sagen würde, ansammeln, wobei sie – nur zum kleinen Teil bewusst, zum großen Teil aber unbewusst verinnerlicht – werden. Verschriftlichtes Denken lässt sich „reaktualisieren" oder in Husserlscher Terminologie „in Form einer neuen Anschauung reaktivieren" (DM 65). Für Stiegler ist das Buch deshalb ein Pharmakon, einerseits ein wirkmächtiges (Heil-)Mittel für die Unterstützung der Generierung von Wissen, anderseits kann es aber auch zum Gift werden, wenn es an die Stelle der Urteilskraft tritt. Es geht um Dosierung und den

mündigen Umgang. Dabei ist die Tatsache zu berücksichtigen, „dass Lektüre und Schriftlichkeit nicht mehr das sind, was sie einst waren. Sie sind digital, hypermedial und gemeinschaftlich geworden" (LS 56). Nach Stiegler bilden die digitalen Medien „den Kernpunkt der hyperindustrialisierten Gesellschaften, das heißt, der (zu einem Kulturkapitalismus gewordenen) industriellen Ökonomie. Und sie ordnen die Beziehungen zwischen den Generationen neu, wobei es letztendlich diese *intergenerationelle Beziehung ist, die die Intelligenz als Aufmerksamkeit erzeugendes Zusammenspiel von Retention und Protention* konstituiert" (LS 56f).

Heute drohen die psychotechnologischen Apparate – so Stiegler – Bestandteil einer *Psychomacht*[2] zu werden, „bei denen das Marketing zur zentralen Funktion der sozialen Entwicklung geworden ist" (LS 28). Die von der Kulturindustrie kontrollierte Psychomacht zerstört die Logik der Sorge, zerstört die Aufmerksamkeit selbst und jede verantwortungsbereite Erziehung, die sich auf einen vertrauensvollen Umgang mit der Nachkommenschaft gründet. Unkontrollierte Industrialisierung der Kultur unterjocht die Phantasie und wird zum Entertainment, um ein Publikum zu generieren. Solcher Zerstörung der Sorge als Aufmerksamkeit sagt Stiegler den Kampf an. Sein Ziel ist, „die Bildung organologisch zu reformieren – die psychosoziale Aufmerksamkeit im Zeitalter der globalisierten Psychotechnologien und Psychomacht wiederherstellen" (LS 60). Dabei geht es darum, dass sich die Erziehungsgemeinschaft ein *genealogisches Verständnis* ihrer hypomnetischen Hilfsmittel als Geschichte der Aufmerksamkeitskonstruktion aneignet. „Denn nur ein genealogischer Zugang zum Wissen, der dessen ursprüngliche technologische Dimension offen legt, ermöglicht das Verständnis dafür, wie das Wissen im modernen Sinne technologisch, also *industriell* wird und als technisch-wissenschaftliches Wissen die Hauptfunktion des zeitgenössischen Produktions- und Konsumptionssystems bildet" (LS 110).

Einen wichtigen Ausgangspunkt dieser Genealogie sieht Stiegler in den Arbeiten Michel Foucaults, der ein Konzept der Technologie der Macht entwickelt und die hypomnetischen Techniken des Wissens in den *Technologien des Selbst* analysiert. Dem geht Stiegler im zweiten Teil seiner Studie, die auf Deutsch unter dem Titel „Von der Biopolitik zur Psychomacht" erschienen ist, im Einzelnen nach. Dabei kritisiert Stiegler allerdings Foucault dahingehend, dass dessen Studien über Disziplinargesellschaften ihn dazu verleiten, psycho- und wissenstechnische Fragen auszuklammern. In seiner Analyse der Schule als Disziplinaranstalt, blende er „einen Umstand völlig aus: den Umstand nämlich, dass die Schrift als Techno-Logie, präziser: als Psychotechnik der Aufmerksamkeit, zugleich pharmako-logisch" (BP 28f) sei. Für Foucault gebe es keine pharmakologischen Herausforderungen. So stelle in seiner Analyse der Schule als Institution „die öffentliche Schulpflicht an keiner Stelle als einen historischen Prozess da, der über die Aufklärung, das heißt über die Modernität verlaufen ist" (BP 41). Für Stiegler formt die Schule dagegen ein materielles und institutionelles Dispositiv, als sich hier die Disziplinen in Bedeutungen bündeln, Zitat (BP 91):

1. Disziplin als ein *System der Sorge*, das die Beziehungen des Individuums zu sich selbst und zu anderen, das heißt zwischen den Generationen, reguliert […],

2. Disziplin verstanden als Transindividuation eines Wissens, das es an die gewöhnlichen Gelehrten, das heißt an die Bürger zu vermitteln gilt […],

3. und schließlich die Disziplin als Dispositiv der Überwachung, der Kontrolle und einer Individualisierung, die offenkundig zur Desindividuierung führen kann.

Damit öffnet Stiegler Foucaults grundlegende Analysen zu Genealogien und Biomacht für sein Bildungskonzept der Formierung von Aufmerksamkeit, bei der sich die Frage der Verantwortung gegenüber den zukünftigen Generationen aufwirft. Verantwortung stellt sich nach Stiegler als das dar, „was sich angesichts der Unabgeschlossenheit der Generationenfolge aufdrängt" (BP 172).

In dieser Neuformulierung der technischen Frage, welche die Genese der Technik mit der Geschichte des Menschen in einer originellen Weise verquickt, zeigt sich die Fruchtbarkeit von Stieglers Denken. Da, wo Marshall McLuhan nur Setzungen macht, liefert Stiegler Erklärungen, vermeidet einfache Zuweisungen und eröffnet stattdessen ein Verstehen für genealogische Abfolgen. Ein großes Verdienst haben die besprochenen kleinen Bände von Stiegler in der Wiederentdeckung von Gilbert Simondon und dessen Konzept der technischen Objekte – das in vielem Begriffsbildungen von Bruno Latour ähnelt. Bei der konkreten Analyse der Formation der digitalen Medien und ihrer Einbettung in die Alltagswelt – in Stieglers Terminologie die zeitgenössischen Mnemotechniken, hypomnemata oder Archive – bleiben Stieglers Analysen ein unfertiger Ansatz, der wohl notwendigerweise im Fluss bleiben muss. Am Schluss kündigt Stiegler auch eine Fortsetzung seiner Theorie der Sorge an (BP 173).

An den Schluss dieser Besprechung sei die Stieglersche Umdeutung des Kantschen kategorischen Imperativs gesetzt: „Wir

**Bernd Robben**

**Bernd Robben** ist wissenschaftlicher Mitarbeiter in der Informatik-AG *Digitale Medien in der Bildung* der Universität Bremen.

müssen mit neuen philosophischen, historischen und politischen Konzepten über die *zeitgenössischen Archive* nachdenken; mit Konzepten, die sich damit auseinandersetzen, dass die neuen Formen der *hypomnemata* ihrem Wesen nach *pharmaka* sind, die als Gifte wirken, die aber zugleich die einzig mögliche Arzneimittelkunde für jene Sozialtherapien bieten, aus denen politische Ideen und Aktionen immer bestehen" (BP 134).

## Referenzen


Stiegler, Bernard 2009: Denken bis an die Grenzen der Maschine. Diaphanes Zürich-Berlin (Original: 2004: Philosopher par accident: Entretiens avec Élie During. Editions Galilée Paris) (DM)

Stiegler, Bernard 2008: Die Logik der Sorge. Verlust der Aufklärung durch Technik und Medien. Suhrkamp Verlag Frankfurt am Main (Original: Prender Soin. De la jeunesse et des générations. Verlag Flammation Paris, Kapitel 1-6) (LS)

Stiegler, Bernard 2009: Von der Biopolitik zur Psychomacht. Suhrkamp Verlag Frankfurt am Main (Original: Prender Soin. De la jeunesse et des générations. Verlag Flammation Paris, Kapitel 7-11) (BP)

Stiegler, Bernard 2009a: Technik und Zeit. Der Fehler des Epimetheus. Diaphanes Zürich-Berlin (Original: 1994: La technique et le lemps. 1. La Faute d'Épimethée. Editions Galilée Paris)

Stiegler, Bernard Ars Industrialis – association internationale pour une politique industrielle des technologies de l'esprit (http://www.arsindustrialis.org/ aufgerufen am 20.7.2013)

Derrida, Jacques 2013: In der Universität fühlte ich mich nie zu Hause. Tageszeitung vom 15. Juli 2013

Foucault, Michel 2005a: Was ist Aufklärung? In: ders. Dits et Ecrits. Schriften. Suhrkamp Verlag Frankfurt am Main, S. 687-707 (Original: „What is Enlightment? (Qu'est-ce que les Lumières?), in: Rabinow, Paul (Hg.) 1984: The Foucault Reader, New York 1984, S. 32-50)

Foucault, Michel 2005b: Was ist Aufklärung? In: ders. Dits et Ecrits. Schriften. Suhrkamp Verlag Frankfurt am Main, S. 837-848 (Original: Technology of the Self (Les techniques des soie. Universität von Vermont, Okt. 1982) in: Hutton, P.H., Guthman, H. und Martin, L.H. (Hg.) Technologies of the self. A Seminar with Michel Foucault, Anherst: University of Massachusetts Press 1988, S. 16-49)

Foucault, Michel 2005c: Technologien des Selbst. In: ders. Dits et Ecrits. Schriften. Suhrkamp Verlag Frankfurt am Main, S. 966-999

Foucault, Michel 2005d: Über sich selbst schreiben. In: ders. Dits et Ecrits. Schriften. Suhrkamp Verlag Frankfurt am Main, S. 503-521 (Original: L'écriture de soi, in: Corps écrit, Nr. 5, L'Autoprotrait, Februar 1983, S. 3-23)

Horkheimer, Max und Adorno, Theodor Wiesengrund 1988: Dialektik der Aufklärung. Fischer Verlag Frankfurt am Main (Original 1944 bei Social Studies Association New York)

Husserl, Edmund 1980: Vorlesungen zur Phänomenologie des inneren Zeitbewusstseins. Max Niemeyer Verlag Tübingen (1. Auflage 1928 in: Jahrbuch für Philosophie und phänomenologische Forschung, Bd. IX)

Husserl, Edmund 1992: Die Krisis der europäischen Wissenschaften und die transzendentale Phänomenologie. In: Gesammelte Schriften 8, hrsg. von Elisabeth Ströker. Felix Meiner Verlag Hamburg (ursprünglich erschienen 1936)

Jonas, Hans 2003: Das Prinzip Verantwortung. Versuch einer Ethik für die technologische Zivilisation. Suhrkamp Verlag Frankfurt am Main (Original erschien 1979 im Insel Verlag Frankfurt am Main)

Kant, Immanuel 1784: Beantwortung der Frage: Was ist Aufklärung? In: Berlinische Monatsschrift, 1784, H. 12, S. 481-494

Martin, Luther H., Gutman, Huck und Hutton, Patrick H. (Hg.) 1993: Technologien des Selbst, Verlag Frankfurt am Main (Original: 1998, Technologies of the Selves, The University of Massachusetts Press Amherst)

Simondon, Gilbert 2012: Die Existenzweise technischer Objekte. Diaphanes Zürich (Original: 1958: Du mode d'existence des objets techniques. Aubier)


## Anmerkungen

1 *Zu der sehr unterschiedlichen kritischen Würdigung Heideggers durch deutsche und französische Intellektuelle vgl. Derrida 2013. Hier könnte man sehr vielen Kontexten und Fäden nachgehen, wie auch dem Bezug zu Horkheimer und Adornos kanonischem Aufsatz über die Dialektik der Aufklärung (Horkheimer und Adorno 1988), was in diesem Rahmen aber zu weit führen würde.*

2 *Stieglers weitergehende und hier nicht zu diskutierende These ist, dass solche Psychomacht die von Foucault analysierte Biomacht ablöst.*

*Der folgende Beitrag zur NSA 1952-1989 ist 1990 entstanden, wir haben ihn etwas gekürzt und redigiert. Die Originalfassung ist in voller Länge auf unserer Website abrufbar.*

*Anlass war die Einrichtung des* Bundesamts für Sicherheit in der Informationstechnik *(BSI). Die* Zentralstelle für das Chiffrierwesen *des BND zusammen mit 40 Stasi-Spezialisten wurde in* BSI *umbenannt und dem BMI zugeordnet. Eine öffentliche Diskussion gab es nicht, weder Politiker und Parteien noch Journalisten und Medien (mit Ausnahme der* Computer Zeitung*) waren damals daran interessiert, eine Debatte Informationssicherheit vs. Grundrechte zu führen. Offenbar hatte niemand die Diskussionen in den 70er und 80er Jahren um Rolle und Struktur der Informationssicherheit in den USA verfolgt. Erst als die NSA sich zunehmend für sensitive Information interessierte, kommerzielle Datenbankfirmen wegen der Überwachung von Datenbanknutzern kontaktierte, hochqualifizierte Firmen für Sicherheitstechnologien wie IBM, Motorola, Intel oder Xerox geheimverpflichtete und den Banken den Verschlüsselungs-Standard DES entziehen wollte, wurde intensiv über das Fehlen einer öffentlichen Kontrolle über die geheime NSA debattiert. Das Ergebnis war 1987/88 ein Gesetz, das die Verantwortung für militärisch-geheimdienstliche und zivile Informationssicherheit trennte. NBS (*National Bureau of Standards*) erhielt die Verantwortung für zivile Informationssicherheit zurück.*

*Inzwischen hat die NSA ihre Hauptaktivitäten vom Abhören, Daten-Sammeln und -Entschlüsseln auf die Analyse von Kommunikationsbeziehungen und die Prognose von Kommunikationsabsichten verlagert.* Big Data Mining *ist das revolutionäre KI-basierte Instrumentarium zur Verarbeitung massiver Datenmengen aus unterschiedlichen Quellen.*

**Retrospektive**

**Manfred Domke**

# Zur Trennung der Verantwortung für militärisch-geheimdienstliche und zivile Informationssicherheit am Beispiel USA

Die Sicherung von nicht als geheim eingestufter Informationen in Kommunikations- und Computersystemen soll nach gängiger US-Regierungs-Politik über die US-Führungsposition bei der Erforschung, Entwicklung und Anwendung von Sicherheitstechnologien erreicht werden. Eine zentrale Frage ist, mit welcher *Struktur* diese Führungsrolle gesichert werden kann.

Die *National Security Decision Directive 145 (NSDD-145)* von 1984 war ein Versuch der Reagan-Regierung, die militärisch-geheimdienstliche und zivile Informations-Sicherheit unter dem Dach des Geheimdienstes *NSA (National Security Agency)* zusammenzuführen. In der öffentlichen Diskussion um die politischen Richtlinien, die durch die NSDD-145 ausgelöst oder verstärkt wurde, ging es primär um die Rollenverteilung zwischen *NSA, NBS (National Bureau of Standards)* und zivilem Bereich. Diese Auseinandersetzungen um die Informationssicherheits-Politik spiegeln eine Reihe unterschiedlicher Interessen wider. Sie reichen von der nationalen Sicherheit über die Rollen von Exekutive und Legislative bei der Festlegung dieser Politik, die Grundrechte und den Persönlichkeitsschutz bis hin zum kommerziellen Bedarf an neuer Sicherheitstechnik.

Der Bericht stützt sich im wesentlichen auf zwei Analysen des *Office of Technology Assessment (OTA)* und ein Papier der *Computer Professionals for Social Responsibility (CPSR)*.

## Traditionelle militärisch-geheimdienstliche Dominanz

Die US-Politik zur Informationssicherheit wurde seit dem 1. Weltkrieg von nationalen Sicherheitsinteressen dominiert, vom Department of Defense (DoD) und seit 1952 auch von der *NSA (National Security Agency)* gesteuert. Die NSA, der Geheimdienst des DoD, war von der Regierung eingerichtet worden, um alle Abhör- und Entschlüsselungsdienste zusammenzufassen und um den Fernmeldeverkehr der Militärs, Geheimdienste und Diplomaten vor fremden Sicherheitsdiensten zu schützen.

Die Kontrolle der Verschlüsselungstechnologien durch die NSA war durch die nationalen Sicherheits- und Abhörinteressen bestimmt und nicht problemlos mit der *neuen Rolle* bei der Entwicklung und *Weitergabe* von Sicherheits-Technologien und -Produkten zu vereinbaren. Denn eine weltweite Verfügbarkeit der besten Verschlüsselungstechnik würde die weltweite Abhörmission der NSA stark behindern oder sogar unmöglich machen.

Später ging es den Verteidigungsbehörden darum, den Sowjets den Zugang zu militärisch nutzbarem Gerät der USA und der Alliierten zu verwehren. Sie begannen auf Exportbeschränkungen für *technische Information* zu drängen, die für militärische oder zivile Zwecke nutzbar war. Gleichzeitig wuchs die Gefahr elektronischer Abhörmaßnahmen durch die Sowjets und andere Länder sowie das Potenzial international organisierter Gegner (Wirtschaftskonkurrenten, Terroristen, Drogenhändler und Verbrecher-Organisationen). Daraus erwuchs das Interesse, auch nicht als geheim eingestufte Information zu schützen, die einzeln oder in der Kombination als schutzwürdig anzusehen war. So entstand eine neue Kategorie nicht-geheimer, so genannter *sensitiver Information*.

### Öffnung in die zivile Richtung

Das NBS, eine zivile Behörde des *Department of Commerce (DoC),* eingerichtet aufgrund einer Kongressinitiative im Jahr

1965 *(Brooks Act)*, entwickelte Leistungsstandards für die Computer der US-Regierung. Um 1970 begann sich die NSA um die Verletzlichkeit des US-Bankensystems zu sorgen und forderte das NBS auf, ebenfalls auf dem Gebiet Computer-Sicherheit aktiv zu werden. Darin lag eine politische Richtungsänderung, eine Öffnung. Zum ersten Male sollte sich eine *zivile Behörde* mit *Kryptographie* befassen. Auch dadurch wuchs im Militär- und Geheimdienstbereich das Interesse, den nichtklassifizierten, ungeschützten Nachrichtenaustausch vor dem Zugriff durch fremde Staaten zu schützen.

Das NBS startete 1973 ein Programm zur Computer- und Kommunikations-Sicherheit, und entwickelte in diesem Rahmen zusammen mit IBM und NSA-Unterstützung den *Data Encryption Standard (DES),* der 1977 US-nationaler Verschlüsselungsstandard wurde.

Das NBS beriet Benutzer und Hersteller bei der Entwicklung von Produkten, validierte kommerzielle Verschlüsselungsgeräte und beteiligte sich weiter an der Entwicklung von Standards, z. B. an der Netzsicherheit im *OSI (Open System Interconnection)*-Zusammenhang.

Im November 1977 hatte der damalige US-Präsident *Carter* über eine *Präsidentendirektive (PD-24)* die gemeinsame Verantwortung für die Telekommunikations-Sicherheit der NSA (über das DoD) und der *National Telecommunications and Information Administration (NTIA,* über das DoC) übertragen. Diese Direktive bezog sich auf den Sicherheitsbedarf für Informationen der Regierung und des zivilen Bereichs, aus denen „Gegner ihren Nutzen ziehen" könnten, also auf klassifizierte und sensitive Information. Welche Information als *sensitiv* zu gelten hatte und wer dies definieren sollte, blieb ungeklärt. Die NSA bekam auch die Zuständigkeit für nicht als geheim eingestufte Telekommunikation. Mit der NTIA erhielt erstmals eine zivile Behörde eine eingeschränkte Verantwortung für die Sicherheit der Regierungskommunikation. Darüber hinaus sollte NTIA die Verwundbarkeit der Informationstechnik mehr in das Bewusstsein der zivilen IT-Anwender und -Benutzer bringen.

Außerdem sollte ein Vorschlag für eine nationale Kryptographie-Politik erarbeitet werden. Weil sich DoD und DoC nicht auf Kompromisse zwischen nationaler Sicherheit, freiem Handel, Innovation und Grundrechten einigen konnten, wurde kein gemeinsamer Vorschlag vorgelegt. Das DoD trat in seinem Vorschlag für eine Fortsetzung der Kontrolle von Kryptographie, Patentwesen, Export von Geräten und Fachkenntnissen durch die Regierung ein. Das DoC trat ein für ein Minimum an Kontrollen und mehr Sensitivität bezüglich nachteiliger Wirkungen solcher Kontrollen auf breitere nationale Interessen.

## Der NSA-Einfluss auf Standardisierung, Forschung und Entwicklung

Die begonnene kontroverse Debatte wurde fortgeführt über die Sicherheit des DES und die NSA-Rolle bei der Standardisierung des DES. IBM hatte nach Aussagen der NSA einen 128-Bit-Verschlüsselungsalgorithmus ohne mathematische Schwächen beim NBS eingereicht, der aber von der NSA nur mit Veränderungen als Standard akzeptiert wurde. Die NSA schlug IBM vor, die Schlüssellänge des eingereichten Algorithmus auf 56 Bit zu kürzen und stattdessen eine neue Matrix in die Algorithmusstruktur einzubauen, die IBM auf *Bitten* der NSA nie veröffentlicht hat. Teilnehmer einer Arbeitsgruppe, die im September 1977 die mathematischen Grundlagen des DES-Algorithmus diskutierten, waren darüber sehr besorgt, weil sie so nicht in der Lage waren, alle Entwurfskriterien zu beurteilen. Kryptographie-Experten gehen davon aus, dass durch diese Veränderungen der Verschlüsselungs-Algorithmus im Interesse der NSA geschwächt wurde und die NSA sich eine *Hintertür* offen halten wollte.

Obwohl die Wissenschaftsgemeinde der Kryptologen sehr klein ist, versucht die NSA aus Gründen der nationalen Sicherheit immer wieder *Einfluss* zu nehmen auf die staatliche *Forschungsförderung*, die *Veröffentlichungen* und *Patentierungen* des privaten Kryptologie-Sektors sowie auf akademische *Forschungsergebnisse*.

Die NSA besitzt *keine gesetzliche Grundlage* zur Vorabprüfung von Veröffentlichungen unabhängiger nichtstaatlicher Forschung. Dennoch hat die NSA zusammen mit einigen Wissenschaftlern ein Gremium zur freiwilligen Überprüfung kryptologischer Manuskripte eingerichtet. Wissenschaftler und Forschungsinstitute, die sich diesem Verfahren unterziehen, geben der NSA Gelegenheit zur Forderung, sensitive Teile von einer Veröffentlichung auszunehmen. Andere, die sich nicht daran beteiligen, sehen darin eine *Bedrohung des freien Austauschs wissenschaftlicher Ideen*.

Diesen ungünstigen Rahmenbedingungen für die Standardisierung und eine freie zivile Kryptographieforschung stehen Anzeichen für ein wachsendes Interesse für Sicherheitsfragen im zivilen Bereich gegenüber:

## Die zentrale Lösung der Exekutive: Die NSA erhält auch die Verantwortung für den zivilen Bereich

Anfang der 80er Jahre wurde der Reagan-Regierung die *Abhängigkeit* von der Informationstechnik zunehmend bewusster und

**Manfred Domke**

**Manfred Domke** arbeitete in Forschung und Entwicklung von 1968 bis 2004 als wissenschaftlicher Angestellter bei der Siemens AG (Simulation eines Vermittlungsrechners), ZfCh (Univac 1110), in mehreren Instituten der GMD (Datenbanken, Softwareproduktion, Petri-Netze, KI) und im Fraunhofer Institut AIS (Robotik, Data Discovery).

gleichzeitig wurden die politischen Richtlinien für den Umgang mit diesen Abhängigkeiten als inadäquat angesehen. Die Behörden sollten über ihren Bedarf an minimalen Sicherheitsvorkehrungen aufgeklärt werden. Die Beziehung zwischen Sicherheitsmaßnahmen für „national security information" und anderen sollte geklärt werden. Aufklärung auf dem Gebiet Sicherheit für Telekommunikation wurde gefordert.

Die NSDD-145 vom 17. September 1984 machte die NSA zur zentralen Regierungsstelle für Kryptographie, Sicherheit in Telekommunikations- und Computersystemen und führte die getrennten Wege militärischer und ziviler Behörden auf dem Gebiet Informationssicherheit unter dem Dach der NSA zusammen. Die Genehmigung aller Sicherheits-Standards, -Techniken, -Systeme und -Geräte für Kommunikations- und Informationssysteme lag in den Händen der NSA.

Die NSDD-145 stand im Konflikt zur Übertragung der Aufgabe an das NBS durch den Kongress *(Brooks Act),* Standards für Computersicherheit zu entwickeln. Hersteller und Benutzer von Informations-Sicherheit-Produkten waren verunsichert bezüglich der Entwicklung von Standards und der Abnahme von Geräten. Sie machten die geeignete Aufteilung der Verantwortung zwischen zivilen und militärischen Behörden sowie das Fehlen der öffentlichen Kontrolle über die geheime NSA zum Diskussionspunkt.

Die Rahmenbedingungen für diese NSA-Aktivitäten wurden von zwei Gremien festgelegt: von der *Systems Security Steering Group* (SSSG) und dem *National Telecommunications and Informations Systems Security Committee* (NTISSC).

Der Umfang der Einflussnahmen der NSA und NTISSC auf Aktivitäten militärischer und ziviler Einrichtungen war abhängig von der *Interpretation des Schlüsselbegriffs „sensitive, nichtgeheime Information"*.

Die Öffentlichkeit wurde hellhörig, als dreierlei gleichzeitig bekannt wurde: die SSSG-Definition von sensitiver Information, eine geheime Air Force Studie zur Einschränkung des Zugangs zu Datenbanken und FBI-, CIA- und NSA-Besuche bei kommerziellen Datenbankfirmen mit dem Ziel, Mechanismen zur Überwachung von Datenbankbenutzern zu erkunden.

Als die NSA 1986 ankündigte, ab 1988 DES-Geräte nicht mehr neu zu zertifizieren und DES durch einen *geheimen Algorithmus (CCEP)* zu ersetzen, der in einer bestimmten Version unter das Exportverbot fiel und daher international nicht benutzt werden konnte, schreckten auch die *Banken* auf. Sie befürchteten, dass CCEP kein DES-Ersatz für die Finanzwelt sein konnte. Sie befürchteten, dass die Kontrolle über ihr Schlüsselmanagement auf die NSA übergehen könnte. Darin sahen sie eine unakzeptable Übergabe von Bankverantwortung an eine Regierungsinstanz. Die Banken setzten sich durch.

Einerseits sollte die Zusammenführung der militärisch-geheimdienstlichen und zivilen Informationssicherheit den Markt stärken. Andererseits befürchteten Neueinsteiger ungünstigere Wettbewerbsbedingungen. Denn erklärtes NSA-Ziel war es, ihre Verschlüsselungskomponenten von hoher Qualität zu günstigen Preisen in die Kommunikationssysteme hochqualifizierter Hersteller einzubauen. Hochqualifiziert war eine Firma dann, wenn 1. sie nicht im Besitz von Ausländern oder einem starken Einfluss von außen ausgesetzt war, 2. sie geheimverpflichtet war, 3. ihre Produkte aus NSA-Sicht marktfähig waren und 4. sie die Fähigkeit beweisen konnte, über die minimalen NSA-Anforderungen hinauszugehen. Für das NSA-Industrie-Joint Venture *Development Center for Embedded Communications Security Products* bekamen folgende U.S.-Unternehmen den Status *hochqualifiziert*: *Harris, Motorola, RCA, Rockwell International, Hughes Aircraft, GTE, AT&T Technologies, IBM, Xerox, Intel* und *Honeywell*.

### Die verteilte Lösung der Legislative: Trennung der Verantwortung für militärisch-geheimdienstliche und zivile Informationssicherheit

Per Gesetz wurde 1987 dem *NBS* die Verantwortung für zivile Informationssicherheit zurückgegeben. Die NSA bleibt zuständig für die Sicherheit klassifizierter Information. Die Problematik *sensitiver* Information bleibt bestehen. Im Gesetz wird jedoch explizit die Definition aus dem NSDD-145-Kontext zurückgewiesen.

Das *NBS* wurde inzwischen in *National Institute of Standards and Technology (NIST)* umbenannt. In einem Memorandum soll 1989 die Arbeitsbeziehung zwischen NIST und NSA für die Entwicklung von Sicherheitsstandards und politischen Richtlinien genauer geklärt worden sein. Mitglieder des Kongresses halten das Memorandum allerdings für gesetzwidrig, weil der NSA darin eine Rolle zugebilligt wird, die über eine technische Beratung von NIST hinausgeht.

## Zusammenfassung: Thema, Ziele, Fragestellungen

Die US-Politik zur Informationssicherheit verfolgt eine Reihe unterschiedlicher Ziele:

- Der zivile Sektor soll befähigt werden, den steigenden Sicherheitsanforderungen ziviler Unternehmen und Behörden gerecht zu werden. Dabei sollen durch unabhängige zivile Sicherheitsmaßnahmen Risiken für Geheimdienste minimiert werden.
- Die Rollen von Bundesbehörden im Bereich Sicherheitstechnologien sind zu klären. Dies gilt besonders für NSA und NIST.
- Wettbewerb, Innovation und Handel sollen gefördert werden.
- Militärisch-geheimdienstliche Behördenaufträge sollen, soweit vertretbar, von Aufträgen ziviler Behörden und Firmen getrennt werden.
- Die Spannungen zwischen Regierungspolitik und zivilem Sektor sollen reduziert werden.

Zur Erreichung dieser Ziele gab es aus OTA-Sicht drei Optionen, von denen keine alle nationalen Zielsetzungen voll befriedigen konnte:

1. Die Zentralisierung aller staatlicher Aktivitäten zur Sicherheit nicht-geheimer Regierungsinformation bei der NSA.

2. Fortsetzung der NSDD-145-Praxis würde die Führungsrolle der NSA für die gesamte Informationssicherheit unterstreichen, das NBS hätte nur eine Unterstützungsfunktion.

3. Nach Meinung der OTA wären beide Lösungen wenig wirksam gewesen.

4. Trennung der Verantwortlichkeiten von NSA und NBS entsprechend der unterschiedlichen militärisch-geheimdienstlichen und zivilen Anforderungen.

Eine Variante dieser Option wurde vom Kongress verabschiedet. Bei der letzten Lösung befürchtete OTA Nachteile für die primären Geheimdienstaufgaben der NSA, wenn die NSA nicht bei allen Sicherheitsentwicklungen beteiligt worden wäre.

**Wichtige Fragestellungen lauten:**

- Können Sicherheitsmaßnahmen, die für Militär und Geheimdienste entworfen werden, den Bedarf kommerzieller Benutzer decken, ohne die Ziele der Nachrichtendienste zu gefährden?

- Kann die NSA ihre traditionelle Geheimdienstrolle in Einklang bringen mit der Offenheit, die zur Lösung ziviler Probleme erforderlich ist?

- Welche Rollen sollen Militär und Geheimdienste in zivilen Angelegenheiten spielen?

- Wie können Offenheit und freier Markt mit Geheimoperationen und Kontrolle sensitiver Informationen koexistieren?

Die Politik für Informationssicherheit, die traditionell von nationalen Sicherheitsinteressen dominiert wurde, kam in den USA auf den Prüfstand, weil sie immer stärker auf zivile Interessen einwirkt. Die Grundfrage bezog sich auf die Reduzierung von Konflikten zwischen der Exekutive und Legislative bei der Festlegung von Politik, sobald Fragen der nationalen Sicherheit berührt sind. Die Tragweite dieser Frage geht weit über die enge Grenze der Informationssicherheit hinaus.

Eine andere Frage bezog sich auf Regierungsmaßnahmen für zusätzliche Kontrolle und Macht über nicht-geheime staatliche und kommerzielle Datenbanken: Wäre ein unkontrollierter Zugang für fremde Regierungen, Konkurrenten und Kriminelle eine Bedrohung für die nationale Sicherheit?

Es galt also, eine Reihe nationaler Interessen in Einklang zu bringen. Gemäß OTA würde eine optimale Lösung

- die Fähigkeit des freien Marktes stärken, Sicherheitstechnologien so zu entwickeln und anzuwenden, dass sie dem vielfältigen Benutzerbedarf gerecht würden,

- während unnötige Handelsbeschränkungen, Innovationshemmnisse, Beschränkungen des freien Informationsflusses und Gefährdungen der nationalen Sicherheit zu vermeiden wären.

## Referenzen


OTA (1986) Federal Government Information Technology: Management, Security, and Congressional Oversight, Congress of the United States, Office of Technology Assessment, OTA-CIT-297, Washington, DC: U.S. Government Printing Office, February.

OTA (1987) Defending Secrets, Sharing Data – New Locks and Keys for Electronic Information, OTA-CIT-310, October.

CPSR (1988) „Sensitive," Not „Secret": A Case Study, Mary Karen Dahl, Computer Professionals for Social Responsibility, Inc., P.O. Box 717, Palo Alto, No. CL-100-1, January.

Schmidt-Eenboom, E. (1989) Uncle Sam's achter Sinn, NSA & Co – Aufklärungsdienste der USA in der Bundesrepublik; in: Mediatus, Sondernummer 6/89, S.1-10.






## Wolfgang-Heilmann-Preis: Privatheit in der E-Society

*Zum 12. Mal vergibt die Integrata-Stiftung für humane Nutzung der Informationstechnologie ihren Wolfgang-Heilmann-Preis, der mit insgesamt € 10.000,– dotiert ist und auf bis zu drei Preisträger verteilt werden kann. Herausragende Vorschläge zum Einsatz von Informationstechnologie, die die Verhältnisse in unserer Informationsgesellschaft nachhaltig zu bessern versprechen, können bis zum 31. Dezember 2013 bei der Integrata-Stiftung, Tübingen, eingereicht werden.*

Die vorliegende Ausschreibung für die 12. Preisverleihung 2013/2014 steht unter dem Motto *Privatheit in der E-Society.* Fragen, ob ein Thema dazugehört oder nicht, werden gerne vertraulich beantwortet unter: *info@integrata-stiftung.de.*

Einreichungen für den Wolfgang-Heilmann-Preis 2013/2014 bitte nur in elektronischer Form bis spätestens 31. Dezember 2013 um 24:00 Uhr (Eingang), entweder per E-Mail an: *info@integrata-stiftung.de* oder per Hochladen auf: *preis.integrata-stiftung.de* (siehe auch *www.integrata-stiftung.de*) in beiden Fällen als eine einzige .zip-Datei bestehend aus folgenden drei pdf-Dateien: Anschreiben mit Begründung und Darstellung des Grundgedankens (1 Seite), Kurzfassung des Vorschlags (2 bis max. 5 Seiten), Langfassung der Beschreibung (evtl. mit Bildern, Links etc.).

Weitere Informationen unter *http://www.integrata-stiftung.de/index.php/preisaktivitaeten/preis-20132014*.

**Britta Schinzel**

# Sandro Gaycken (Hg.) – „Jenseits von 1984“

## Datenschutz und Überwachung in der fortgeschrittenen Informationsgesellschaft Eine Versachlichung

*Der Herausgeber behauptet, als Geisteswissenschaftler eine objektive Haltung zum Thema Freiheit versus Sicherheit im Kontext der neuen Überwachungstechnologien einzunehmen. Die Verurteilung der Kritik des Chaos Computer Clubs am Bundestrojaner gleich im ersten Absatz der Einleitung als vorurteils- und sendungsgetriebene Politik im Mantel vorgeblich objektiver Kritik, ohne irgendeinen Nachweis auch im Weiteren des Bandes, zeigt hingegen unmittelbar eine parteiliche Positionierung. Zudem legt ein Fehler (eine redaktionelle Überarbeitung hätte dem Band angesichts der Schreibfehler auch insgesamt gut getan) auf Seite 4 unten der Einleitung des Herausgebers nahe, dass ihm der Begriff Quellen-TKÜ unbekannt ist, wie sich überhaupt beim Lesen der Texte der Eindruck verhärtet, dass der Herausgeber die Beiträge seines Buches nicht kennt oder nicht versteht.*



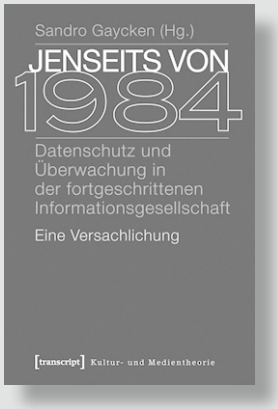
Der hohe Anspruch von Objektivität der Autoren an sich selbst muss nicht nur wegen der Komplexität der Technik selbst, mehr noch der technisch-politischen und sozialen Wechselwirkungen, sondern schon angesichts der vielen Unbekannten, die das jeweils sehr stark verzögerte Bekanntwerden neuer technischer Möglichkeiten und ihrer Diffusion in immer neue Bereiche notwendigerweise als naives Wunschdenken abgetan werden. Ja, es wird den Herausgebern (und dem Verlag) nach der Veröffentlichung der Internetüberwachungsprogramme PRISM (das immerhin schon von der Bush-Regierung 2007, also 6 Jahre vor dem Erscheinen dieses Bandes, etabliert wurde) und *Tempora* wohl selbst inzwischen gedämmert sein, wie sehr viele Texte in dem Buch schon beim Erscheinen überholt bzw. falsifiziert worden sind.

Der Forderung von *Patrick Voss-de Haan* nach mehr öffentlichen Diskursen zum Thema wird niemand widersprechen, doch bleibt der Text so abstrakt, dass daraus wenig Gewinn zu ziehen ist, während er, wo er tatsächlich konkret wird, ebenso von Fehleinschätzungen geprägt ist wie der des Herausgebers. Gefordert wird eine nationale Institution für solche Diskussionen. Nirgends aber wird die geradezu kontradiktorische Diskrepanz zwischen den Gesetzgebungen der nationalen europäischen Regierungen und ihren viel folgenschwereren Entscheidungen zu Regulierungen im europäischen Parlament erwähnt, die speziell von deutscher Seite gerade im Kontext von Überwachung und Datenschutz doppelzüngiger und scheinheiliger nicht sein könnte.

Gottlob sind die nachfolgenden Artikel weder so überheblich noch qualitativ so angreifbar wie die beiden ersten. Interessanterweise stammen im Folgenden auch nicht nur fast alle relevanten Inhalte der Texte aus den zuvor getadelten Quellen CCC, FIfF, HU, DVD und ihren Mitgliedern, sondern nahezu durchgehend auch deren Analysen und Bewertungen.

Lesenswert für nicht Eingeweihte erscheinen *Gabriel Brönnimanns* Text zur Vorratsdatenspeicherung (welcher sich weitgehend aus Quellen der kritischen Informatik-Netzwerke speist), *Kai Biermanns* mäßigender Text über die aus politischen und publizistischen Gründen beabsichtigte Rolle der Medien, Angst zu erzeugen und der Text von *Wendy Füllgraf* zu Cyberkriminalität. Der auch weitgehend abstrakt bleibende Text von *Andreas Dewald et al.* zu Problemen und Grenzen der Computerforensik bietet immerhin einen Einblick in relevante Literatur.

Etwas näher möchte ich beispielsweise eingehen auf das vierte Kapitel zur Begründung des Datenschutzes. Hier argumentiert




Sandro Gaycken (Hg.) (2013) – Jenseits von 1984. Datenschutz und Überwachung in der fortgeschrittenen Informationsgesellschaft. Eine Versachlichung. Bielefeld: [transcript] Verlag, Reihe Kultur- und Medientheorie

*Nils Zurawski* mit Constanze Kurz, dass es heute den alles überwachenden *Big Brother* nicht mehr gebe, dass vielmehr viele Agenten Daten sammeln und austauschen, die zum Teil auch durchaus freiwillig und mit und ohne Wissen der Konsequenzen verfügbar gemacht werden. Weiter hält er dagegen, alle Überwachungsprobleme nur unter dem Aspekt des Datenschutzes und des Schutzes der Privatsphäre zu betrachten, es gehe beispielsweise auch darum, sich unerkannt in der Öffentlichkeit bewegen und sich dort frei äußern zu können. Schließlich ist sein wichtigster Punkt, die Überwachung nicht nur unter technikzentrierter Perspektive, sondern auch in Kontexten sozialer Entwicklungen und Wunschvorstellungen zu betrachten, oder umfassender, Technik als materielle Kultur zu begreifen. Zum Nachweis zieht er die Beispiele elektronische Kundenkarten und Biometrie heran. Die Diskrepanz zwischen den öffentlich kommunizierten, also weitgehend bekannten Datenschutzproblemen und ihrer Nichtbeachtung zeigt sich bei Kundenkarten vor allem an den durch seine eigene Empirie auf dem Lande festgestellten sozialen Bindungen an Einkaufsorte, die nebst den vernachlässigbaren Rabatten wichtiger erscheinen als die Kontrollmöglichkeiten. Überzeugender wäre hier die breite Nutzung von überwachten Handys und Tablets gewesen.

Das zweite Beispiel, die Biometrie, soll dafür herhalten, wie sehr die Materialität der Technik die Sicht auf die Welt, und den Umgang mit ihr beeinflusst. Dem ist zuzustimmen, wenngleich die Auseinandersetzung anhand dieses Textes sich m.E. zu sehr in der Unterscheidung von Identität und Identifizierbarkeit, bzw. der Abweisung der eindeutigen Identifizierbarkeit und somit eines Zusammenhangs zwischen beiden verfängt. Natürlich ist es

im Rahmen eines solchen Artikels nicht möglich, die umfangreiche Literatur zu Identität, auch zu virtuellen Identitäten abzuhandeln, noch weniger die noch viel umfangreichere zur Veränderung der Weltsicht und der Sicht des Menschen durch biometrische und neurowissenschaftliche bildgebende Verfahren, doch hätte man sich eine etwas stringentere Erklärung zum Titel gewünscht.

Der letzte Text, die Darstellung einer empirischen Untersuchung aus dem Bereich der Akzeptanzforschung stellt – wenig überraschend – Zusammenhänge zwischen allgemeinen Ängsten und der Akzeptanz von Überwachungstechnologien fest, sowie die allgemeine Abnahme von deren Akzeptanz, während sie gleichzeitig immer umfassender und vertiefter in die Privatsphäre der Bürger eingreift.

So muss man insgesamt feststellen, dass der Anspruch des Herausgebers, die Debatten um Datenschutz und Überwachung zu versachlichen, nirgends über das Bekannte hinaus eingelöst oder dieses auch nur erreicht wird. Alles Inhaltliche und Kritische in diesem Buch, die relevanten Analysen und Bewertungen stammen von Quellen aus den Bereichen der Informatik, Jura oder der Polizeiarbeit, der Netzaktivisten und NGOs – und zwar ohne diese zu kritisieren oder über das dort Gesagte hinauszugehen.

Dennoch möchte ich dem Band nicht jeden Wert absprechen, denn für Uneingeweihte bietet er einen partiellen Überblick über aktuelle Diskussionen, sofern sie nicht von PRISM und Tempora überholt worden sind.





**Dietrich Meyer-Ebrecht**

# Manfred Spitzer – „Digitale Demenz“

## Ein Appell an unsere Verantwortung gegenüber unseren Kindern

*Es war einmal ein Kaiser – so beginnt Hans Christian Andersen in seinem Märchen von des Kaisers neuen Kleidern –, dem schwatzten Betrüger teure Kleider mit einer ganz besonderen Eigenschaft auf: Nur wer nicht dumm sei, könne sie sehen. Und niemand wollte zugeben, sie nicht sehen zu können, auch der Kaiser selbst nicht. Bis ein Kind in die Menge rief, dass der Kaiser gar keine Kleider anhabe …*

Es war einmal eine neue Technologie, die mit rasanter Geschwindigkeit in alle unsere Lebensbereiche einzog, uns Arbeiten erleichterte oder sogar abnahm, uns immense Information erschloss, uns weltweit kommunizieren ließ, uns unbeschränkt Unterhaltung bot. Und eine ‚kinderleichte' Handhabung. Ein ideales Werkzeug für die Bildung, verkündeten unisono Industrievertreter und Bildungspolitiker. Jedem Kind sein Laptop, war die Parole. Schule, Kindergarten – man kann nicht früh genug damit beginnen. Kauft euren Kindern Smartphones und Spielkonsolen, macht sie ‚medienkompetent', lasst sie teilhaben am digitalen Bildungsangebot. Nur, diesmal ist da kein Kind, das in die Menge ruft, „ich lerne ja gar nicht wirklich, ich vergeude meine Zeit, ich bleibe dumm und werde einsam!“ Denn die Kids sind schon in den Bann der faszinierenden Technik gezogen, den Gruppenzwängen erlegen, angefixt vom Suchtpotential einschlägiger Softwareprodukte. Eltern unterstützen sie aus Angst, ihnen Bildungschancen vorzuenthalten. Lehrerinnen und Lehrer wollen sich modern geben, Schulen müssen ministeriellen Vorgaben folgen, in den Ministerien werden Erlasse, Lehrpläne und Budgetzuweisungen von praxisfernen, von Lobbyisten umworbenen Bürokraten erstellt. Die Regierung beruft Enquête-Kommissionen, die sich ihre ‚Experten' aus der einschlägigen Industrie einladen, und die Mainstream-Medien singen dazu ein euphorisches Loblied. Derweil freuen wir uns, dass dieser Markt mit seinem immensen Umsatz nicht unwesentlich dazu beiträgt, IT-Produkte immer leistungsfähiger und billiger werden zu lassen.

Dennoch, ein ungutes Gefühl haben wir schon immer gehabt, wenn wir lesen, dass sich Jugendliche in einem erschreckend großen Teil ihrer Tageszeit von Computer oder Smartphone vereinnahmen lassen, surfend, chattend, spielend oder Videos


Manfred Spitzer (2012):
Digitale Demenz.
Wie wir uns und unsere Kinder um den Verstand bringen.
München: Droemer.
ISBN 978-3-426-27603-7

schauend (in Deutschland liegt die Mediennutzungszeit von Neunklässlern einer großen Studie zufolge bei knapp 7,5 Stunden täglich). Mahnende Stimmen sind sehr wohl zu vernehmen. Eine sehr prononcierte erhebt Manfred Spitzer seit vielen Jahren. Sein jüngstes Buch „Digitale Demenz“ ist untertitelt „Wie wir unsere Kinder um den Verstand bringen“ – provozierend, zugegeben. Aber Spitzer ist Arzt und Wissenschaftler. Als Facharzt für Psychiatrie erlebt er die Folgen eines ungebremsten jugendlichen Internetkonsums, als Experte für Neurowissenschaften und Lernen geht er Ursachen und Zusammenhängen auf den Grund.

Wenn man das einleitende Kapitel mit allgemeinen, ein wenig lamentierenden Feststellungen hinter sich gelassen hat, wird das Buch spannend. Denn nun beginnt Spitzer in einem Dutzend aufeinander aufbauender Kapiteln einen Bogen zu schlagen über die unterschiedlichen Wechselwirkungen zwischen men-

talen Prozessen und Computernutzung – vom Lernen und Begreifen über das Kommunizieren bis zu gesundheitlichen Auswirkungen. Wenn er die Mechanismen beschreibt, begründet er sie neurophysiologisch, wenn er über Folgewirkungen berichtet, belegt er sie ausnahmslos mit Studien.

So greift Spitzer auf aktuelle Erkenntnisse der Hirnforschung zurück, wenn er – um eines seiner anschaulichen Beispiele anzuführen – die Mechanismen des Lernens und die durch Lernen bewirkte Ausbildung des Hirns darlegt: Galt bis vor wenigen Jahren noch das Paradigma von einer bereits im frühen Kleinkindalter abgeschlossenen Ausbildung der Hirnsubstanz, das eine spätere Neubildung von Neuronen ausschloss, so belegen neuere Forschungsergebnisse – wie die einer Forschergruppe am Klinikum der Friedrich-Alexander-Universität in Erlangen –, dass eine Neubildung von Neuronen zumindest im Hippocampus bis ins hohe Alter erfolgt. Diese Hirnregion ist gleichsam eine Art Informationsmanager. Hier werden alle von den Sinneszentren gelieferten Informationen bewertet, eingeordnet und verknüpft. Und es werden die Bezüge zu bereits in der Hirnrinde gespeicherten Informationen hergestellt, indem die Bildung von Vernetzungen der beteiligten Neuronen der Hirnrinde ausgelöst wird. Der Hippocampus sorgt also dafür, dass aufgenommene Eindrücke langfristig abgespeichert und miteinander vernetzt werden, dass aus Information Wissen wird. Der Hippocampus ist folglich eine viel beschäftigte Hirnregion, seine Zellen sind hoch strapaziert, und sie haben deshalb eine sehr begrenzte Lebenszeit. Neugebildete Neuronen des Hippocampus können nun ihre wichtige Funktion erst wahrnehmen, nachdem sie trainiert worden sind, analog zu neu gebildeten Muskelzellen. Werden diese nicht im Gebrauch trainiert, bleibt der Muskel schlaff. Entsprechend müssen auch die Neuronen des Hippocampus trainiert werden: durch Lern-Arbeit – *learning by doing* im buchstäblichen Sinn! Für eine nachhaltige Lernarbeit ist es nun entscheidend, dass auch unsere Sinne eingesetzt werden, möglichst sogar in ihrem Zusammenwirken. Sprache, beispielsweise, nur durch Hören zu lernen, ist, wie Studien ergeben haben, signifikant weniger nachhaltig, als wenn gleichzeitig mit dem akustischen Wahrnehmen die Lippenbewegungen der realen (!) Sprecherin verfolgt werden.

Spitzer macht es sich nun nicht so einfach, dass er einem Lernen mit oder durch Medien diese Qualitäten grundsätzlich abspricht. Eines seiner Hauptargumente ist vielmehr, dass die Beschäftigung mit dem Computer oder Smartphone, wenn sie zu einem großen Anteil aus Surfen, Chatten, Spielen besteht, dazu die Rezeption von Videos, Kindern einfach kaum noch Zeit lässt, Lernen in der realen Welt zu praktizieren – im Bewegungsspiel, im Experimentieren mit Gegenständen und Materialien ihrer realen Umwelt, in einem realen sozialen Umgang. In einem Großteil der oben zitierten siebeneinhalb täglichen Stunden wird die Medientechnik ja nicht als Lernmittel benutzt. Vielmehr hält sie das Kind vom Lernangebot der realen Umwelt ab, verarmt also die Lernwelt. Sicherlich will Spitzer nicht die Medientechnik von Kindern fernhalten. Sie gehört zu unserer heutigen und zukünftigen Lebenswelt und muss ebenso auch in ihren Funktionen erfahren und in ihrem Umgang erlernt werden. Auf ein vernünftiges Maß kommt es ihm an. Darauf, dass Kindern die Chance zu vielgestaltigem Lernen erhalten bleibt.

Warum der provokante Titel, „Digitale Demenz"? Nach heutigen Erkenntnissen lässt sich die funktionale Entwicklung des Hirns, unseres Geistes – lateinisch *mens* – durch eine Kurve beschreiben, die über die Zeit des Lernens kontinuierlich ansteigt, früher oder später ihren Zenit erreicht und schließlich auch wieder abfällt, unausweichlich, auch wenn der Abbau – *de-mens* – nicht zusätzlich noch pathologisch beschleunigt wird. Interessant ist nur, wie lange die Kurve aufsteigt und von welcher vorher erreichten Höhe der Abbau beginnt. Haben wir in unserem Leben, besonders in den lernintensiven frühen Lebensjahren viel für's Lernen getan, brauchen wir einen dramatischen Verlust unsere geistigen Fähigkeiten auch im hohen Alter nicht so sehr zu befürchten. Auch dies ist in repräsentativen Studien belegt, darunter die so genannte *nun study*, eine retrospektive Studie an Nonnen, deren geistige Aktivität über einen langen Lebenszeitraum dokumentiert war. Gehirnsektionen der meist erst in hohem Alter verstorbenen Teilnehmerinnen ergaben nicht selten bereits deutliche diagnostische Hinweise auf Alzheimer-Demenz – bei erwiesener intellektueller Leistungsfähigkeit bis unmittelbar vor dem Tod! Werden die Chancen für das Lernen nicht genutzt, bleibt der Anstieg der Lernkurve flach und sie erreicht früh ihren Zenit – schlechte Aussicht für langes Leben mit klarem Kopf …

Digitale Demenz – sie machen nicht dement, die digitalen Medien, will uns Spitzer sagen, aber durch einen unkontrollierten Umgang mit den Medien, insbesondere in der Kindheit und Jugend, verwirken wir die Chance, dem natürlichen altersbedingten – und auch dem krankheitsbedingten – Abbau unserer Geisteskräfte wirkungsvoll vorzubauen. Denn mit ihrer Sogwirkung verdrängen die digitalen Medien Lernmöglichkeiten, mit ihrem unermesslichen Informationsangebot lassen sie Lernmotivation verkümmern. Dazu kommen Bewegungsarmut, Schlafstörungen, Verarmung der – realen – sozialen Kontakte, Selbstkontrollverlust, Suchterscheinungen. Auch diesen Begleitphänomenen widmet Spitzer jeweils ein Kapitel.

Wie steht es nun mit den digitalen Medien, wenn sie *für* das Lernen eingesetzt werden? Ein weiter Markt hat sich für Lernsoftware aufgetan, für die Erwachsenenbildung, für die Unterstützung des Studiums, für den Schulunterricht, bis hin zu Produkten für den Kindergarten und für die Babystube. Angesichts der schlechten PISA-Resultate wird von Unterrichtssoftware regelrecht das Heil für die Erzielung besserer Quoten im internationalen Vergleich erwartet. Geht es jedoch nicht um ein zusätzliches Angebot, sondern um den Ersatz, die Ablösung bisheriger Formen des Unterrichts, stehen euphorischen Berichten repräsentative Studien gegenüber, die eher nachteilige Wirkungen bezeugen: Schülerinnen und Schüler, die unter vorwiegender Verwendung digitaler Medien unterrichtet worden waren, zeigten gegenüber Vergleichsgruppen überwiegend keine signifikant besseren, teils sogar schlechtere Leistungen. Hinterfragt man dagegen Studien, die zu positiven Ergebnissen kommen, werden deren Ergebnisse zweifelhaft, etwa wenn Elternhaus und soziales Umfeld nicht in das Studiendesign einbezogen wurden.

Spitzer genügt nun nicht allein die Feststellung der Ergebnisse solcher Studien. Er versucht vielmehr, die lernpsychologischen und lernphysiologischen Gründe dafür zu identifizieren. Nachvollziehbar erklärt er die Wirkungsmechanismen an Hand einer Vielzahl von Experimenten, so zum Beispiel wie und warum Multitasking – eine typische Herausforderung in Computerspielen – gerade nicht im Sinne eines Lerntrainings wirkt, sondern im Gegenteil zu Aufmerksamkeitsstörungen führt. Oder warum

bessere Lernerfolge nachweisbar sind, wenn Lernaufgaben mit einem Be-greifen verbunden sind.

Offen lässt Spitzer nur leider, was Eltern und Pädagogen am dringendsten interessiert: Wie können wir auf das Verhalten unserer Kinder den gewünschten Einfluss nehmen? Welche Rolle fällt der Schule zu? Sind gesellschaftspolitische Prozesse notwendig? Wie sind die Medien in ihre Verantwortung zu nehmen, die Lobbyverbände der Industrie in ihrer politischen Einflussnahme zu bremsen? Leider brandmarkt er nur, dass nichts geschieht, dass Kritik nicht gehört werden will. Dennoch, es ist eine Stärke dieses Buches, dass der Autor die Sachebene selten verlässt. Er argumentiert, wenn immer möglich, auf der Grundlage wissenschaftlicher Studien. Alle Fakten werden mit Quellen belegt, knapp 400 umfasst die Quellensammlung am Ende des Buches.

Die Grundlage, sachliche Debatten zum Thema zu führen, ist also durchaus gegeben. Stattdessen polarisiert sich die Szene. Hier ist die große Koalition der Befürworter, Pädagogen, Schul- und Bildungspolitiker, Medienvertreter, Industrielobbyisten im engen Schulterschluss – dort eine kleine Gruppe Kritiker. Eine sachliche Auseinandersetzung mit deren kritischen Standpunkten findet offensichtlich nicht ihren Weg auf die bildungspolitische Entscheidungsebene. Auf der Handlungsebene – Familie und Schule – wird die Diskussion durch den unseligen gesellschaftlichen Konsens, den grundsätzlichen Nutzen digitaler Medien nicht infrage zu stellen und kritische Einwände als gestrig zu brandmarken, blockiert. Es sollte nicht wundern, dass Kritiker sich ausgebremst fühlen, dass ihre Kritik unter dem Frust, nicht wahrgenommen gewollt zu werden, schließlich verbissen wirkt. Wir kennen dies aus anderen Bereichen der gesellschaftlichen Auseinandersetzung, vor allem wenn die Kritik handfeste wirtschaftliche Interessen bedroht.

Übrigens, wo bleibt hier eigentlich das FIfF, seine Mission Informatik und gesellschaftliche Verantwortung? Verletzung der informationellen Privatsphäre, menschenverachtende Arbeitsbedingungen in der IT-Industrie, Missbrauch unserer Wissenschaft für die Rüstung – das sind zweifelsfrei wichtige Themen. Aber für das Fortbestehen unserer Kultur, für die Erhaltung unserer Lebensbedingungen, für die Lösung existenzieller Problem der Zukunft müssen die Köpfe der nächsten Generation höchste Priorität haben – Bildung und Ausbildung, auch ein nicht geringer Beitrag für den Frieden. Ich bin gespannt, was das vorliegende Heft in diesem Kontext bieten wird …



**Kai Nothdurft**

## Marc Elsberg – „Blackout – Morgen ist es zu spät“

Der Thriller Blackout erzählt die Geschichte eines Cyberterror-Anschlags auf den europäischen Stromnetzverbund. Als es zu Stromausfällen im europäischen Netzverbund kommt, untersucht der Informatiker Piero Manzano seinen Smartmeter und entdeckt eine Manipulation. Er vermutet einen Zusammenhang und schöpft Verdacht, doch niemand nimmt ihn zunächst ernst. Später gerät er gar selbst unter Verdacht. Die Geschichte fesselt von Anfang an und bleibt bis zum Ende spannend.


Marc Elsberg (2012): Blackout – Morgen ist es zu spät. Roman. Gütersloh: Blanvalet, 800 Seiten, ISBN 978-3-7645-0445-8, auch als Taschenbuch erhältlich

Die eigentlichen Täter und ihre Motive bleiben im Hintergrund. Trotzdem ist der Roman alles andere als unpolitisch. Elsberg geht detailliert auf die Handlungen der Verantwortlichen in den Krisenstäben in Staat und Wirtschaft ein. Er stellt sehr anschaulich dar, wie stark die Abhängigkeiten der modernen zivilisierten Gesellschaft von einer stetigen Versorgung mit Energie ist. Schon nach kurzer Zeit führt deren Ausfall zu einem Aufbrechen der gewohnten Abläufe und zum Wegbrechen wesentlicher Elemente der modernen Gesellschaft. Viele reagieren mit Verunsicherung und es kommt zu Gewalthandlungen nach dem Recht des Stärkeren.

Die dargestellte Attacke auf die Stromversorgung durch Ausnutzung von IT-Schwachstellen basiert auf einem technisch realistischen Szenario. Auch die Reaktionen von Krisenstäben und der Gesellschaft insgesamt wirken ausgesprochen glaubwürdig. Der Autor recherchierte augenscheinlich sorgfältig die fachlichen Hintergründe. Einige Details wurden dabei modifiziert, um keine Vorlage für echte Angriffe zu liefern.

Elsberg führt mit *Blackout* die Risiken eines weitflächigen Stromverbundes und die Verletzlichkeit intelligenter Stromnetze vor Augen, die als wesentlicher Baustein der Energiewende gelten.

Die Handlung spielt in der Gegenwart und ist hoch aktuell. Die Reaktorkatastrophe von Fukushima wurde bereits verarbeitet. In Deutschland beginnt zur Zeit die Ausstattung der privaten Haushalte mit Smartmetern. Die Spezifikation für die Sicherheitszertifizierungen dieser Geräte durch das BSI wurde erst im Dezember 2012 finalisiert und demnächst kommen die ersten Geräte auf den deutschen Markt.

Der Roman stellt damit auch eine kritische Auseinandersetzung mit den Risiken dieser Technik dar und bietet auch technisch weniger versierten Lesern die Chance, sich dieser Problematik zu nähern.

*Hinweis: Es besteht Verwechselungsgefahr mit dem Roman „Blackout“ von Andreas Eschbach.*

**Humanistische Union u. a.**

# Grundrechte-Report 2013

*Der von acht namhaften Bürgerrechtsorganisationen herausgegebene Report zieht eine kritische Bilanz zum Umgang mit den Bürger- und Menschenrechten in Deutschland.*

Beate Rudolf, Direktorin des Deutschen Instituts für Menschenrechte, erklärte anlässlich der Präsentation des Grundrechte-Reports: „Es ist geboten, die Identifizierung der Polizeibeamten und -beamtinnen im Einsatz sicherzustellen und Vorkehrungen für eine unabhängige Ermittlung in Fällen von Polizeigewalt zu treffen, etwa durch unabhängige Beschwerdestellen, um eine wirksame Strafverfolgung zu garantieren."

Der Polizeieinsatz am 1. Juni 2013 bei der Blockupy-Demonstration in Frankfurt zeigt, wie wichtig ein solcher Schutz vor Polizeigewalt ist. Was der Grundrechte-Report hinsichtlich der Blockupy-Proteste für das Jahr 2012 dokumentiert, hat sich in verschärfter Weise am letzten Wochenende durch einen drakonischen Polizeieinsatz wiederholt. Die Herausgeber des Grundrechte-Reports sehen dies als verfassungsrechtlichen Skandal an. Elke Steven vom Grundrechtekomitee stellt für die Herausgeber fest: „Wir sind entsetzt, in welch unvorstellbarer Weise Grundrechte ausgehebelt und Gerichtsurteile mit Füßen getreten wurden." Die Demonstration war früh durch die Einkesselung der ersten Blöcke verhindert worden. Teils brutale Polizeigriffe, Schlagstock- und Pfeffersprayeinsätze führten zu Hunderten Verletzten auf Seiten der Demonstrierenden. Das Demonstrationsrecht – für eine Demokratie schlechthin konstituierend – wird ebenfalls verletzt, wenn es durch Platzverweise, Videoüberwachung, Verbote und Auflagen ausgehöhlt wird.

Der Zustand der Verfassungswirklichkeit zeigt sich gerade am Umgang mit den Schwächsten in der Gesellschaft. So wurden im Jahr 2012 Asylsuchende aus Serbien und Mazedonien im Asylverfahren massenhaft abgelehnt und umgehend die Abschiebung in ihre Herkunftsländer vorbereitet. „Mit einem rechtsstaatlichen Verfahren hat dies nichts mehr zu tun", sagte Marei Pelzer, PRO ASYL, im Namen der Herausgeber. Manifeste Eingriffe in die Grundrechte finden aber auch da statt, wo durch Nacht-und-Nebel-Abschiebungen Familien getrennt werden, wie etwa der im Report geschilderte Fall der syrischen Familie Naso beleuchtet. Opfer von staatlicher Diskriminierung werden sowohl Deutsche als auch Nicht-Deutsche, wenn die Polizei meint, in Zügen, auf Bahnhöfen oder im „grenznahen Raum" Menschen allein aufgrund ihrer Hautfarbe kontrollieren zu dürfen (Racial Profiling). Pelzer fordert, diese rassistische Diskriminierung endlich zu beenden.

Der Grundrechte-Report befasst sich angesichts des Versagens der Verfassungsschutz- und Sicherheitsämter bei den Morden des sogenannten „Nationalsozialistischen Untergrunds" in einem weiteren Schwerpunkt mit dem Thema Geheimdienste. Der Verfassungsschutz habe sich grundlegend diskreditiert und werfe fundamentale Fragen nach seiner demokratischen Legitimierbarkeit auf, stellten die Herausgeber fest.

Der jährliche Report zur Lage der Bürger- und Menschenrechte in Deutschland zieht auch in seinem 17. Erscheinungsjahr mit 42 Beiträgen kritisch Bilanz zum Zustand der Grundrechte. Der im Fischer Taschenbuch Verlag verlegte, 1997 erstmals erschienene Grundrechte-Report versteht sich als „alternativer Verfassungsschutzbericht". Acht Bürger- und Menschenrechtsorganisationen dokumentieren darin jährlich den Umgang staatlicher Stellen mit dem Grundgesetz.

*Quelle: Pressemitteilung der Humanistischen Union.*




Till Müller-Heidelberg, Elke Steven, Marei Pelzer, Martin Heiming, Heiner Fechner, Rolf Gössner, Ulrich Engelfried und Falko Behrens (Hg.) (2013): Grundrechte Report 2013 – Zur Lage der Bürger- und Menschenrechte in Deutschland; Preis €10,99; 240 Seiten; ISBN 978-3-596-19648-7; Frankfurt am Main: Fischer Taschenbuch Verlag

## Impressum

| | |
|---|---|
| **Herausgeber** | Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF) |
| **Verlagsadresse** | FIfF-Geschäftsstelle<br>Goetheplatz 4<br>D-28203 Bremen<br>Tel. (0421) 33 65 92 55<br>*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** | Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck, Sara Stadler |
| **Schwerpunktredaktion** | Stefan Hügel (Datenausspähung)<br>Hans-Jörg Kreowski (Bildung) |
| **V.i.S.d.P.** | Stefan Hügel |
| **FIfF-Überall** | Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert.biskup@gmx.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 *redaktion@fiff.de* |
| **Lesen, SchlussFIfF** | Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de* |
| **Layout** | Berthold Schroeder |
| **Titelbild** | Dr. Johannes W. Dietrich |
| **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*)

**Freedom not Fear 2013**
27. bis 30. September in Brüssel

**FIfF-Jahrestagung 2013**
25. bis 27. Oktober in Siegen
Arthur Woll Haus, Am Eichenhang 50, 57076 Siegen
*„Cyberpeace"*

**FIfF-Mitgliederversammlung**
27. Oktober, 11:00 bis 14:00 Uhr
Arthur Woll Haus, Am Eichenhang 50, 57076 Siegen

**41.5 KIF**
30. Oktober bis 3. November in Erlangen

**30C3 – Chaos Communication Congress 2013**
27. bis 30. Dezember in Hamburg

**FIfF-Klausurtagung 2014**
21. bis 23. März 2014 in Bad Hersfeld

---

**FIfF-Kommunikation**
**4/2013** »Faire Computer«
Sebastian Jekutsch
Redaktionsschluss 1.11.2013

**1/2014** »Cyberpeace«
Sylvia Johnigk, Kai Nothdurft, Stefan Hügel
Redaktionsschluss 1.2.2014

---

**W&F – Wissenschaft & Frieden**
2/13 – Kriegslügen
3/13 – Jugend und Konflikt
4/13 – Pazifisches Jahrhundert
1/14 – Innergesellschaftliche Konflikte
2/14 – Neuer Kolonialismus
3/14 – Krieg und Frieden und die Künste

---

**DANA – Datenschutz-Nachrichten**
1/13 – Löschen
2/13 – Konzernprivileg
3/13 – Kommunale Software

## Das FIfF-Büro

**Geschäftsstelle FIfF e.V.**
Ingrid Schlagheck (Geschäftsführung) – Bremen
Sara Stadler – Bremen
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:** Wir bitten alle Mitglieder und Abonnenten, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

# Schluss FIfF

## For Snowden – 6.000 miles

Original: 500 Miles – The Hooters, alternativer Text: Sylvia Johnigk und Kai Nothdurft, 1.9.2013


*Foto: Trojan_Llama, CC BY-NC-SA 2.0*

*If you missed the flight I'm on you will know that I am gone*
*you can hear the whistle blow 6000 miles*
*6000 miles 6000 miles 6000 miles 6000 miles*
*you can hear the whistle blow 6000 miles*

*Not a shirt on my back not a penny to my name*
*and the land that I once loved is not my own*
*lord I'm two lord I'm three lord I'm four lord I'm five*
*lord I'm 6000 miles away from home yea*

*A million spies in cyberspace a one man stands and stops the race*
*someday soon the tide will turn and I'll be free*
*I'll be free I'll be free I'll come home to my country*
*someday soon the tide will turn and I'll be free*

*If you miss the flight I'm on you will know that I am gone*
*you can hear the whistle blow 6000 miles*
*lord I'm two lord I'm three lord I'm four lord I'm five*
*lord I'm 6000 miles away from home*

*Lord I'm 6000 miles away from home yea*
*I'll be free I'll be free I'll come home to my country*
*lord I'm 6000 miles away from home*

*You can hear the whistle blow 6000 miles*
*lord I'm 6000 miles away from home*

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