H 7625

FIfF-Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

30. Jahrgang 2013 Einzelpreis: 7 EUR

4/2013 – Dezember 2013

Faire Computer

ISSN 0938-3476

• Menschenrecht auf Privatheit • FIfF-Studienpreis 2013 • Internet-Polizei •

FIfF Kommunikation

Titelbild: Oh Wunder Kommunikationsdesign

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Inhalt

Ausgabe 4/2013

inhaltt

Editorial

Smartphones, Tablets, Notebooks oder – inwischen immer seltener – „einfache" Handys sind uns zur täglichen Gewohnheit geworden. Manche von uns sind mittlerweile regelrecht abhängig davon, wir können uns ein Leben ohne ständige Erreichbarkeit – und gleichzeitig ohne Andere ständig erreichen zu können – fast nicht mehr vorstellen. Doch offenbar reicht uns das nicht aus: Es muss auch immer die neueste Version sein. Sei es, um dem immer schneller voranschreitenden technischen Fortschritt zu folgen, sei es, um ständig mit dem aktuellsten Statussymbol glänzen zu können, oder sei es, weil wir auf die Marketing-Strategien der Anbieter hereinfallen: Spätestens nach zwei Jahren eilen wir zum Handy-Shop, um dort das neueste Modell zu erstehen.

Was beim Konsum ein wenig aus dem Blick gerät, ist die Produktion dieser kleinen Geräte. Von einem besonders wichtigen Aspekt des Lebenszyklus handelt der Schwerpunkt in diesem Heft: Seinen Auswirkungen auf die betroffenen Menschen.

Befassen wir uns genauer mit dem Thema, lesen wir viel über Konfliktmineralien, Selbstmorde in Fertigungswerken oder giftige Entsorgung von Elektroschrott in Afrika. In diesem Heft wollen wir jedoch nicht weiter klagen, sondern uns den Gegenstrategien widmen: Wie können wir zu einer sozialverträglicheren Produktion von Elektronikprodukten gelangen? Eine Reihe von Autoren bekannter Institute und Organisationen und Vertreter aus der Wirtschaft berichten über Ideen und Wege hin zu faireren Computern. Gesetzliche Regelungen müssen her, Zertifikate und Labels sind wichtig, Recherche und Aufklärung tut Not, Graswurzelbewegungen fangen einfach mal an, Gewerkschaften müssen gestärkt werden ... dies sind einige der Ansätze, die in diesem Heft vorgestellt werden. Ein eigenes Schwerpunkt-Editorial führt detaillierter in das Thema ein. Neben der Verbesserung der Situation der in diesem Sektor beschäftigten Menschen muss dabei auch das Wissen der Nutzerinnen und Nutzer verbessert werden: Damit befasst sich ein Artikel über die Einbindung von *Fair IT* in den Schul- und Hochschulstoff, der auch gut in den Schwerpunkt *Informatik und Bildung* des letzten Heftes gepasst hätte.

Während wir dies lesen, hält der Angriff auf unsere Privatsphäre durch staatliche Behörden an: Auch wenn Bundeskanzlerin Angela Merkel auf ihre eigene Ausspähung empört reagiert hat – die millionenfache Verletzung der Persönlichkeitsrechte der Bevölkerung scheint sie weniger zu interessieren. Das mag daran liegen, dass offenbar auch deutsche Behörden, unter der Kontrolle aller Bundesregierungen seit dem zweiten Weltkrieg, die Ausspähung unterstützen und betreiben.

Aus rechtlicher Sicht wirft *Marie-Theres Tinnefeld* einen Blick auf die Überwachungspraxis der Geheimdienste. „*Ergänzung des völkerrechtlichen gesicherten Grundrechtsschutzes, mehr Transparenz nachrichtendienstlicher Tätigkeit und die Bereitstellung sicherer Verschlüsselungsverfahren als Standard und Normalfall*" fordert sie in ihrem Beitrag *Das Menschenrecht auf Privatheit und Kommunikation*.

Durch die Studie *Überwachtes Deutschland* von *Josef Foschepoth* wurde die verfassungswidrige Überwachung des Post- und Fernmeldeverkehrs durch alliierte und deutsche Behörden seit der Gründung der Bundesrepublik bekannt. *Britta Schinzel* hat den Band rezensiert. Nicht nur in der ehemaligen DDR hat das Post- und Fernmeldegeheimnis offenbar faktisch nicht existiert, sondern mindestens ebensowenig in der BRD. „*Foschepoths These ist, dass die Überwachung ein wesentlicher Struktur bildender Teil des historischen Prozesses der Weststaatsbildung der BRD war. ... Es ist ein sehr trauriges Buch*" resümiert sie in ihrer Rezension.

Was seit der letzten Ausgabe der *FIfF-Kommunikation* passiert ist, und welche weiteren Enthüllungen ans Licht gekommen sind, hat *Sara Stadler* in der Fortsetzung ihrer Chronik zusammengetragen. Mit einem Beispiel der Überwachung, die parallel zu der öffentlich zur Schau getragenen Empörung weiter vorangetrieben wird, befasst sich der Beitrag von *Stephan Geelhaar*: *Ausbau der Internet-Polizei*, die sich mit der Neuregelung der Bestandsdatenauskunft im Bundesland Mecklenburg-Vorpommern auseinandersetzt.

Bereits im letzten Jahr hatte sich das FIfF mit der Neubesetzung eines für *Informatik und Gesellschaft* besonders bedeutenden Lehrstuhls befasst – dem *Lehrstuhl für Informatik und Bildung* an der Humboldt-Universität zu Berlin, den bisher *Wolfgang Coy* inne hatte. Wir befürchteten damals eine fachfremde Besetzung und appellierten an die Verantwortlichen, diese fachfremde Besetzung zu vermeiden. *Klaus Fuchs-Kittowski* macht in seinem Beitrag deutlich, dass unser Appell ungehört verhallt ist. Er bezeichnet die Umprofilierung in einen Lehrstuhl, der sich hauptsächlich mit intelligenten Tutoringsystemen – lies automatisierter Studierendenausbildung – beschäftigt, als klare Fehlentscheidung.

Vom 25.-27. Oktober 2013 fand in Siegen unsere Jahrestagung *Cyberpeace – Frieden gestalten mit Informatik* statt. Einer der vielen Höhepunkte der Tagung war wieder die Verleihung des *FIfF-Studienpreises*. Nach einer Zusammenfassung der Tagung berichten wir über die Preisverleihung und drucken die Laudationes auf die Preisträgerinnen und Preisträger ab. Das nächste Heft wird sich der Tagung ausführlich widmen.

Dietrich Meyer-Ebrecht befasst sich in einer weiteren Rezension mit dem Sammelband *Töten per Fernbedienung*, der, von *Peter Strutynski* herausgegeben, sich mit der Intensivierung des weltweiten Drohnenkrieges auseinandersetzt. Berichte von Tagungen und Veranstaltungen runden die Ausgabe ab.

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

Stefan Hügel
für die Redaktion

Brief an das FIfF

„Oh! Wir werden ausgespäht!“

Ich schwöre,
dass ich meine Kraft dem Wohle des deutschen Volkes widmen,
seinen Nutzen mehren,
Schaden von ihm wenden,
das Grundgesetz und die Gesetze des Bundes wahren und verteidigen,
meine Pflichten gewissenhaft erfüllen
und Gerechtigkeit gegen jedermann üben werde.
(Eidesformel der Bundeskanzlerin nach Art. 56 GG und Art. 64 GG)

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

spätestens seit dem 6. Juni 2013 wissen wir, dass unsere Kommunikation durch Geheimdienste – allen voran die US-amerikanische NSA und das britische GCHQ – umfassend ausgespäht wird. Es verdichten sich Erkenntnisse, dass auch der *Bundesnachrichtendienst* (BND) und das *Bundesamt für Verfassungsschutz* (BfV) großen Anteil an dieser Ausspähung hatten und haben.

Doch die nun veröffentlichten Informationen bilden offenbar nur die Spitze des Eisbergs. Die Untersuchungen des Freiburger Historikers Professor Dr. *Josef Foschepoth* zeigen, dass bereits unmittelbar nach dem zweiten Weltkrieg eine umfassende Überwachung der deutschen Bevölkerung in der Bundesrepublik begonnen hat – erst unter Besatzungsrecht, später formaljuristisch legitimiert durch das G10-Gesetz. Details wurden stets geheim gehalten. Die öffentliche Aufmerksamkeit, wie wir sie jetzt erleben, erhielt das Thema erst durch die Enthüllungen des ehemaligen US-amerikanischen Geheimdienstmitarbeiters *Edward Snowden* – auch wenn es bereits in der Vergangenheit vereinzelt diskutiert wurde, beispielsweise bei der Abhöraffäre 1963/64 oder im Zusammenhang mit dem Spionagesystem *Echelon*.

Die Bundesregierung reagierte – scheinbar – gleichgültig. Erst als bekannt wurde, dass offenbar auch Bundeskanzlerin Angela Merkel ausgespäht wurde, wurde ihr Interesse geweckt: An ihrer eigenen Ausspähung, nicht etwa an der Ausspähung der gesamten Bevölkerung.

Unklar ist nach wie vor, wie es möglich gewesen sein soll, dass im politischen Berlin – und Bonn – niemand etwas von der offenbar seit 60 Jahren bestehenden Überwachung gewusst hat. Sind hier wirklich Geheimdienste außer Kontrolle geraten, oder haben sie im Gegenteil genau so agiert, wie es die politisch Verantwortlichen von ihnen erwartet haben? Besonders die wissenschaftlichen Erkenntnisse von Foschepoth legen den Verdacht nahe, dass mit der zur Schau getragenen öffentlichen Empörung sowohl der bisherigen Regierungspartei CDU als auch der bisherigen Oppositionspartei SPD ein Volkstheater zur Beschwichtigung der Menschen aufgeführt wird. Man hat den Eindruck, dass keineswegs die Absicht besteht, irgendetwas an der grundsätzlichen Situation zu ändern – sofern man nicht selbst davon betroffen ist.

Im Gegenteil: Den Nachrichten zufolge, die aus den Koalitionsverhandlungen an die Öffentlichkeit dringen, soll nicht nur die Vorratsdatenspeicherung wieder eingeführt werden, die das Bundesverfassungsgericht (in der damals bestehenden Form) verworfen hatte, die gerade vom Europäischen Gerichtshof einer Überprüfung unterzogen wird und die der frühere Bundesinnenminister *Otto Schily* mit den Überwachungsmaßnahmen der NSA verglichen hat. Einzelnen Nachrichten zufolge werden sogar weitere Ausspähmaßnahmen ins Spiel gebracht: Die Abkehr von der strikten Zweckbindung der Mautdaten von *Toll Collect* – damals eine explizite Voraussetzung für die Inbetriebnahme des Systems – und sogar das Abgreifen von Kommunikationsdaten an Netzknotenpunkten nach dem Beispiel von NSA und GCHQ werden offenbar diskutiert. Auch wenn entsprechende Nachrichten schnell dementiert wurden – offensichtlich haben solche Vorhaben ihre Befürworter. Bestürzend sind auch Nachrichten über Versuche der britischen Regierung, die freie Presse einzuschüchtern und in die Nähe des Landesverrats zu rücken.

Durch Untersuchungen von *Amnesty International* kam gerade wieder eine besonders hässliche Seite der informatikgestützten Kriegführung in die öffentliche Diskussion. Die Kriegführung vor allem der Amerikaner mit Drohnen, deren öffentliche Akzeptanz nur schwer nachzuvollziehen ist.

Den Untersuchungen zufolge erfüllen manche Drohneneinsätze den Tatbestand eines Kriegsverbrechens – ein Kriegsverbrechen, das wohl nie angeklagt werden wird. „Ich hatte bisher keine Angst vor Drohnen, aber jetzt, wenn sie über unsere Köpfe fliegen, frage ich mich: ‚Werde ich die nächste sein?‘“, zitiert Amnesty International ein achtjähriges Mädchen, das dem Bericht zufolge zusehen musste, wie ihre Großmutter Opfer eines Drohnenangriffs wurde. Es ist enttäuschend und verstörend, dass der als Lichtgestalt angetretene US-Präsident Barack Obama, der kurz nach seinem Amtsantritt gar mit dem Friedensnobelpreis ausgezeichnet wurde, diese Form des Krieges mit dem Ziel der Tötung tatsächlicher und vermeintlicher Terroristen ohne gerichtliches Verfahren und mit nicht hinnehmbaren zivilen Opfern offenbar intensiviert und vorantreibt.

Eine weitere Tragödie wird gerade durch die Ereignisse vor Lampedusa sichtbar: Die weitgehende Freizügigkeit innerhalb der Europäischen Union erkaufen wir uns dadurch, dass wir die EU nach außen zur Festung ausbauen. Eine Politik, die verschiedenen Berichten zufolge bereits tausende Menschenleben gekostet hat – die Ereignisse der letzten Wochen werfen lediglich ein Schlaglicht auf das, was seit Jahrzehnten immer wieder geschieht. Trotzdem sind politisch Verantwortliche nicht bereit, Menschen, die zum Schutz vor politischer Verfolgung und wirtschaftlichem Elend zu uns kommen, angemessene Hilfe zu leisten. Die diskriminierende Behandlung von Geflüchteten im SPD-regierten (!) Hamburg ist leider nur ein Beispiel dafür.

Turnusgemäß wird alle zwei Jahre ein neuer FIfF-Vorstand gewählt – so auch dieses Jahr bei der Jahrestagung in Siegen, für die ich den Organisatoren, allen voran *Sylvia Johnigk*, *Kai Nothdurft*, *Jens Rinne*, unserem Gastgeber *Volker Wulf* und *Ingrid Schlagheck* und *Sara Stadler* aus der Geschäftsstelle sehr herzlich danke. Vieles ist konstant geblieben – drei neue Mitglieder gehören dem Vorstand nun an: *Rainer Rehak* aus Berlin, *Werner Winzerling* aus Fulda und *Eberhard Zehendner* aus Jena. *Raffael Rittmeier* kandidierte nicht mehr und scheidet damit aus dem Vorstand aus. Vielen Dank an Raffael für die in den vergangenen vier Jahren im Vorstand geleistete Arbeit und herzliche Glückwünsche an alle neu- und wiedergewählten Mitglieder.

Mit FIfFigen Grüßen

Stefan Hügel

CC BY

FIfF e.V.

FIfF-Jahrestagung Cyberpeace – Frieden gestalten mit Informatik

vom 25.-27. Oktober 2013 im Artur-Woll-Haus an der Universität Siegen

Im Zentrum der 29. FIfF-Jahrestagung, die unter dem Motto Cyberpeace – Frieden gestalten mit Informatik *an der Universität Siegen stattfand, stand die Auseinandersetzung mit dem Einsatz der Informationstechnologie zur Kriegsführung, Spionage und Überwachung, aber auch mit ihrem emanzipatorischen Potenzial im Sinne der Aufklärung und politischen Willensbildung, der Schaffung einer kritischen Gegenöffentlichkeit und der Organisation von Protest. Die rund 100 ExpertInnen und Interessierten diskutierten in Vorträgen und Arbeitsgruppen Strategien, dem anhaltenden Cyberwar die positive Vision eines Cyberpeace entgegenzusetzen, das Wettrüsten mit Cyberwaffen zu beenden, Erkenntnisse und Produkte der Informatik friedlich zu nutzen, digitale Rechte zu etablieren und im virtuellen Raum ‚safe places' für NutzerInnen und AktivistInnen zu schaffen.*

Einig waren sich die Vortragenden darin, dass die aktuelle Spähaffäre dem Tagungsthema zusätzliche Aktualität und Dringlichkeit verliehen hat. Die von den USA und anderen eingesetzten Programme zur militärischen und geheimdienstlichen Aufklärung stellen nicht nur einen massiven Eingriff in die Privatsphäre von TelekommunikationsnutzerInnen dar, sondern dienen eben auch der Ausspähung politischer Angriffsziele und der Vorbereitung digitaler Kriegsführung.

Kai Nothdurft, Mitglied des FIfF-Vorstands, bedankte sich im Rahmen der Tagung bei dem Whistleblower *Edward Snowden*, für dessen Schutz sich das FIfF gemeinsam mit anderen bürgerrechtlichen Organisationen einsetzt. „Ohne diesen mutigen Menschen würde das, was wir bislang über das Ausmaß der weltweiten Telefon- und Internetüberwachung nur vermutet haben, wohl immer noch als paranoid gelten. Nun wissen wir, dass das tatsächliche Ausmaß unsere kühnsten Vorstellungen noch übersteigt", so Nothdurft.

Prof. Dr. *Günter Müller* von der Universität Freiburg behandelte in seinem Vortrag *Datenschutz heute: 30 Jahre zurück statt 30 Jahre voraus?* die Unterschiede im Datenschutz zwischen den USA und Europa, weshalb aus seiner Sicht die informationelle Selbstbestimmung Nutzer überfordert und weshalb die gegenwärtigen Verfahren mit Transparenz ergänzt werden müssen, soll Privatheit auch im Internet in den kommenden 30 Jahren befriedigender als heute durchgesetzt werden können.

Sebastian Schweda, Mitglied von *Amnesty International*, zeigte in seinem Vortrag *Das Imperium schlägt zurück – zur Lage der Menschenrechte im digitalen Zeitalter* anhand einiger Beispiele die ambivalenten Folgen der Digitalisierung für die Menschenrechte: Während moderne Informations- und Kommunikationstechnologien dem Einzelnen neue Chancen zur Wahrnehmung seiner Rechte eröffnen, geben sie Regierungen auch neue Instrumente an die Hand, diese Aktivitäten wirksam zu unterbinden, zu behindern oder zu kontrollieren. Exzessive staatliche Eingriffe in diesem Umfeld zeigen, dass die volle Durchsetzung der Menschenrechte – allen voran des Rechts auf freie Meinungsäußerung, auf freien Informationszugang und auf den Schutz des Privatlebens – zunehmend gefährdet ist. Regierungen überall auf der Welt scheinen gegenwärtig darauf hinzuwirken, die Erleichterungen, die moderne Informations- und Kommunikationstechnologien für die Wahrnehmung der Menschenrechte gebracht haben, unter dem Vorwand der nationalen Sicherheit zu einem erheblichen Teil wieder zu beseitigen oder deutlich einzuschränken.

Foto: Ben Kees

Prof. Dr. *Gloria Mark* von der University of California, Irvine, behandelte in ihrem Vortrag *ICT use to support resilience in regions of conflict: The case of Iraq and the Arab Spring*, wie Informations- und Kommunikationstechnologien in Umgebungen verwendet werden können, in denen Krieg geführt wird, und um Menschen bei politischen Aufständen zu unterstützen. Im Irak wurde beispielsweise untersucht, wie diese Technologien beim Wiederaufbau von Infrastrukturen helfen können. Es wurde untersucht, wie Blogs – und allgemein soziale Medien – unter repressiven Rah-

menbedingungen genutzt werden können. Prof. Mark diskutierte in dem Vortrag, wie die neuartige und veränderte Nutzung von Informations- und Kommunikationstechnologien zu tiefgreifenden strukturellen Veränderungen in den Gesellschaften geführt hat.

Rainer Rehak, Preisträger des FIfF-Studienpreises 2012, behandelte in seinem Vortrag *Geheimnisse und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, welche Implikationen das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in einer globalisierten und digitalisierten Welt hat, wenn die 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?

In Arbeitsgruppen wurde darüber hinaus die Themen *Mitten im Cyberkrieg – der Angriff auf die Zivilgesellschaft*, *Hackertools*, *Videoüberwachung* und *Menschenrechte in einer digitalisierten Welt* behandelt und eine Crypto-Party gefeiert.

Die Arbeitsgruppe *Rüstung und Informatik: Mitten im Cyberkrieg – der Angriff auf die Zivilgesellschaft* des *AK RUIN* ordnete die NSA-Affäre in die von den US-Diensten selbst definierte Begrifflichkeit ein und untersuchte die Folgen für die IT-Sicherheit. Dies wurde ergänzt durch die Vorstellung der Fähigkeiten und militärpolitischen Aktivitäten auf deutscher Seite. Die Betrachtung möglicher Handlungsoptionen führte zu einer intensiven Debatte über Lösungsmöglichkeiten auf technischer und politischer Ebene. Der Workshop *Strukturen des gesichtslosen Blicks – revisited* des *AK Videoüberwachung und Bürgerrechte* zeigte deutlich, dass das Thema Videoüberwachung nichts an Brisanz eingebüßt hat. Die erste Session war von begrifflichen, strukturellen und technischen Themen geprägt. Die zweite Session startete mit zwei Beiträgen zur rechtlichen Einhegung der Videoüberwachung. In die Diskussion überleitend wurde schließlich gezeigt, wie durch die Automatisierung der Videoüberwachung deren gesellschaftliche Folgen zugespitzt und ausgeweitet werden.

In der Arbeitsgruppe *Hackertools* wurde gezeigt, wie leicht die Handhabung ist, und wie viele Möglichkeiten man bekommt, wenn man diese Tools einsetzt. Besonders beeindruckend war, dass man vielfach die Anleitung zu den gezeigten Hacks, durch einfaches ixquick(en) (formerly known as googlen) findet und nachvollziehen kann, ohne tiefgehende Kenntnisse erwerben zu müssen.

Die Arbeitsgruppe *Menschenrechte in einer digitalisierten Welt* diskutierten wie ExpertInnen und IT-Fachleute aus dem FIfF und anderen „IT-lastigen Gruppen und Verbänden" zusammen mit Aktiven aus Menschenrechtsgruppen auf die Risiken der IT-Nutzung hinweisen und Lösungsmöglichkeiten skizzieren können, um der Überwachung durch Behörden zu entgehen.

Auf der Mitgliederversammlung des FIfF wurden neben dem alljährlichen Bericht des Vorstands gemeinsame Forderungen des FIfF zum Cyberpeace verabschiedet. Das FIfF positioniert sich damit erneut gegen die informatikgestützte Kriegsführung, die seit seiner Gründung zu den Kernthemen zählt. Cyberpeace umfasst aber mehr als diese Kritik. „Cyberpeace ist der Gegenentwurf zu den Dystopien des totalen Überwachungsstaates, der Gegenentwurf zu den Kassandrarufen, Privatsphäre war gestern, der Gegenentwurf zur Gleichgütigkeit", wie der stellvertretende FIfF-Vorsitzende *Dietrich Meyer-Ebrecht* hervorhob.

Ebenfalls im Rahmen der Versammlung fand die Neuwahl des FIfF-Vorstands statt. *Stefan Hügel* wurde erneut als Vorsitzender, *Dietrich Meyer-Ebrecht* als sein Stellvertreter gewählt. Als BeisitzerInnen wurden gewählt: *Sylvia Johnigk*, *Hans-Jörg Kreowski*, *Kai Nothdurft*, *Rainer Rehak*, *Jens Rinne*, *Britta Schinzel*, *Ingrid Schlagheck*, *Werner Winzerling* und *Eberhard Zehendner.*

CC BY

Mitgliederversammlung des FIfF

Universität Siegen, Artur-Woll Haus, 27. Oktober 2013, 12:15-14:50 Uhr

– Beschlussprotokoll[1] –

Sitzungsleitung: Stefan Hügel als Vorsitzender des FIfF.

1. Begrüßung und Feststellung der Beschlussfähigkeit und der Protokollführung

Zur Versammlung ist ordentlich eingeladen worden und diese ist dadurch beschlussfähig. Es sind 19 stimmberechtigte Mitglieder anwesend.
Das Protokoll führt: Sylvia Johnigk.

2. Beschlussfassung über Tages-, Geschäfts- und Wahlordnung

Tagesordnung in vorliegender Form und Geschäfts- und Wahlordnung wird von den Anwesenden in bekannter Form genehmigt.

3. Bericht des Vorstands (einschl. Kassenbericht)

Stefan Hügel berichtet über die Arbeit des FIfF und die Vorstandsarbeit in 2013, sowie den Haushalt 2013.
Dabei werden keine Beschlüsse gefasst.

4. Bericht der Kassenprüfer

Für die am 16. Mai 2013 in Bremen durchgeführte Kassenprüfung berichtet Michael Ahlmann der MV. Aus dem Kassenprüfungsprotokoll: *„Dem Vorstand wird eine dem Vereinszweck entsprechende, ordnungsgemäße Kassenführung bescheinigt. Einer Entlastung des Vorstandes steht nach unserer Auffassung nichts entgegen."* (Derzeitige Kassen-

prüfer: Michael Ahlmann, Kurt Fussangel, Klaus Lüttich und Gernot Lucks.)
Dabei werden keine Beschlüsse gefasst.

5. Diskussion der Berichte

Dabei werden keine Beschlüsse gefasst.

6. Entlastung des Vorstandes

Michael Ahlmann beantragt die Entlastung des Vorstands, dieser Antrag wird einmütig angenommen.

7. Neuwahl des Vorstands

Die MV bestimmt einmütig bei einer Enthaltung Peter Bittner als Wahlleitung. Peter Bittner übernimmt die Sitzungsleitung und stellt fest, dass 19 stimmberechtigte Mitglieder anwesend sind.
Wahl der/des Vorstandsvorsitzenden:

Vorschlag:
Stefan Hügel

gültig abgegeben:	19
ja:	17
nein:	0
enthalten:	2

Stefan Hügel ist gewählt und nimmt die Wahl an.

Wahl der/des stellvertretenden Vorstandsvorsitzenden:

Vorschlag:
Dietrich Meyer-Ebrecht

gültig abgegeben:	19
ja:	17
nein:	0
enthalten:	2

Dietrich Meyer-Ebrecht ist gewählt und nimmt die Wahl an

Wahl der Beisitzerinnen und Beisitzer:

19 abgegeben, davon: 19 gültig, 0 ungültig

Vorschläge	ja/nein/enth.	Wahl angenommen
Eberhard Zehendner	15 / 3 / 1	
Werner Winzerling	16 / 0 / 3	ja
Rainer Rehak	19 / 0 / 0	ja
Ingrid Schlagheck	17 / 0 / 2	ja
Sylvia Johnigk	17 / 1 / 1	ja
Kai Nothdurft	18 / 0 / 1	ja
Jens Rinne	18 / 0 / 1	
Hans-Jörg Kreowski	19 / 0 / 0	ja
Britta Schinzel	17 / 0 / 2	
Julia Stoll	Keine Kandidatur	

Alle Kandidierenden sind gewählt und Britta Schinzel, Jens Rinne und Eberhard Zehendner müssen ihre Annahme schriftlich erklären. Die anderen gewählten Personen sind anwesend und nehmen die Wahl an.

8. Neuwahl der Kassenprüfer

Stefan Hügel übernimmt als Vorsitzender des FIfF die Sitzungsleitung.
Die MV wählt Kurt Fussangel (19 ja/0 nein/0 enth.), Michael Ahlmann (19/0/0), Gernot Lucks (19/0/0) und Klaus Lüttich (19/0/0) vorbehaltlich der Zustimmung der nicht anwesenden Kandidaten zu den neuen Kassenprüfern des FIfF. Michael Ahlmann nimmt die Wahl an.

9. Diskussion über Ziele und Arbeit des FIfF, aktuelle Themen, Verabschiedung von Stellungnahmen

Es werden keine Beschlüsse gefasst.

10. Anträge an die Mitgliederversammlung

Die Mitgliederversammlung hat den geänderten Antrag über die Forderungen des FIfF zum Cyberpeace einstimmig verabschiedet.

11. Verschiedenes

Es werden keine Beschlüsse gefasst.
Die Mitgliederversammlung dankt Raffael für seine Arbeit im Vorstand.
Die Anwesenden danken für die tolle Organisation dieser Jahrestagung.

12. Genehmigung des Protokolls

Das Protokoll wird einstimmig genehmigt.

---

1 Inoffizielle Fassung, formal redigiert.

Uraufführung „For Snowden – 6.000 miles"
Text siehe SchlussFIfF 3/2013, Foto: Ben Kees

FIfF-Studienpreis 2013 verliehen

Arbeiten aus dem Gebiet *Informatik und Gesellschaft* ausgezeichnet

Im Rahmen der 29. FIfF-Jahrestagung, die unter dem Motto Cyberpeace – Frieden gestalten mit Informatik *an der Universität Siegen stattfand, wurden zum dritten Mal herausragende Qualifikationsarbeiten aus dem Themenbereich Informatik und Gesellschaft mit dem* FIfF-Studienpreis *prämiert. Mit der Verleihung des Studienpreises möchte das FIfF einen Beitrag leisten, die immer wieder von Sparzwängen an den Hochschulen betroffene Forschung zu den gesellschaftlichen Auswirkungen der Informationstechnologie zu fördern.*

Die PreisträgerInnen wurden von einer Jury ausgewählt, die mit Prof. Dr. *Britta Schinzel* (Freiburg im Breisgau), Prof. Dr. *Marie-Theres Tinnefeld* (München), Prof. Dr. *Jochen Koubek* (Bayreuth), *Rainer Rehak* (Berlin) und *Stefan Hügel* (Frankfurt am Main) besetzt war.

Der erste Preis ging in diesem Jahr an *Daniel Spittank* für seine Arbeit *Auswahl und Gestaltung mobiler Informatiksysteme für den Einsatz im Informatikunterricht*. Die Arbeit, die im Rahmen der Ersten Staatsprüfung an der Bergischen Universität Wuppertal verfasst wurde, beschäftigt sich mit den Kriterien, nach denen mobile Systeme wie Tablets und Smartphones im Unterricht eingesetzt werden sollten. Wie der Studienpreisträger des Jahres 2012, *Rainer Rehak*, in seiner Laudatio erläutert, beschränkt sich die Relevanz der Fragestellung dabei keineswegs auf den schulischen Informatikunterricht. Daniel Spittanks Arbeit nimmt sich vielmehr der dringlichen Aufgabe an, der jungen Generation eine mündige Teilhabe an der digitalen Gesellschaft zu ermöglichen.

Mit dem zweiten Preis wurde die Diplomarbeit *‚Due to legal Issues' – Packet Inspection* von *Agata Królikowski* ausgezeichnet, die an der Humboldt-Universität zu Berlin entstanden ist. Mit der untersuchten Packet Inspection (PI) können Verkehrsdaten analysiert werden, deren Auswertung die Erstellung von Sozialbeziehungs- und Bewegungsprofilen erlaubt. Die Arbeit stellt diese Technologie dar und untersucht, ob und mit welchen technischen oder rechtlichen Maßnahmen sich NutzerInnen vor Angriffen auf ihre Kommunikation schützen können. Damit lenkt

Die Preisträger und die Laudatoren, alle Fotos: Benjamin Kees

Agata Królikowski den Fokus auf ein Thema von hoher aktueller Relevanz, wie der FIfF-Vorsitzende *Stefan Hügel* in seiner Laudatio unterstreicht. Verkehrsdaten sind ein wesentlicher Bestandteil der weltweiten Datenausspähung. Auch wenn Agata Królikowski zu dem Schluss kommt, dass es letztlich keinen Schutz gegen PI-Angriffe gibt, ist das Sichtbarmachen der Problematik ein erster Schritt in Richtung einer umfassenden Aufklärung und Sensibilisierung.

Der dritte Preis wurde an *Julia Hofmann* für ihre Dokumentation der betrieblichen Projektarbeit an der TU Darmstadt mit dem Titel *Zweckgebundener Datenbrief für das Identitätsmanagementsystem mittels Web-basiertem Benutzerinterface* verliehen. Mit dem erstellten Datenbrief sollen sich Angehörige der

1. Preis	**Daniel Spittank** **Bergische Universität Wuppertal** *Auswahl und Gestaltung mobiler Informatiksysteme für den Einsatz im Informatikunterricht*	Laudatio: Rainer Rehak
2. Preis	**Agata Królikowski** **Humboldt-Universität zu Berlin** *‚Due to legal Issues' – Packet Inspection*	Laudatio: Stefan Hügel
3. Preis	**Julia Hofmann** **Technische Universität Darmstadt** *Zweckgebundener Datenbrief für das Identitätsmanagementsystem mittels Web-basiertem Benutzerinterface*	Laudatio: Britta Schinzel
Sonderpreis	**Helge Peters** **University of London** *Biopolitical Simulations: Governing Live in FuturICT*	Laudatio: Britta Schinzel

Die Preisträger im Überblick

TU Darmstadt über ein Benutzer-Interface selbstständig informieren können, welche personenbezogenen Daten für welchen Zweck im Hochschulrechenzentrum verarbeitet werden. Wie *Britta Schinzel* in der Laudatio hervorhebt, ist die Transparenz der Speicherung und Verwertung personenbezogener Daten ein Thema von aktueller gesellschaftlicher Bedeutung, das in der Arbeit praktisch umgesetzt wird.

Die Auswahlkommission hat sich in diesem Jahr entschieden, eine Sonderurkunde für gesellschaftliche Relevanz zu verleihen, mit der *Helge Peters* für seine Masterarbeit an der University of London *Biopolitical Simulations: Governing Life in FuturICT* ausgezeichnet wurde. Peters untersucht das von der Europäischen Union geförderte Projekt *FuturICT*, das durch die Gewinnung von *Big Data* vorausschauende Simulationen globaler sozialer und ökonomischer Systeme herstellen will. Er greift dabei auf *Michel Foucaults* Konzept der *Biomacht* zurück und fragt, inwieweit die in dem Projekt angestrebte digitale Berechenbarkeit des Lebens Ausdruck einer spezifischen Form der *Biopolitik* ist. Wie *Britta Schinzel* in ihrer Laudatio hervorhebt, dient das von Helge Peters untersuchte Projekt der Naturalisierung des Sozialen, und damit der Stabilisierung bestehender Verhältnisse und ist so auch Ausdruck einer wissenschaftlichen Unterstützung des Überwachungsstaates. Peters plädiert für eine situierte Positionierung der WissenschaftlerInnen als bescheidene ZeugInnen, statt eines angeblich objektiven Blicks von nirgendwo. Darin liegt die hohe gesellschaftliche Relevanz seiner Arbeit.

Das FIfF gratuliert allen PreisträgerInnen herzlich und wird auch im nächsten Jahr wieder einen Studienpreis vergeben. Einreichungen hierzu sind sehr willkommen.

CC BY

Rainer Rehak – Laudatio für den ersten Preis

Daniel Spittank: *Auswahl und Gestaltung mobiler Informatiksysteme für den Einsatz im Informatikunterricht*

Man sagt ja, dass eine Technik dann in der Gesellschaft angekommen ist, wenn sie nicht mehr als solche wahrgenommen wird. Nur ganz gelegentlich wird uns bewusst, dass ein Stromanschluss in jedem Haushalt doch eigentlich nach wie vor etwas ziemlich Bemerkenswertes ist. Diese Verschleierung entzieht die Technik aber auch dem breiten gesellschaftlichen Diskurs, der dann nur durch Brüche oder spezielle Umstände zeitweilig wieder belebt wird.

Beim elektrischen Strom ist die Tiefenwirkung auf einzelne Menschen und der Einfluss auf die Strukturierung der Gesellschaft jedoch weniger folgenreich, als es aktuell die breite Nutzung informatischer Systeme ist. Der Teil der Gesellschaft wird immer kleiner, der überrascht ist, dass man Computer nicht nur für geschäftliche E-Mail-Kommunikation oder arbeitsbezogene Informationsbeschaffung nutzen kann, sondern auch ganz privat für höchstpersönliche Tätigkeiten und Interaktionen, soziale Netzwerke, private Interessenausübung, Unterhaltung, Einkauf oder politische Partizipation. Der größere Teil der Gesellschaft ist eben nicht mehr *manchmal online*, sondern nur noch *manchmal offline* und bald wird auch die Aussage *online sein* keinen Sinn mehr ergeben, weil es jeder immer sein wird.

Vor diesem Hintergrund stellt sich natürlich die Frage, wie man junge Menschen darauf vorbereiten kann, in den neuen, scheinbar freien Räumen voller *aktuell angesagter* Videos und *von Freunden empfohlener* Produkte zu bemerken, wo privat-vermachtete Konsumräume beginnen, wo interessengeleitete Akteure verdeckt ihre Agenda umzusetzen suchen, wo technische Ideologien ihre überzogenen Heilversprechen darbieten, aber auch, wo sich fantasievolle Aufrichtigkeit ausdrückt, wo kritische Reflexionen auf Wissenshungrige warten oder wo freie Ideen nach freien Mitstreitern rufen.

Neu an diesen orientierenden Fragestellungen ist die genuintechnische Dimension: Wie entstehen Wikipedia-Artikel, was ist

Daniel Spittank

das Geschäftsmodell von Facebook, wie sortiert Google Ergebnisse, wie entstehen Apps, warum gibt die NSA jährlich eine Milliarde Dollar für Kryptologen aus, wo liegen meine Cloud-Daten, was ist freie Software, welche Daten hinterlässt mein Browser, wem gehört Youtube? All diese wesentlichen Fragen haben einen spezifisch-technischen Teil; daher ist es nur folgerichtig, für eine verpflichtende informatische Bildung aller Schülerinnen und Schüler einzutreten.

Diese Forderung aber auch gleich konsequent mit einem ganzheitlichen Ansatz in ein Unterrichtsrahmenmodell zu transformieren, welches ausgearbeitet ist von der Explikation des Menschenbildes und des Bildungsverständnisses, über die Analyse und Herausarbeitung einer konkreten Lernumgebung bis zur Erstellung einer Python-Klassenbibliothek für verstehen-orientiertes Lernen, das finden wir vom FIfF höchst bemerkenswert und auszeichnungswürdig, daher herzlichen Glückwunsch, *Daniel Spittank*, zum ersten Platz des Studienpreises 2013 vom Forum der InformatikerInnen für Frieden und gesellschaftliche Verantwortung.

Daniel Spittank konstatiert in seiner Arbeit zunächst anhand von Studien die wesentliche Durchdringung des Alltags mit informatischen Systemen – insbesondere in der Welt der Jugendlichen – und leitet daraus ab, dass informatische Allgemeinbildung dringender denn je benötigt wird, wenn das pädagogische Ziel der Befähigung zur mündigen Teilnahme an der informatisch-vernetzten Gesellschaft erreicht werden soll.

Leider, so Daniel Spittank weiter, ist optionaler Informatikunterricht in traditionellen, unflexiblen Computerräumen mit festen Arbeitsplätzen für diese Aufgabe gänzlich unbrauchbar; vor allem, wenn auch in anderen Fächern Computereinsatz gefragt ist.

Bei der Herausarbeitung der Anforderungen an derartig verwendbare Informatiksysteme kommt er zum Schluss, dass nur mobile Systeme mit (möglichst) freier Software dafür geeignet sind; sowohl hinsichtlich der Verstehbarkeit und Anpassbarkeit, aber auch in Hinblick auf Datenschutz und die Sicherheit der Systeme. (Mobile Systeme sind dabei Systeme, die mobil verwendet werden können, also Smartphones und Tabletcomputer; nicht zu verwechseln mit transportablen Informatiksystemen wie Laptops.) Dabei ist es natürlich kein Zufall, dass diese Geräte bei Kindern und Jugendlichen ohnehin am weitesten verbreitet und für sie sehr bedeutsam sind.

Apples iOS-Geräte sind ohne Jailbreaking reine Konsumplattformen, was sie sogleich für die hier relevanten pädagogischen Zwecke disqualifiziert. Aktuell favorisiert Daniel Spittank daher Googles Android unter der Nutzung von Python for Android. Wirklich freie Alternativen stehen jedoch unter erwartungsvoller Beobachtung.

Ganz wesentlich ist die Bearbeitung der Frage, wie die verfügbaren Systeme für einen praktischen Unterrichtseinsatz (um-)gestaltet werden müssen. Der übergeordnete Ansatz dafür kann mit dem Slogan *Durchblicken statt ‚rumklicken'* beschrieben werden, denn Daniel Spittank möchte weg von weit verbreiteten reinen Anwendungsanleitungen hin zur Beschreibung und Erklärung grundlegender (informatischer) Prinzipien. Einerseits kann sonst keine vernunftgeleitete Auseinandersetzung mit dem Informatiksystem stattfinden, aber andererseits würde mit jeder neuen Programmversion im Zweifelsfall auch ein neuer Lehrgang fällig.

Um es mit seinen Worten zusammenzufassen:

> *„Doch um beim Umgang mit Informatiksystemen selbstbestimmt und frei handeln und erst recht, um aktiv und konstruktiv gestaltend an der Gesellschaft mitwirken zu können, reichen technische Fertigkeiten nicht aus. Es ist vielmehr notwendig, informatische Vernunft zu entwickeln, die ein Verständnis der zugrunde liegenden informatischen Prinzipien bedingt."*

E-Learning-Apps mit den dazu passenden Schritt-für-Schritt-Anleitungen, natürlich auch für die Eltern, jedoch ohne Vermittlung von Hintergrundwissen, müssen folglich vermieden werden. Der Überblick und die Analyse vorhandener Broschüren, Ratgeber und Lehrmaterialien zum Thema mobile Lernsysteme ergeben jedoch auch kein gutes Bild: Mangelnde Qualität, veraltete Inhalte und versteckte Kaufanreize für die Marken der Sponsoren stehen im Vordergrund und lassen auch die engagierte Lehrkraft letztendlich ohne Unterstützung. Überaus positiv werden jedoch die fachdidaktischen Arbeiten von Carrie, Heming und Humbert hervorgehoben, die sich auch schon praktisch in Pilotkursen mit mobilen Informatiksystemen bewährt haben; auch im Hinblick auf die Gender-unabhängige Begeisterung der Schülerinnen und Schüler für derartigen Unterricht. An dieser Stelle: Respekt für die sehr umfangreiche Literatur- und Kursrecherche.

Auf die konkreten Argumentationsstränge und Ergebnisse bezüglich der Umsetzung werde ich allerdings nicht weiter eingehen, da Daniel Spittank das sicher jetzt gleich oder auch später schriftlich in der *FIfF-Kommunikation* zusammenfassend tun wird.

Einzig über eine detailliertere Diskussion der gesellschaftlichen Relevanz mobiler Informationssysteme hätten wir uns gefreut, sodass der gesamtgesellschaftliche Kontext stärker hätte herausgearbeitet werden können, aber trotzdem: für die konkrete Ausarbeitung, den zukünftigen Einsatz, sowie die Weiterentwicklung der Lernumgebung wünschen wir Dir, Daniel Spittank, viel Erfolg und bedanken uns für die beeindruckend nützliche Arbeit.

Stefan Hügel – Laudatio für den zweiten Preis

Agata Królikowski: *‚Due to legal issues' – Packet inspection*

Am 6. Juni 2013 wurde erstmals in der britischen Tageszeitung *The Guardian* über das Programm PRISM der US-amerikanischen *National Security Agency* berichtet. Zahlreiche weitere Berichte, die seither – teilweise in schneller Folge – veröffentlicht wurden, zeigen, dass die freie, unbeobachtete Kommunikation – ein wesentlicher Stützpfeiler von Freiheit, Menschenrechten und Demokratie – eine Illusion war. Die Überwachungsprogramme, die zum Beispiel unter den Namen PRISM, *Tempora* und *XKeyScore* bekannt geworden sind, stellen alle bisherigen Ansätze zur Ausspähung der Bevölkerung in den Schatten.

Zwei Arten von Informationen werden bei solchen Ausspähprogrammen erfasst: Inhaltsdaten, also die versendeten Nachrichten selbst, und Verkehrsdaten, die die Information enthalten, wer wann, von wo aus und mit wem kommuniziert hat. Letztere werden häufig als harmlos dargestellt – ob aus Ahnungslosigkeit oder zur bewussten Irreführung der Öffentlichkeit, soll heute keine Rolle spielen. Doch ohne jeden Zweifel können damit zum Beispiel detaillierte Bewegungsprofile oder auch komplette Sozialbeziehungsgraphen erstellt werden.

Um Informationen aus den Datenströmen zu gewinnen, werden Verfahren der *Packet Inspection* eingesetzt. Dabei werden die Datenpakete einzeln „inspiziert" und damit auf die enthaltenen Informationen hin untersucht.

Mit Packet Inspection – differenziert nach Deep Packet Inspection und Statistical Packet Inspection – befasst sich die Arbeit von *Agata Królikowski* von der Humboldt-Universität zu Berlin, die die Jury des *FIfF-Studienpreises* heute mit dem zweiten Preis auszeichnet.

Die Arbeit stellt die Technologie der Packet Inspection dar und untersucht, ob und welche technischen und rechtlichen Maßnahmen zur Verfügung stehen, um sich vor Angriffen auf die Kommunikation mit Verfahren der Packet Inspection zu schützen.

In diesem Sinne behandelt die Autorin zwei Fragen:

- Wie funktionieren Paketanalysemethoden und wie effizient sind sie?
- Gibt es für die Nutzerinnen und Nutzer des Internet einen technischen oder rechtlichen Schutz gegen diese Analysen?

Sie untersucht die Funktionsweise von Deep Packet Inspection und erörtert anhand der üblichen Schutzziele – Vertraulichkeit, Integrität, Verfügbarkeit – technische Schutzmaßnahmen. Ebenso stellt sie die Funktionsweise von Statistical Packet Inspection dar und erörtert ebenfalls Schutzmaßnahmen dagegen. Dabei behandelt sie die Änderung statistischer Eigenschaften der Datenpakete und die Erkennung von Paketdiskriminierung. Als Letztes behandelt sie den rechtlichen Schutz gegen Packet Inspection.

Die Autorin kommt dabei zu dem Ergebnis, dass es letztlich keinen Schutz gegen Angriffe auf die Kommunikation durch Packet Inspection gibt. Kann man sich gegen Angriffe mit Deep Packet Inspection noch durch Verschlüsselung des Inhalts schützen, sind gegen statistische Analysen auch Verschlüsselungs- und Verschleierungsmechanismen weitgehend machtlos. Die Eigenschaft der Protokolle, Verbindungen nach bestimmten Mustern auf- und abzubauen, und die Bedingung, möglichst effizient zu kodieren, sorgt für genug Information, um bestimmte Standardprotokolle auch verschlüsselt noch identifizieren zu können.

Auch juristisch besteht wenig Schutz: Bei personenbezogenen Daten greift zwar der Datenschutz – ob er technisch durchsetzbar ist, ist aber fraglich. Auch das Telekommunikationsgesetz hilft hier nicht weiter: Verkehrsdaten können aufgrund der Protokolleigenschaften erhoben werden; eine staatliche Analyse bestimmter Datenpakete erfolgt bereits heute. Damit scheitert auch hier der rechtliche Schutz an der technischen Realität. Die Leistungsfähigkeit der zur Überwachung eingesetzten Technik ist heute ausreichend, um den anfallenden Datenverkehr an den Netzknoten – wie beispielsweise DE-CIX in Frankfurt am Main – zu analysieren. Darüber hinaus wurde mit dem Internet die Hemmschwelle zur Überwachung deutlich gesenkt.

Dass die Skepsis, die in der Arbeit zum Ausdruck kommt, mehr als begründet ist, zeigen nicht nur die bereits erwähnten Überwachungsprogramme.

Als Konsequenz fordert die Autorin dazu auf, angesichts der Universalität des Internet unsere bisherigen rechtlichen Vorstellungen zu überdenken. Aus technischer Sicht sollten Verfahren entwickelt werden, die technische Prozesse auch für Laien sichtbar machen, und es sind weitere Schutzmaßnahmen erforderlich, um Nutzerinnen und Nutzer gegen Angriffe zu schützen. In der Politik, bei Juristen und bei weiteren Entscheidungsträgern ist Aufklärungsarbeit notwendig, um die Problematik der Überwachung und der dabei eingesetzten Methoden deutlich zu machen.

Laudator Stefan Hügel mit der Preisträgerin Agata Królikowski

Die Arbeit verbindet ein Thema der Informatik – Analyse der Datenübertragung im Internet – mit dem juristischen Thema Datenschutz. Die Autorin leistet damit einen Beitrag zum Schutz der unbeobachteten Kommunikation, also des verfassungsrechtlich garantierten Fernmeldegeheimnisses. Sie demonstriert dabei eindrucksvoll die erforderliche Verbindung von Technik und Datenschutz. Datenschutz im Telemedien- und Telekommunikationsbereich wird im jeweiligen Anwendungsbereich unter rechtlichen und sicherheitstechnischen Aspekten geprüft. Die Autorin zeigt die spezifischen Gefahren der räumlich distanzierten Kommunikation für Nutzerinnen und Nutzer auf, und bietet Problemlösungen an. Mit diesem Ansatz zeigt sie, wie ein rechtlicher Schutz gegen die Packet Inspection technisch verwirklicht werden könnte, wenn die Nutzer ihre Rechte auch deutlich erkennen und einordnen könnten.

Wünschenswert wäre gewesen, Grundannahmen stärker herauszuarbeiten – beispielsweise die angenommene Irrelevanz des Inhalts, wenn man weiß, zwischen wem die Kommunikation stattfindet, oder die Bedeutung des Umstands, dass Provider die Verschleierung von Nachrichten durch Kommunikationsteilnehmer bemerken. Auch hätte die Analyse und Auswirkung des *neuen* Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, das das Bundesverfassungsgericht 2008 aus dem allgemeinen Persönlichkeitsrecht geschöpft hat, eine vertiefte Grundierung der Fragestellung bringen können. An der Preiswürdigkeit der Arbeit ändert das jedoch nichts.

Die Arbeit bringt ein technisches Thema, das gleichwohl für den Datenschutz wesentlich ist, deutlich zum Ausdruck und berührt damit Fragen der Stabilität und Pluralität der Gesellschaft. Sie zeugt von einer hohen Sensibilität für besondere Persönlichkeitsgefährdungen durch neue informationstechnische Systeme. Aus diesem Grund hat sich die Jury des *FIfF-Studienpreises* einhellig für die Auszeichnung der Arbeit entschieden.

Herzlichen Glückwunsch, Agata Królikowski, zum zweiten Preis des *FIfF-Studienpreises* 2013.

CC BY

Julia Hofmann: *Zweckgebundener Datenbrief für das Identitätsmanagement-System mittels Web-basiertem Benutzerinterface*

Unser dritter Preis ist insofern ungewöhnlich, als er an eine Fachinformatikerin/Fachrichtung Anwendungsentwicklung (IHK) für eine Abschlussarbeit geht, die eine Dokumentation eines Software-Entwicklungsprojekts darstellt. Es handelt sich dabei um eine Projektdokumentation, die als Qualifikationsarbeit für die Ausbildung als Fachinformatikerin an der Industrie- und Handelskammer Darmstadt entstanden ist. Die entstandene Software ist nutzbar am Hochschulrechenzentrum (HRZ) der TU Darmstadt, wo Julia Hofmann jetzt im Angestelltenverhältnis arbeitet. Dafür hat sie einen Datenbrief entwickelt, der es Angehörigen der TU Darmstadt erlauben soll, sich über ein Benutzerinterface selbstständig zu informieren, welche personenbezogenen Daten für welchen Zweck im Hochschulrechenzentrum verarbeitet werden.

In nahezu allen Verwaltungsprozessen werden heute personenbezogene Daten verarbeitet. Dabei ist es ein Desiderat, dass die betroffenen Personen Kenntnis über Art und Zwecke solcher Verarbeitung erhalten sollen, ja mehr noch, dass ein Bewusstsein und der Wunsch dafür entwickelt werden sollen, sich über diese Zwecke und die Art und Weise des Schutzes ihrer Privatheit zu informieren.

Der zweckgebundene Datenbrief ist eine Web-basierte Anwendung, mit der sich die TU-Angehörigen in sehr einfacher Weise informieren können, wozu ihre Daten im Identitätsmanagement der TU Darmstadt benutzt werden. An jedem Ort und zu jeder Zeit ist es damit möglich, die eigenen Daten über einen gängigen Browser abzurufen. Der Datenbrief wird über den Daten des Identitätsmanagement-Systems (IdM-System) erzeugt und ist unmittelbar abrufbar. Keine weitere Kommunikation und kein besonderer Schriftwechsel sind von Nöten, womit ja häufig, und nicht nur im wirtschaftlichen Umfeld die Realisierung solcher Auskunftspflichten abgelehnt wird. Hierdurch wird das bisherige umständliche Verfahren überflüssig, bei dem das Hochschulrechenzentrum wiederholt persönlich aufgesucht werden musste, um diese Informationen zu bekommen. Ein weiteres Ziel der Arbeit war, dass dadurch auch Verwaltungsprozesse offengelegt und auch transparent gemacht werden. Anforderungen an ein Web-basiertes Benutzerinterface im Identitätsmanagement-System, um einen geregelten und geschützten Zugriff zu garantieren, sind nicht durch Standard-Software zu lösen. Mit ihrer Implementierung hat Julia Hofmann gezeigt, dass solche Auskünfte mit nicht gerade unmenschlichem Aufwand der Implementierung und geringem Aufwand der Auskunft Suchenden durchaus möglich sind.

Es gibt so einen Datenbrief bisher an keiner deutschen Universität. An der Uni Jena gibt es ein ähnliches Projekt, das seit Jahren ohne Ergebnis läuft. Das macht den Datenbrief zu einem Modell- und Vorzeigeprojekt für andere Rechenzentren in Deutschland und weit darüber hinaus für alle Verwaltungsprozesse.

Wie sah und sieht das Identitätsmanagement nun am HRZ der TUD aus? Dort werden ca. 45 000 Benutzer-Accounts von TU-Angehörigen und Kooperationspartnern verwaltet. Bisher war im IdM-System ein einfaches Skript hinterlegt, das bei persönlichem Aufsuchen eines TU-Angehörigen beim HRZ Service gestartet werden konnte. Dabei waren die personenbezogenen Daten des anfragenden TU-Angehörigen im sofortigen Blickfeld der Diensttuenden im HRZ-Service. Zusätzlich mussten die per Skript extrahierten Daten manuell aufbereitet werden, um für technisch weniger versierte Kunden des HRZ-Service verständlich zu sein; d.h. die TU-Angehörigen konnten die Übersicht über ihre Daten selten sofort im Ausdruck mitnehmen, sondern mussten ein zweites Mal kommen. Dieses umständliche Verfahren, das zudem noch durch besonders vertrauensvolle Personen durchgeführt werden musste, ist durch den zweckgebundenen Datenbrief im Web-basierten Benutzerinterface im IdM-System vollständig abgelöst.

Britta Schinzel überreicht Julia Hofmann den Studienpreis

Die Betreuerin Julia Stoll schreibt: „Der Datenbrief ist durch ein Login mit TU-ID (Benutzerkennung) und geteiltem Geheimnis geschützt. Der durch das HRZ standardisierte Authentifizierungsprozess basiert entweder auf der TU-ID und einem persönlichem Passwort oder auf einer personenbezogenen digitalen Karte (Athene-Karte) mit Zertifikat, das im IdM-System hinterlegt und besonders geschützt ist. Das garantiert ein hohes Maß an Vertraulichkeit. Auch die neueren, mit der Europäischen Datenschutz-Grundverordnung anstehenden Schutzziele, wie Transparenz, Zweckgebundenheit und Intervenierbarkeit, wurden mit dem Datenbrief umgesetzt. Die Einsichtnahme der TU-Angehörigen auf ihre personenbezogenen Daten ist gewährleistet und transparent. Offen gelegt ist die Zuordnung der personenbezogenen Daten zu ihrer Nutzung im Sinn der Zweckgebundenheit, besonders gut zu erkennen im sorgfältig erstellten Navigationsdiagramm. Im Navigationsdiagramm sind die an das IdM-System übermittelten Daten in Funktionsgruppen zusammengefasst. Neben den eigenen Daten zur Identifikation sind je nach Zielgruppe – Studierende, Beschäftigte oder Kooperationspartner – Studiendaten, Dienst- oder Unternehmensangaben einzusehen. Allen TU-Angehörigen sind per-

sonenspezifisch ihre Mail-Daten und ihre Notfallangaben zugänglich, die z. B. zu einer Passwort-Wiederherstellung genutzt werden können. Der Rückbezug auf einzelne IT-Systeme in einer heterogenen IT-Infrastruktur wird von Julia Hofmann in origineller Weise geschickt umgangen. Denn parallel einsehbare Dienstvereinbarungen und/oder Verfahrensverzeichnisse erlauben eine Zusammenfassung der hierin wohldefinierten Schnittstellen. Das IdM-System dient überdies der Datenaggregation und -konsolidierung personenbezogener Daten aus der Personal- und Studienverwaltung und im Weiteren der Datenversorgung und -entsorgung an angeschlossene Zielsysteme, die in einer heterogenen IT-Infrastruktur gerade zu verbergen sind. Deshalb ist der zweckgebundene Datenbrief ein integraler Bestandteil des Benutzerinterface des IdM-Systems, mit dessen Hilfe personenbezogene Daten in ihrer Gesamtheit zu überblicken sind. Zudem ist mit ihm für die TU-Angehörigen eine Möglichkeit geschaffen, beim HRZ-Service zu intervenieren, wenn personenbezogene Daten inkorrekt gespeichert sind oder nicht übereinstimmen mit dem was die TU-Angehörigen erwarten. Der gesamte dargestellte verwaltungstechnische Prozess orientiert sich sehr deutlich an den Interessen und Belangen der TU-Angehörigen."

Die Arbeit *Zweckgebundener Datenbrief für das Identitätsmanagementsystem mittels Web-basiertem Benutzerinterface* hatte den Rahmen eines Projekts, in dem zunächst eine Machbarkeitsstudie hinsichtlich der rechtlichen Aspekte, der Schutzziele, und der organisatorischen und wirtschaftlichen Machbarkeit durchgeführt wurde. Es folgte die Projektplanung mit dem Ablauf, wofür Personal- und Sachmittel kalkuliert werden mussten und eine Kosten-/Nutzen-Abschätzung nötig war. Durchgeführt wurde das Projekt dann mit den Phasen Analyse, Design und schließlich der programmtechnischen Realisierung. Als Ergebnis liegt nun der Datenbrief für die Einsichtnahme durch TU-Angehörige auf ihre personenbezogenen Daten vor, womit auch die Zuordnung der Daten zu ihrer Nutzung transparent wird. Der Dienst kann zu jeder Zeit an jedem Ort in Anspruch genommen werden. Für Rückfragen und Interventionen beim Service wurde ein E-Mail-Dienst etabliert. Die Umsetzung der Vertraulichkeit erfolgt durch den Zugriff auf die Daten erst nach dem Login mit der TU-ID und dem Passwort.

Von uns zu beurteilen ist nun die Dokumentation, die das Softwareprojekt begleitet. Frau Hofmann befasst sich zunächst mit der Kundensicht auf einen solchen Datenbrief als Dienst im HRZ, nimmt die projektspezifischen Schnittstellen auf und stellt die Systemarchitektur des IdM-Systems als zentrales System zur gesicherten Datenhaltung vor, in das nun die Web-Anwendung Datenbrief so integriert ist, dass nicht mehr auf mehrere Quellsysteme einzeln zugegriffen werden muss, da die Weitergabe an angeschlossene Zielsysteme automatisiert wurde. Mit der digitalen Identität stehen ein Authentifizierungsmechanismus und diverse Autorisierungsmechanismen bereit. Der Datenbrief stellt dar, wie Zweck (i. e. Identifikation, Zuordnung von Nutzerkreisen in Abhängigkeit von Zugehörigkeiten und deren Tätigkeiten) und eigene Daten zusammengehören. Ein guter Teil der Arbeit ist den rechtlichen Aspekten mit den Schutzzielen gewidmet. Die genannten Planungsschritte, Machbarkeitsanalysen, Modellierung und Implementierung sind genau beschrieben.

Diese Abschlussarbeit ist ihrer Schwierigkeit und ihrem inhaltlichen Wert nach einer Bachelor-Arbeit mindestens gleichwertig. Der Datenbrief ist, wie schon gesagt, neuartig für deutsche Hochschulrechenzentren und angesichts der bekannt gewordenen weit reichenden Sicherheitslücken hochaktuell. Die vollständige Realisierung der Datenschutz-, Transparenz- und Informationsziele gemäß Bundesdatenschutzgesetz hat über Hochschulrechenzentren hinaus Modellcharakter für alle möglichen kommerziellen und institutionellen Verwaltungssysteme, gegen die meist geäußerte Ausrede, dass solche Auskünfte aus wirtschaftlichen oder technischen Gründen nicht möglich seien. Die Lösung der Aufgabe, den zweckgebundenen Datenbrief Web-basiert zu modellieren und zu implementieren zeigt, wieweit sich Julia Hofmann – im Rahmen ihrer Ausbildung zur Fachinformatikerin/Anwendungsentwicklung – auf die Fragen und komplizierten Zusammenhänge im Bereich des technischen Datenschutzes einlassen konnte. Denn neben der im Bundesdatenschutzgesetz geforderten unentgeltlichen Auskunftspflicht in §34 sind Designansätze verwirklicht, die sich aus den diversen Schutzzielen ergeben. Der Datenbrief hält sich also an die rechtlichen Vorgaben und modelliert auf kompetente Weise kontingente individuelle Anforderungen, Nutzungsmöglichkeiten kenntlich zu machen und die Privatheit an der TU Darmstadt zu schützen. Die Betreuerin der Arbeit, Julia Stoll, bemerkt, dass die Arbeit aus technischer Sicht dem *state of the art* entspricht: Mit dem Java-basierten Spring-Framework sind dynamische Web-Seiten durch Spring-Web-Flow erzeugbar und mit Spring-Security und Spring-LDAP kann ein geschützter Zugriff garantiert werden. Der Quellcode kann eingesehen werden. Die Betreuerin bewundert die Programmierleistung von Julia Hofmann, die in einem Model-View-Controller die Datenhaltung des IdM-Systems (als Modell) eingebunden hat, über die Views zweckspezifische Web-Seiten erzeugt und mehrere Controller konfiguriert hat, die die oben genannten Sicherheitsmechanismen berücksichtigen. Somit sind die im Rahmen einer Abschlussarbeit mögliche Kreativität und Originalität mehr als gegeben.

Die Arbeit ist inhaltlich vollständig und sowohl in informatischer wie in rechtlicher Hinsicht korrekt, die Literatur ist hinreichend berücksichtigt, und die Implementierung vollständig gelungen, sodass das System bereits fehlerfrei laufen kann. Ein Glossar rundet den Text ab.

Mit der Berücksichtigung gesellschaftlicher und aller gesetzlich vorgeschriebenen rechtlichen Anforderungen, sowie unmittelbaren Nutzbarkeit (und Nutzung) des Datenbriefs für alle Mitglieder der TU enthält die Arbeit auch die Aspekte von *Informatik und Gesellschaft* für eine Identifikation mit den Zielen des FIfF. Zudem hat dieses System Modellcharakter für ein automatisiertes Auskunftssystem über Datenhaltung und Privatheit für alle möglichen Informationssysteme und weist so über die engere Arbeit hinaus.

Wir vergeben Julia Hofmann für diese ungewöhnliche Leistung den dritten FIfF-Studienpreis und gratulieren ihr sehr herzlich dazu.

Britta Schinzel – Laudatio für den Sonderpreis

Helge Peters: *Biopolitical Simulations: Governing Life in FuturICT*

Mit dieser Auszeichnung bepreisen wir eine Arbeit, die zwar nicht im Zentrum informatischer Methodik und Entwicklung steht – daher der Sonderpreis – sondern eher im kultur- und medienwissenschaftlichen Bereich angesiedelt ist, die sich aber mit kulturwissenschaftlichen Methoden einem interdisziplinären IT-Projekt kritisch zuwendet, das informatische Methoden verwenden und die IT-Entwicklung im Bereich sozialer und ökonomischer Systeme vorantreiben soll. Herrn Peters' Arbeit hat uns auf das von 2007 bis 2013 von der EU geförderte Projekt-Proposal *FuturICT* aufmerksam gemacht. Es beschäftigte bisher Hunderte von europäischen Wissenschaftlern und steht jetzt im Rennen für weitere 10 Jahre Förderung über eine Billion € als Flagship-Projekt unter 7 riesigen Projektanträgen unter der Ausschreibung *Moving the ICT Frontiers – a strategy for research on future and emerging technologies in Europe* – Entscheidung vermutlich November 2013.

Ziele und Nebenwirkungen dieses EU-Projekts müssen uns als FIfF interessieren, wie übrigens auch einige der anderen Proposals (wie *Guardian Angels for a Smarter Planet*, ITFoM – *The IT Future of Medicine* und CA-RoboCom – *Coordination Action for the Design and Description of the FET Flagship Candidate Robot Companions for Citizens*[1]). Ich gehe zunächst auf dieses Projekt-Proposal FuturICT ein, um mich danach Herrn Peters' Arbeit zu widmen.

Das Projekt geht von der ETH Zürich aus und es ist EU-weit international zwischen Sozialwissenschaften, Komplexitätswissenschaften und Informationstechnik angesiedelt. Es verspricht enorme Ansprüche zu erfüllen. Das reicht vom globalen Untersuchen, Verstehen und Managen der gesamten Welt, Natur und der Menschen, über das Design adaptiver, sozial interaktiver, robuster und vertrauenswürdiger Technik durch Integration sozialwissenschaftlicher und komplexitätswissenschaftlicher Methoden und Erkenntnisse bis zur Entwicklung selbstorganisierender ICT und einer neuen Wissenschaft mit dem Ziel einer Co-Evolution von ICT und Gesellschaft. Der Nutzen wird darin gesehen, dass mit dem universalen Blick auf Komplexitäten und Interaktivität mittels ICT frühere Fehler, Krisen und unerwünschte Effekte vermieden werden könnten. Die Autoren begründen die Notwendigkeit eines solchen europäischen Langzeitprojekts aus ihrer Vorstellung einer Welt außer Kontrolle (Beispiel Finanzkrise, Griechenland, ökologische Katastrophen), die durch Wissenschaft und Technik gebändigt werden müsse.

Es ist klar, dass ein solch hypertrophes Projekt einer techno-integrierenden Universalwissenschaft, das sich explizit *God's eye view* anmaßt, unmittelbar Skepsis und Widerspruch hervorruft. GenderforscherInnen springt der misogyne Impetus der Kontrolle und Fesselung von Leben unmittelbar ins Auge. „Leben" wird hier als integriertes reales und virtuelles Leben begriffen, wobei nach Auffassung der Zürcher Autoren *Helbing* und *Balietti* die elektronischen IT-Gebäude dringend auf Füllung mit solchem „Leben" warten (*it is obvious that virtual threedimensional worlds are waiting to be filled with life*). Damit wird Leben als steuerbares Wissens-Objekt (seiner Funktionalität, nicht seiner äußeren Erscheinung) behandelt, was im Weiteren zur Autorisierung der sich selbst organisierenden Produktion von wissenschaftlichen und virtuellen Tatsachen verwendet werden soll. Die Hybris ist nicht zu überbieten – die Autoren glauben, ihre Simulationen erfassten nichts weniger als *life on earth and everything it relates to*, in einer umfangreichen Bedeutung als biologisches und soziales klassisch materielles und künstliches, von Materie unabhängiges Leben.

Helge Peters

Es sind durchaus ältere Visionen, Phantasmen und Paradigmen, die sich hier zu einem angeblichen Neuansatz amalgamieren, wie Kybernetik, Interaktivität und die Selbstorganisation emergenter Systeme, Künstliche Intelligenz und Künstliches Leben (AL). Auch der soziologische, systemtheoretische Ansatz ist keineswegs neu, sondern wurde in Biologie, Mathematik und Informatik seit den 80er Jahren verfolgt. Neu sind allerdings – von den Autoren unverschuldet – die inzwischen entwickelten neuen Möglichkeiten der Prozessierung ungeheurer Datenmengen, der Big-Data-Analyse, des Data-Mining und der Überwachungstechnologien, welche in dem integrierten Ansatz benutzt werden sollen. Neu ist auch der verwegene Anspruch, über Simulationstechniken des von ihnen allumfassend gemeinten Biologischen, soziotechnische Entwicklungen vorhersagen und steuern und so Krisen vermeiden zu können. Die Antragsteller wollen sich der *Big Data* der großen IT-Firmen bedienen (können) und dennoch natürlich auch die rechtlichen Anforderungen an Privatheit und Datenschutz berücksichtigen. Dies soll laut einer neuen Publikation eines der Autoren des Projekts, *D. Helbing*, anlässlich der letzten von der EU bezahlten Future-ICT-Tagung im Juli 2013 nicht durch Überwachung, sondern durch vertrauenswürdige, sich selbst regulierende IT-Architekturen gelingen. Wie solche vertrauenswürdigen Architekturen aussehen könnten, wird nicht genannt. Allerdings gibt es auch aus der beteiligten Community der Komplexitätswissenschaften Zweifel an den Wahrheitsansprüchen des Projekts, und ein Beteiligter schlägt vor, die Effektivität der Modellbildung zu evaluieren und die Grenzen der Wissensbildung zu explizieren. Dagegen kommt gleich aus der gleichen Community der Anspruch der Wissenschaft der Komplexität auf eine Omniscience, die angetreten ist, die Lösung für ethisch-politische Probleme zu bieten.

Wir alle wissen, dass solche absurden und in jeder Hinsicht problematischen Ziele unerreichbar sind, und wahrscheinlich wissen das die Antragsteller, wenn sie nicht so berauscht sind von ihrer Idee wie die Videos nahe legen. Und sicher wissen das die Gutachtenden auch, was aber nicht heißt, dass das Projekt nicht gefördert werden wird. Nach dem Motto, mal sehen was herauskommt, wie dies schon im amerikanischen SDI-Programm gemacht wurde, weshalb David Parnas, einer unserer Geehrten, ausstieg. Und was dann also auch nicht heißt, dass das Projekt nicht schädliche Wirkungen z. B. auf unsere Sprache und Vorstellungswelt, auf die beteiligten Fächer, auf Entwicklungen und Überwachung haben würde.

Herr Peters' Arbeit bedient sich der Methodologien der *Science and Technology Studies* und der *feministischen Technikkritik*. Er untersucht auf der Grundlage des Konzepts von Biopolitik und Biomacht von *Michel Foucault* und anderen, wie sich die Betrachtung des Lebens als abstraktes Wissensobjekt und als Objekt von und für Governance im Projekt FuturICT auswirkt, und welche Konsequenzen das hat. Im Kontext der Projektdarstellungen von FuturICT führt ihn das zur Analyse eines Szenarios biologisierter Medien, mediatisierter Biologie und digitalisierter Bevölkerung, in dem Leben berechenbar gemacht und die Natur durch objektives Wissen beherrscht werden soll. Damit werden neue Grenzen zwischen Natur und Gesellschaft gezogen, wobei vielmehr die biologische Evolution die gesamten gesellschaftlichen Entwicklungen einhüllt. Die Simulation sozialer Strukturen und die konstruktiven Techniken gesteuerter Selbstorganisation, die in FuturICT eingesetzt werden sollen, rufen ein spezielles konstruiertes Wissen hervor, das als angeblich biologisch essentialisiert und naturalisiert wird, wodurch es der Beherrschung von Menschen dienen kann, weil es ja angeblich einer natürlichen Evolution unterworfen ist. Das legt die Annahme einer prospektiven Form der Biopolitik nahe, bei der Leben in weitaus größerem Ausmaß instrumentalisiert werden kann und soll als dies bisher mit Reproduktionstechnologie, Gewebe-Engineering, Neuroenhancement etc. bereits geschieht.

Die FuturICT-Autoren schlagen ein Biomimetisches Government vor, das sich insbesondere mit Nichtlinearität, der aus der Mathematik herrührenden Katastrophentheorie, später in den Naturwissenschaften Chaostheorie genannt, beschäftigt. Es würde Biomacht in den dort vorgeschlagenen Simulationen und Modellierungen und deren emergierenden Effekten erstellen, sich seine Legitimität aus deren Naturalisierung als Leben holen, und aus der Instrumentalisierung solchen Lebens die Autorisierung der Ermächtigung. Da die technologische Rationalität ohne Reflexion der historisch ausgebildeten sozialen Verhältnisse und deren Veränderlichkeiten zum Tragen kommen soll, würde solches Vorgehen gerade die globalen Probleme hervorrufen, die es zu lösen verspricht.

Eine konstruktive Wendung erfährt Herrn Peters' Analyse über der Genderforscherinnen *Donna Haraway* und *Lucy Suchman's* Forderung, die ja immer situierten wissenschaftlich-technischen Praktiken explizit zu machen und auch die scheinbare Transparenz der Visualisierungen zu dekonstruieren, ihre Kontingenz darzustellen. Somit sollte der Trick, als *Gods eye view* von nirgendwo her zu sehen, ersetzt werden durch *views from somewhere*, womit die Subjektposition des Zeugen (Donna Haraway's *modest witness*) in den Akten der wissenschaftlichen Bezeugung notwendigerweise perspektivischer und partieller Wissensproduktion zurückgeholt wird. Der politische Akt, der in der Wahl der Modelle und der künstlichen Agenten und der Wahl bzw. Verfügbarkeit der Verhaltensdaten besteht, folgt einer dominanten Logik, die dazu tendiert, bestehende Verhältnisse zu stabilisieren, und muss daher begründet und relativiert werden. Statt mit der Rhetorik von Emergenz und Evolution die Wege zu Veränderungen verschließen, müssen verkörperte Subjektivität und historische Kontingenz aufgezeigt werden und damit Wege zu Differenz und Transformation geöffnet werden. Im Folgenden zeigt Peters in den von FuturICT präsentierten Videos den westlich zentrierten vergeschlechtlichten *Bias* auf, der sich in den präsentierten Personen darstellt, und ihre Angst, dass menschliches Überleben auf der technisch durchdrungenen und verknüpften Erde, die „außer Kontrolle gerate" unmöglich werden könnte, wenn nicht Komplexität und Risiken durch technologische Mittel in Schach gehalten würden. Die unregierbare wilde Natur, also die entfesselte Komplexität, zu bändigen, sei moralische Verpflichtung der objektiven Wissenschaft und Technologie. Mit Haraway aber ist die Situierung des wissenden Subjekts in seiner Umgebung – gekoppelt mit seinem Untersuchungsobjekt – das, was situiertes Wissen hervorbringt, welches keiner Sicherheitstechnologie bedarf und nicht instrumentalisiert wird zur Stabilisierung von Biomacht.

Angloamerikanischer Tradition folgend, hat die Arbeit die Form einer Erzählung, bei der Zitate der FuturICT-Selbstdarstellungen und Äußerungen der Projektbeteiligten den passend ausgewählten Zitaten der genannten Literatur gegenübergestellt werden. Der Eigenbeitrag besteht in der Adaption der für ein Jahrhundert früher entwickelten Kritik an der damaligen Biopolitik und der jüngeren feministischen Technikkritik an die Projektsprache und -ideen. Die so entstehende Analyse wird kompetent, angemessen und akribisch genau entwickelt.

Aus der so entwickelten Argumentation ergeben sich zwar unmittelbar Zurückweisungen mit Bezug auf mögliche Veränderungen der Vorstellungen von Menschen über die Natur, das Leben und sich selbst, und als Folge die vorauszusehende Schaffung von Akzeptanz von Machtverschiebungen unter solcher Art von Biopolitik.

Auch stellt Peters richtig fest, dass die Naturalisierung des Sozialen als komplexes lebendes System die Möglichkeit dazu verschließt, politische Streitfragen zu behandeln und gegebene Ordnungen über solche der Transformation zu privilegieren.

Im Hinblick auf die Informatik und die Anliegen des FIfF aber fehlt der Peters'schen Arbeit die Kritik an der Durchführbarkeit der Ansätze von FutureICT und mehr noch eine Technikfolgenabschätzung der erwartbaren Forschungsprozesse und -ergebnisse, die sich auf maßlose Kontroll- und Überwachungswünsche, Konflikte derselben mit europäischen Datenschutzrichtlinien und partielle Durchsetzung hinauslaufen dürften. Es ist, ähnlich wie das amerikanische SDI-Programm 1985 zur feindlichen Raketenabwehr, ein von vorneherein zum Scheitern verurteiltes, aber mit den machbaren Anteilen äußerst schädliches Projekt. Die Einsicht, wie primitiv evolutionäre informatische Systeme, also beispielsweise evolutionäre Algorithmen vor-

gehen, wäre Voraussetzung für eine fundamentale Kritik an den Projektideen. Dass Big-Data- und Data-Mining-Technologien dank statistischer und heuristischer algorithmischer Methoden ungeheure Analysekapazitäten zur Exploration und Kontrolle von Bürgern haben, bedeutet nicht, dass diese angemessen konstruktiv umgesetzt werden könnten, dass die formalen Modelle von Leben auch nur im Kleinsten annähernd Leben und Soziales abbilden könnten; das ja schon allein deshalb nicht, weil die Eigenschaften von Leben in einem umfassenden Sinn nicht bekannt sind. Das Loslassen evolutionärer Methoden oder zellulärer Automaten oder von konnektionistischen Systemen ist so ungeheuer kontingent, dass Projektionen auf die Zukunft in größerem Ausmaß vollkommen unmöglich erscheinen. Aber auch politisch ist das Projekt höchst bedenklich, denn u. a. legitimiert es Wünsche, wenn nicht Aktivitäten von Politikern, z. B. Innenminister Friedrich, zur Etablierung total überwachender Systeme analog denen der NSA, indem es die wissenschaftliche Notwendigkeit der Gewinnung von Big Data begründet. Zudem würde der Ankauf von Daten bei Google, Microsoft, Apple etc. vermutlich die Billion € Forschungsmittel bereits verschlingen. Oder stellen sich die Antragsteller vor, die Daten der Geheimdienste oder von Eurohawks anzapfen zu können?

Wäre es nicht viel sinnvoller, wenn die EU die Entwicklung unabhängiger Netze, Systeme oder Systemkomponenten, sozialer Netzwerksysteme oder auch kommerzieller Dienste fördern würde?

So scheint es uns wichtig, Herrn Peters zu einer Zusammenarbeit zu gewinnen, v.a. für den Fall der Förderung des FuturICT für eine transdisziplinäre FuturICT-Technikfolgenabschätzung, um analog zu unseren kritischen Aktivitäten im Kontext des EU-Projekts INDECT tätig zu werden.

Wir geben Herrn Peters für seine Arbeit den (unüblichen und daher ideell besonders wertvollen) Sonderpreis, gratulieren sehr herzlich und hoffen auf fruchtbare Kooperation.

Anmerkung

1 vgl. http://cordis.europa.eu/fp7/ict/programme/fet/flagship/roadmap_en.html

CC BY

Rainer Rehak, Constanze Kurz

Des FIfFs Kern: die kritische Informatik

Replik zur Replik des Kommentars zum dritten Platz des FIfF-Studienpreises 2012

Dieser Text ist die gewünschte Weiterführung einer Diskussion um die Studienpreisvergabe im letzten Jahr.[1] Dabei soll unsere Hartnäckigkeit, eine Antwort auf die Replik der Jury in der FIfF-Kommunikation 1/2013 zu formulieren, weniger als Angriff auf die damals ausgezeichnete Arbeit Liquid Democracy *verstanden werden, sondern eher als Frage und Hinweis auf die Grundmotivation der Studienpreisvergabe und somit auch Ergründung bzw. Schärfung der inhaltlichen Ausrichtung des FIfF selbst.*

Unserer Ansicht nach hat sich die Debatte nicht an einem Satz der Laudatio entzündet, sondern an der Einschätzung und Einordnung der Arbeit durch die Jury insgesamt. Kern unserer Kritik ist die Auszeichnung einer Arbeit, die durch Nichtbeachtung elementarer Wahlgrundsätze beim Design von digitalen Wahlsystemen gekennzeichnet ist. Diese Herangehensweise ist nicht einmal rein technisch betrachtet richtig, denn der Entwurf technischer Systeme richtet sich nach seinen Anforderungen, seinem Verwendungskontext. Gerade in diesem Fall sind diese Anforderungen ganz klar durch die gesellschaftliche Rolle gegeben, die dieses System übernehmen soll: demokratische Wahlen nach den anerkannten Wahlgrundsätzen zu ermöglichen. Die Arbeit hat eben nicht die generelle „Bürgerbeteiligung am Demokratischen Entscheidungsfindungsprozess" zum Thema, auch wenn das der Liquid-Democracy-Ansatz ist. Die Crux der Arbeit besteht ja gerade im Umbau des Kommunikationswerkzeuges *Adhocracy* in ein demokratisch zulässiges Wahlsystem.

Wie sollten das Wahlgesetz und die Vorgaben aus Karlsruhe für ein digitales Wahlsystem jedoch nur „begleitenden Charakter" haben – so wie in der Replik der Jury behauptet? Was bliebe da als Anforderung überhaupt noch übrig? Sicherlich einige technisch interessante Aspekte, die jedoch in unserem Sinne nur Elfenbeinturm-Charakter haben können, denn sozial-gesellschaftliche Spezifikationen können und dürfen nicht nur „begleitenden Charakter" für ein solches technisches System haben. Die Wahlgrundsätze wurden ja gerade formuliert, um Abwägen und Auswählen zu können, welche technischen und organisatorischen Mittel wir für demokratische Wahlen einsetzen wollen und können. Dies zu verkennen ist in unseren Augen eine Fehleinschätzung, die den FIfF-Grundsätzen direkt entgegensteht.

Folglich gibt es bei der Arbeit von Angel Tchorbadjiiski unserer Meinung nach zwei FIfF-Interpretations- und Bewertungssichten:

Constanze Kurz und Rainer Rehak

Dr. **Constanze Kurz,** Informatikerin, Sprecherin des Chaos Computer Club und Mitglied im Beirat des FIfF.
Rainer Rehak, Informatiker, Preisträger des FIfF-Studienpreises 2012.

1. Entweder es handelt sich um eine technische Arbeit, die sich einige Spezifikationen aus den insgesamt komplexeren gesellschaftlichen Anforderungen herausgesucht und daraus ein System entwickelt hat, die aber nur Erkenntnisse und Aussagen über diesen begrenzten technischen Bereich erlaubt. Diese Arbeit wäre sicherlich technisch interessant, für das FIfF aber wenig relevant, ja sogar elementar kritikwürdig, weil derartige Systeme immense gesellschaftliche Implikationen haben können, die natürlich kritisch hätten analysiert werden müssen.

2. Oder aber die Arbeit will explizit alle gesellschaftlichen Anforderungen mit einbeziehen und die Thematik im technischen sowie nichttechnischen Kontext behandeln, so wie es das FIfF für die Informatik insgesamt fordert. Dann wäre die Arbeit für die Ziele des FIfF hochrelevant. Folglich hätten aber das deutsche Wahlrecht, verwandte Regelungen und insbesondere das Urteil des Bundesverfassungsgerichtes zu Wahlcomputern in der Arbeit eine angemessene Rolle spielen müssen.

Während ihr expliziter Einbezug der Wahlgesetze und ihre scheinbare gesellschaftliche Ausrichtung die Arbeit also in den Fokus des FIfF rücken, konterkariert die beiläufig-unvollständige und gänzlich unkritische Betrachtung dieser Zusammenhänge quasi im Vorbeistolpern eines der Kernziele des FIfF: die gesellschaftliche Verantwortung und kritischen Fähigkeiten der Informatiker in den Vordergrund zu rücken und durch Auszeichnung zu fördern. Aber viel schlimmer noch, die mehrfache und unmissverständliche „Erkenntnis", das entwickelte System sei für Parlamentswahlen in Deutschland geeignet (S. 26, siehe auch S. 9, 25, 62 und 64), „weist […]" eben nicht „auf die grundsätzliche Problematik hin", sondern stellt sie völlig falsch dar und bewertet sie zudem fatal: Nichttechnikern werden – wie in der Informatik leider so häufig – wieder nur hehre Versprechungen gemacht, die die Technik gar nicht einlösen kann.

Abschließend: Unserer Ansicht nach sollte bei dem Studienpreis des Forums Informatiker und Informatikerinnen für Frieden und gesellschaftliche Verantwortung die kritische Einordnung und Bewertung gesellschaftliche relevanter informationstechnischer Entwicklungen im Vordergrund stehen, nicht nur deren bloße Dokumentation und/oder praktische Fortführung. Die rein technische Analyse informatischer Systeme kann daher gerade nicht Gegenstand der Auszeichnung sein, aber die Einordnung und Bewertung dieser Technologie ist in der Arbeit misslungen. Es gibt keine Vieldeutigkeit oder mögliche Missverständnisse bezüglich der Aussage, man könne das System für parlamentarische Wahlen in Deutschland verwenden. Doch das kann man nicht; gegenteilige Behauptungen nähren ausschließlich die Technikgläubigkeit.

Dieses Jahr geht das FIfF unserer Meinung nach den richtigen Weg, indem es bei der aktuellen Preisvergabe auch selbst Position bezieht, Kritik formuliert und so den konstruktiv-kritischen Diskurs fördert.

Anmerkung

1 *http://fiff.de/publikationen/fiff-kommunikation/fk-2013/fk-2013-1/fk-2013-1-s72*

Marie-Theres Tinnefeld

Das Menschenrecht auf Privatheit und Kommunikation

Nationale und internationale Perspektiven in einer ausgespähten Gesellschaft

I Die Entsicherung des Datenschutzes

Das Erschrecken über die weitgreifenden Überwachungspraktiken der Geheimdienste wächst dank der Dokumente des Whistleblowers Edward Snowden. Sie klären darüber auf, dass die Dienste von einer Art „Goldrausch" (Gerhart Baum) erfasst worden sind. Die NSA und die britische Spionage-Agentur *Government Communications Headquarters* (GCHQ) haben Post- und Telekommunikation mit Hilfe von Überwachungssystemen wie PRISM (USA) und Tempora (England) in digitalen Netzwerken, Glasfaserkabeln (Upstreamsystemen) und Internetknotenpunkten mit der Begründung abgegriffen, dass sie nur auf diese Art und Weise Terroristen in der Informationsflut rechtzeitig aufspüren können.

In Deutschland ist es der Bundesnachrichtendienst (BND), der als Auslandsgeheimdienst auch unter Einsatz des amerikanischen Programms XKeyscore zur Erfassung und Analyse von Internetdatenströmen an der strategischen Fernmeldeüberwachung beteiligt ist. Dabei handelt es sich um eine verdachtslose Telekommunikationsüberwachung, eine Art Rasterfahndung in bestimmten Gefahrenbereichen der Vorfeldaufklärung (z. B. internationale terroristische Anschläge mit unmittelbarem Bezug zu Deutschland), die ausschließlich vom BND durchgeführt wird. Die gesetzlichen Voraussetzungen dazu sind im Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses geregelt (G10).

Mit der Zunahme des Terrorismus wurden in Deutschland die Weichen für eine dauerhafte Überwachung des Post- und Telefonverkehrs durch eine Änderung des Art. 10 GG ermöglicht. Das maßgebliche G10 trat mit Wirkung zum 1. November 1968 in Kraft und ermächtigt die drei Geheimdienste, die Verfassungsschutzbehörden des Bundes und der Länder (BfV und LfV), den Bundesnachrichtendienst (BND) und den Militärischen Abschirmdienst der Bundeswehr (MAD) zur präventiven Abwehr möglicher oder drohender Gefahren für die freiheitlich-demokratische Grundordnung und die Sicherheit der BRD unter Einbeziehung der Sicherheitsinteressen der Allierten. Das G10 wurde in einigen verfassungsrechtlich fraglichen Normen 1978 konsolidiert, insbesondere wurden die Behörden verpflichtet, Betroffene über durchgeführte Überwachungsmaß-

nahmen zu informieren. Der Historiker *Josef Foschepoth* gibt in seinem Werk *Überwachtes Deutschland* (3. Auflage 2013) eine interessante Übersicht über die Entstehung und den Verlauf der Post- und Telefonüberwachung in der alten Bundesrepublik, die vermuten läßt, dass auch nach der Wiedervereinigung noch Überwachungsrechte der Allierten fortbestehen.

Parallel dazu rückte das Thema des belauschten Bürgers in den Fokus einer rechtsstaatlichen Debatte. Damals schrieb der Jurist *Adolf Arndt* am 28. Februar 1977 in der Zeitschrift *Der Spiegel*:

> *„Das Problem des belauschten Bürgers birgt nicht nur den Zweifel, ob der Mensch vor sich bestehen kann, sondern wirft auch die Frage auf, ob Demokratie so noch möglich ist. Denn um Demokratie von der Wurzel her wachsen zu lassen, ist für den Jedermann, der ein ‚Einzelner' ist, Freiheit von Furcht das erste Erfordernis. Der belauschte Bürger ist jedoch der geängstigte Bürger. Er ist der aus dem Dunklen geröntgte Mensch, der von Blicken durchdrungen wird, die er nicht sieht. Sein Staat liegt nicht mehr verlässlich im Hellen."*

Deutlich wurde bereits zu diesem Zeitpunkt, dass die Politik, die den grundrechtlich basierten Rechtsstaat verteidigen sollte, aus eben dieser Aufgabe das Recht ableitete, jenseits des verfassungsrechtlichen Gebots der Verhältnismäßigkeit in Fällen des Terrorismus empfindliche Freiheitseingriffe vorzunehmen. Denn je größer eine Gefahr ist oder gemacht wird, desto berechtigter erscheinen auch solche Eingriffe. Die gebündelten weltweiten Abhörpraktiken im 21. Jahrhundert lassen vermuten, dass die Einschränkungen der Privatheit, insbesondere auch der vertraulichen Kommunikation, nicht mehr in einem angemessenen Verhältnis zum Sicherungszweck stehen.

Die Entwicklung ist umso dramatischer, als etwa das G10 eine Ausnahme zur vollen gerichtlichen Kontrolle (Art. 19 Abs. 4 GG; Art. 10 Abs. 2 GG) enthält. Eine Maßnahme der Nachrichtendienste unterliegt zunächst der Kontrolle der G10-Kommission (§13 G10), die kein Organ der Gerichtsbarkeit ist. Erst dann, wenn sie dem Betroffenen mitgeteilt worden ist, steht diesem der gerichtliche Rechtsschutz offen.

Hier bleibt anzumerken, dass die Rechtsweggarantie untrennbarer Bestandteil der Rechtssicherheit und ein wesentliches Merkmal der Rechtsstaatlichkeit ist, die zum Kernbereich des Grundgesetzes gehört und daher nicht angetastet werden darf (Art. 79 GG).

II Schutz der Privatheit

Die Grund- und Menschenrechte sind in der Zeit der Aufklärung erstmals normiert worden, um die Autonomie des Einzelnen gegen politische Instrumentalisierungen durch den Staat zu verteidigen. Inzwischen ist diese Gefahr aber auch durch Private für die Selbstbestimmung und Kommunikation des Einzelnen so groß geworden, dass er auf staatlichen Schutz angewiesen ist. Die Lücke des Schutzes etwa gegenüber Konzernen und anderen Privaten im deutschen Grundrechtssystem wurde bereits im berühmten *Lüth-Urteil* vom 15. Januar 1958 geschlossen. Das Bundesverfassungsgericht begründete darin die Lehre von der Drittwirkung der Grundrechte und weitete den Schutz des Einzelnen vor Eingriffen des Staates auf den Schutz in Privatrechtsbeziehungen mit „Dritten" aus. Die geplante Datenschutzgrundverordnung der EU erfasst sogar weitgehend öffentliche und private Bereiche in gleicher Weise.

1. Grundrechtliche Gewährleistungen des Persönlichkeitsschutzes in Deutschland

Das Grundgesetz gewährleistet zunächst durch spezielle Grundrechte den Schutz des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG). Dazu gehört u. a. die Unverletzlichkeit der Wohnung (Art. 13 GG) und das Telekommunikationsgeheimnis (Art. 10 GG). Da das verfassungsrechtlich verankerte Persönlichkeitsrecht ein entwicklungsoffenes Auffanggrundrecht ist, hat das Bundesverfassungsgericht aus ihm sowohl das Grundrecht auf Datenschutz (1983) als auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (*IT-Grundrecht*, 2008) geschöpft. Diese Rechte sind international mit dem Schutz von Privatheit und Intimität verbunden. Sie gewährleisten dem Einzelnen ein Recht auf persönliche Freiräume und vertrauliche Kommunikation, sowie ein Mitgestaltungsrecht an ihn betreffenden Informationen. Mit diesem Schutz hat das Bundesverfassungsgericht verfahrensrechtliche Regelungen verbunden (z. B. Transparenz der Datenvorgänge durch Aufklärung, Einrichtung und Beteiligung unabhängiger Datenschutzinstanzen, Datenschutz durch Technik), und damit die Rechte des Betroffenen gestärkt.

2. Regionaler europäischer Schutz der Privatheit und Kommunikation

Der Privatheitsschutz ist primärrechtlich in der EU-Grundrechte-Charta (Art. 7 und Art. 8 EGRC) geregelt. Beide Normen basieren auf der Europäischen Menschenrechtskonvention (Art. 8 EMRK):

> *„(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is nesssary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

Danach ist das Recht auf Privatsphäre einschließlich der Familie und Wohnung und der Korrespondenz bzw. Telekommunikation ein Menschenrecht, das auch im Hinblick auf eine entsprechende personenbezogene Datenverarbeitung zu schützen ist.

Im Vertrag über die Arbeitsweise der EU (Art. 16 Abs. 2 AEUV) sind Gesetzgebungsorgane der EU ermächtigt, Verordnungen oder Richtlinien im Bereich des Datenschutzes zu erlassen, „*die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr*". Zu den aktuellen Fragen gehört, ob Geheimdienste vom supranationalen EU-Recht erfasst werden

und im Rahmen des geplanten Sekundärrechts (Datenschutzgrundverordnung und EU-Richtlinie zur Datenverarbeitung zum Zwecke der Strafverfolgung und der Polizei) normiert werden können.

Der Anwendungsbereich der polizeilichen Zusammenarbeit umfasst jedoch nur dann die Tätigkeit von Geheimdiensten, wenn sie polizeiliche Aufgaben wahrnehmen (Art. 87 Abs. 1 AEUV). In Deutschland besteht grundsätzlich ein Trennungsgebot zwischen Polizei und Nachrichtendiensten, das es in anderen europäischen Ländern so nicht gibt. Allerdings werden auch andere europäische Geheimdienste mit Rücksicht auf ihre Traditionen teilweise aus dem Anwendungsbereich des sekundären Unionsrechts herausgenommen.

Die Trennung von polizeilicher Exekutivgewalt und nachrichtendienstlichen Informationssammlungen in Deutschland sollte auch zukünftig ihren hohen Stellenwert behalten und nicht im Wege des Antiterrorkampfes unter dem Motto „um Schlimmeres zu verhindern" auf der Strecke bleiben. In diesem Zusammenhang sei auch der Europäische Gerichtshof für Menschenrechte aus dem Jahr 1978 im Fall *Klass gegen Deutschland* zitiert, wonach unter dem Gesichtspunkt der Grundrechte *„die Vertragsstaaten nicht im Namen des Kampfes gegen Spionage und Terrorismus zu jedweder Maßnahme greifen dürfen, die ihnen geeignet erscheint"*. Der Gerichtshof hat auch immer wieder betont, dass die Befugnis zur Überwachung des Telekommunikationsverkehrs als Eingriff in das Privatleben und die Korrespondenz bzw. Telekommunikation (Art. 8 EMRK) zu werten sei.

Angesichts der millionenfachen Überwachung von Telefonverbindungen durch die NSA, aber auch durch andere Geheimdienste, erscheint ein internationales Datenschutzabkommen erforderlich, das globale Standards zum Schutz der Telekommunikation und zum Schutz personenbezogener Daten bestimmt, wie sie im Internationalen Pakt über bürgerliche und politische Rechte (IPbpR) angelegt sind. Denn die Verteidigungslinien der Freiheit sind politisch je nach der Gefahrenlage zwar beweglich, die erkämpften Sicherungen menschlicher Freiheit sind aber seit 9/11 weltweit aus dem Ruder gelaufen.

3. Völkerrechtliche Verankerung der Rechte auf Privatheit und Kommunikation

Aus dem Internationalen Pakt über bürgerliche und politische Rechte der Vereinten Nationen sind alle Vertragsparteien, auch die Amerikaner, verpflichtet, das *Right to Privacy* zu schützen. Art. 2 Abs. 1 IPbpR formuliert: *„Each State to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdication the rights recognized in the present Covenant […]."* Und Art. 17 Abs. 1 enthält die Formulierung *„No one shall be subjected to arbitrary or unlawful interference."* Mit anderen Worten, der Staat ist nicht alleiniger Normadressat, auch Private können verpflichtet werden. Jedermann hat zudem Anspruch auf Schutz durch das Recht, wozu auch ein Rechtsweg durch Verfahren gehört.

Die Vertragstaaten sind verantwortlich für den Schutz der Privatheit und Telekommunikation. Dieser Schutz gilt nicht nur im Verhältnis zu den eigenen Bürgern, sondern für Jedermann auch im Verhältnis zu den jeweiligen Geheimdiensten. Danach müssen auch gesetzlich vorgesehene Abhörmaßnahmen verhältnismäßig sein. Sie dürfen sicherheitspolitischen Forderungen nicht untergeordnet werden. Da heißt aber nicht, dass Fragen der globalen Sicherheit unter Einbeziehung des Internet keine wichtige Rolle spielen.

Aufgrund der massiven globalen Spähaktionen von Geheimdiensten wäre es sinnvoll, ein Zusatzprotokoll zu Art. 17 IPbpR anzustreben, um die Tätigkeit der Geheimdienste konkret an die Menschenrechte zu binden, insbesondere an die Achtung der Privatheit in Verbindung mit einem speziellen Schutz der vertraulichen Telekommunikation. Aus Gründen der Datensicherheit wären außerdem weitere Forderungen zu beachten:

1. Der Menschenrechtsschutz sollte bereits in der Technologie selbst angelegt werden;

2. Informationstechnologien sollten von unabhängigen Datenschutzinstanzen auf ihre Vereinbarkeit mit den Menschenrechten geprüft werden, bevor sie auf den Markt kommen.

Eine „Welt ohne Privatheit" ist nicht *„livable"*. *Georges Orwell* hat in seinem Roman *1984* (abgeschlossen 1948 und veröffentlicht 1949) die Vision einer totalitären Welt ohne Privatheit vorgestellt :

„WAR IS PEACE
FREEDOM IS SLAVERY
IGNORANCE IS STRENGTH"
(Propaganda des Wahrheitsministers)

Davis Eggers folgt den Spuren von Orwell und stellt in seinem umstrittenen neuen Roman *The Circle* (erschienen 2013) ebenfalls drei Slogans als Warnung vor dem Verlust des letzten Bereichs von Privatheit vor, die sich nach den Enthüllungen von Snowden abzeichnen:

Marie-Theres Tinnefeld

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

„SHARING IS CARING
SECRETS ARE LIES
PRIVACY IS THEFT"

Die Slogans verweisen zumindest auf eine erschreckende neue Gefährdung der Privatheit, nicht zuletzt auch durch TK-Diensteanbieter. Sie kooperieren teilweise freiwillig mit den Geheimdiensten. Teilweise sind sie aber auch verpflichtet worden, Eingriffe in die private Telekommunikation zuzulassen und zwar im Rahmen der Anordnungen eines eigens für die geheime Kontrolle der Auslandsaufklärung geschaffenen Gerichtshofs, dem *Foreign Intelligence Surveillance Court* (FISC, nach dem ihm zugrundeliegenden Gesetz auch *FISA Court* genannt).

Seit 9/11 erhielten NSA und FBI erweiterte Überwachungskompetenzen. Dazu schrieb *James Bamford* 2008 in seinem Buch *The Shadow Factory*: *„Although the NSA will still have to obtain a FISA order to target Americans, they can now target foreigners outside the country simply by submitting to the court a list of suspected terrorist groups rather than individual names."* US-Bürger im Ausland unterfallen weiter dem Schutz des Gerichts.

Der Gerichtshof hat großen US-Internet- und Telekommunikationsdiensten auferlegt, Millionen von Datensätzen über Telekommunikations-Verkehrsdaten täglich an die NSA und teilweise auch andere US-Nachrichtendienste zu liefern. Im Rahmen des PRISM-Programms soll die NSA aber auch Zugriff auf Kommunikationsinhaltsdaten genommen haben. Bei den von Snowden aufgedeckten Abhörtechniken handelt es sich um Arkanpraktiken der Dienste, die geeignet sind, die individuellen Grundrechtspositionen aus sicherheitspolitischen Gründen oder aber auch aus wirtschaftspolitischen Interessen zu untergraben.

III Fazit

Der Schutz von Privatheit und Telekommunikation ist abhängig von einem wirkkräftigen Datenschutzniveau, das sich weltweit realisieren lässt. Globale Spähaktionen von Geheimdiensten können nur unzureichend im Rahmen eines regionalen Völkerrechts effektiv geregelt werden. Daher wäre ein Zusatzprotokoll im Internationalen Pakt über bürgerliche und politische Rechte wünschenswert. Zudem ist eine Sicherheitsstruktur gefragt, die nicht jeden (unbescholtenen) Bürger unter Terrorismusverdacht stellen kann. Im Kern geht es also um eine Freiheitsarchitektur, die im öffentlichen und privaten Bereich universelle Menschenrechte sichert.

Mit dem Schutz der Privatheit und Telekommunikation sollten folgende Forderungen verbunden werden:

- Ergänzung des völkerrechtlichen gesicherten Grundrechtsschutzes,
- mehr Transparenz nachrichtendienstlicher Tätigkeit,
- Bereitstellung sicherer Verschlüsselungsverfahren als Standard und Normalfall.

Am 22. Oktober 2013 erklärte die Pressestelle des Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) zu den neuen Vorschlägen aus dem Europäischen Parlament u. a.:

> *„Datenübermittlungen an ausländische Behörden und Gerichte sollen nur noch auf der Basis von Rechtshilfeabkommen oder internationalen Vereinbarungen bei voller Transparenz gegenüber den Datenschutzbehörden erlaubt sein. Damit würde der Datenschutz beispielsweise gegenüber ausländischen Geheimdiensten deutlich gestärkt."*

So gesehen kann das bestehende Informationsmonopol der Geheimdienste auch nach dem Urteil des BfDI *Peter Schaar* rechtsstaatlich eingegrenzt werden.

Britta Schinzel

Josef Foschepoth – „Überwachtes Deutschland – Post- und Telefonüberwachung in der alten Bundesrepublik"

„Ein bisschen Heuchelei" sei Angela Merkels Reaktion auf die Nachricht gewesen, dass auch sie vermutlich abgehört wurde, denn „die NSA hat deutsche Politiker schon immer ganz legal observiert". Sie als Kanzlerin müsse von den zugrunde liegenden Vereinbarungen wissen und über die Zusammenarbeit der Dienste informiert sein, sagte der Freiburger Historiker Josef Foschepoth *in einem Interview mit der Zeit am 25. Oktober 2013.*[1]

In einem Interview mit der *Süddeutschen Zeitung* vom 9. Juli 2013, dessen Link inzwischen nicht mehr aufrufbar ist, sagt Foschepoth: *„Die NSA darf in Deutschland alles machen. Nicht nur aufgrund der Rechtslage, sondern vor allem aufgrund der intensiven Zusammenarbeit der Dienste, die schließlich immer gewollt war und in welchen Ausmaßen auch immer politisch hingenommen wurde."*[2]

Und so ist ganz korrekt, was der amerikanische Geheimdienstdirektor *James Clapper* erklärt, nämlich dass nur für „gültige Geheimdienstbelange" und „niemals unrechtmäßig" ausspioniert würde.[3]

Zumindest in Deutschland.

Über die Verträge zwischen Deutschland und den ehemaligen Alliierten, die eine solche Überwachung erlauben, kann jede und jeder sich seit 2012 in Josef Foschepoths Buch (inzwischen in der zweiten Auflage) informieren. Josef Foschepoth hatte bei Recherchen im Bundesarchiv Koblenz unbeschreibliches Glück

als ihm eine Akte mit der Aufschrift „Postzensur“, 1951, in die Hände fiel. Dieser Zufallsfund enthielt nicht weniger als einen Teil der Geschichte zur Überwachung des Post- und Fernmeldeverkehrs in der Bundesrepublik. Aufgrund einer Sondergenehmigung durch das Bundesministerium des Innern, nach Sicherheitsüberprüfung durch den Verfassungsschutz, bekam der Autor weitgehend ungehinderten Zugang zu den Verfassungsschutz-Akten der Bundesregierung, mit Ausnahme der Akten der Geheimdienste. Mit seinem Buch veröffentlichte er seine Entdeckungen.

Es erstaunt nicht wenig, in diesem Band zu lesen, dass es nicht nur in der ehemaligen DDR kein Post- und Fernmeldegeheimnis gab, sondern faktisch ebenso wenig – oder noch viel weniger – in der BRD. Die Foschepoth zugänglich gewordenen Quellen zeigen, wie seit 1949 zunächst die alliierten Westmächte auf ungehinderter Überwachung bestanden, im Weiteren aber alle deutschen Regierungen unter Umgehung des Grundgesetzes diese Überwachung durch die Alliierten tolerieren mussten, wollten und selbst fortsetzten. Unter dem Druck der Verhältnisse musste der Staatsschutz als ein höherwertiges Rechtsgut als das Grundrecht auf Unverletzlichkeit des Post- und Fernmeldegeheimnisses behandelt werden, obgleich im Grundgesetz festgeschrieben ist: „*die Grundrechte stehen […] über dem Staat und sind unmittelbar geltendes Recht, das alle drei Gewalten bindet. Aufgrund ihres vorstaatlichen und überpositiven Charakters dürfen und können sie durch keine Verfassungsänderung abgeschafft werden.*“ Insgesamt handelt es sich nicht nur um die Überwachung der Post- und Telekommunikation, sondern auch um individuelle Überwachung, um strategische Überwachung in Ost-, aber auch in Westeuropa und in der Bundesrepublik selbst, sowie Überwachung für staatliche und geheimdienstliche Zwecke.

Foschepoth analysiert die Entwicklung der heimlichen Überwachung unter den verschiedenen Gesetzgebungen von Beginn des Jahres 1949 an bis zur Bespitzelung nach der deutschen Wiedervereinigung 1989 – auf Wunsch und im Interesse der Alliierten.

Dabei lassen sich verschiedene Epochen, rechtliche Maßnahmen, Sprachregelungen und Legitimierungsstrategien unterscheiden, ab 1949 unter Siegerrecht, ab 1951 unter alliiertem Besatzungsrecht und 1954 unter Vorbehaltsrecht. Bis 1968 hatte der deutsche Staat nur äußerst beschränkte Souveränität. In den Westverträgen wurde den Westmächten mit Konrad Adenauers Einwilligung bestimmte Vorbehaltsrechte gewährt. Die Strategie zur Westintegration der Bundesrepublik war die der *doppelten Eindämmung*, nämlich der Eindämmung der „*deutschen und der sowjetischen Gefahr*“, mit der die intensive Überwachung des Post- und Fernmeldeverkehrs begründet wurde. Das alliierte Recht verlangte, dass die Bundesregierung die Überwachung nicht nur dulden, sondern auch aktiv daran mitwirken sollte. Adenauer handelte 1954 mit den Alliierten neue Geheimdienst- und Überwachungsrechte als *Vorbehaltsrechte* der Besatzungen aus, womit auch das Grundgesetz hinsichtlich des Post- und Fernmeldegeheimnis umgangen werden konnte. Die Ausübung der Vorbehaltsrechte wurde den drei Botschaftern in Bonn übertragen. Bei den Pariser Verhandlungen musste Adenauer neben dem Berlin-, dem Deutschland- und dem Truppenstationierungsvorbehalt auch den Notstands-, den Überwachungs- und den Geheimdienstvorbehalt akzeptieren. Ein wichtiges Instrument der doppelten Eindämmung war die Überwachung des internationalen und nationalen Post- und Fernmeldeverkehrs in der Bundesrepublik. Beteiligung und autonome Überwachungsaktivitäten des westdeutschen Staates wurden durch interne Verordnungen und Richtersprüche mit der Notwendigkeit begründet, Broschüren und kommunistisches Agitationsmaterial aus der DDR abzufangen. „*Der neue Staat wurde jedenfalls nicht von der Demokratie, sondern die Demokratie vom Staat her gedacht und aufgebaut*“ (Seite 17). Foschepoth nennt dies eine Staatsdemokratie.

Josef Foschepoth (2012): Überwachtes Deutschland. Post- und Telefonüberwachung in der alten Bundesrepublik. Göttingen und Bristol, CT, USA: Vandenhoeck & Ruprecht

1968 „gelang“ der Übergang in deutsches Recht durch die *G10-Gesetze*, und die folgende Übernahme des Überwachungsapparates durch die deutschen Geheimdienste, sowie die gesetzliche Verpflichtung der Bundesregierung, den Post- und Fernmeldeverkehr in der Bundesrepublik durch individuelle und allgemeine Überwachungsmaßnahmen zu überwachen. In Westberlin galt bis 1990 Besatzungsrecht.

Das Bundesamt für Verfassungsschutz und die Geheimdienste der drei Westmächte waren schon in den 1950er Jahren zu einem „einheitlichen nachrichtendienstlichen Organismus“ verschmolzen worden, wie später der Präsident des Bundesamtes für Verfassungsschutz, *Hubert Schrübbers,* während der Abhöraffäre 1963 erklärte.[4]

In der DDR erfolgte die westliche Fernmeldeüberwachung durch alliierte und westdeutsche Geheimdienste, die Kontrolle der Post hingegen musste gegen Einsprüche und Widerstände des Bundespostministeriums von Beamt_innen und Angestellten der Bundespost und des Zolls durchgeführt werden. Den Postler_innen war bekannt, dass sie sich mit den verlangten Eingriffen in rechtliche Zwickmühlen begaben, denn die einzige Rechtsgrundlage hierfür war bis 1968 nur die Treuepflicht der deutschen Beamt_innen dem Staat gegenüber, während im Widerspruch dazu das Grundgesetz die Unverletzlichkeit des Post- und Telefongeheimnisses garantieren sollte.

Es gab mehrere Anzeigen wegen nachweislich vielfach verschwundener Post, die jedoch von willfährigen Gerichten niedergeschlagen, d.h. deren Verfolgung wegen Mangels an Beweisen eingestellt wurde. Mehrfach verlangte die Bundesregierung vom Postminister einen eigenen gesetzlichen Vorschlag zur Legitimierung der Überwachung, die dieser jedoch immer wieder abschlägig beschied, mit der korrekten Begründung, nicht Überwachung sei Aufgabe der Post, sondern der Trans-

port. Doch weder im Parlament noch in der Öffentlichkeit wurden diese Dinge erörtert.

1961 aber verabschiedeten die Abgeordneten ein Gesetz zur Überwachung strafrechtlicher und anderer Verbringungsverbote, das „*sicher stellen sollte, dass keine Materialien eingeführt würden, die aus Gründen des Staatsschutzes strafrechtlich verfolgt wurden. Die Formulierung ‚stellen sicher' diente dazu, die Kontrolle und Durchsuchung der gesamten Post aus der DDR zu legitimieren und zu ermöglichen*" (Seite 268).

Erst die Abhöraffäre 1963/64 brachte die bundesrepublikanische Überwachung des Post- und Fernmeldeverkehrs aus der DDR an den Tag, sowie Informationen über die Besetzung des Verfassungsschutzes mit ehemaligen SS-Angehörigen und Nazigrößen – in Umkehrung des Auftrags der doppelten Eindämmung, jedenfalls der Eindämmung von Naziaktivitäten in der Bundesrepublik. Nach anfänglichen Leugnungen und Beschwichtigungen wurde ein Untersuchungsausschuss eingesetzt, der eine umfassende Analyse von immerhin mindestens 82 echten verfassungswidrigen Überwachungsfällen zutage förderte. In Wahrheit ging es um Massen von Postgut, um hundert Millionen Briefe und mehr, das damals überwacht, zensiert und zu einem Gutteil auch vernichtet wurde. Fünf Jahre dauerte es, bis die Überwachung, nun durch die Brandt-Regierung, in gesetzlichen Rahmen gefasst wurde. 1964 wurden infolge der Abhöraffäre 12 der 16 SS-Angehörigen des Verfassungsschutzes in andere Ämter abgeordnet.

Mit der großen Koalition 1968/69 ging eine Wende in der Rechts-, Politik- und Gesellschaftspolitik einher. 1968 wurde auf die nie wirksam gewordenen Notstandgesetze, das G10-Gesetz zur Beschränkung des Post- und Fernmeldegeheimnis still und leise, aber wirksam aufgesetzt. Somit wurden 1968 die alliierten Forderungen deutsches Recht und Verfassungsrecht und jede Bundesregierung verpflichtet, auch ohne Überwachungsvorbehalt der Alliierten deren Überwachungswünsche zu erfüllen und zu ermöglichen. Obgleich es ein ähnliches Gesetz in keinem westlich demokratischen Staat gibt, wurde es nicht öffentlich diskutiert, da die Überwachung nach Anordnung der Alliierten einer strikten Geheimhaltungspflicht unterlag, die auch mit rigiden Anordnungen rechtlich verankert und mit dem Schutz der Sicherheit der alliierten Streitkräfte begründet wurde. Dabei wurde u. a. das Trennungsgebot zwischen Verfassungsschutz und Polizei aufgehoben. Am intensivsten arbeitete der Bundesnachrichtendienst (BND) in Sachen der Post- und Telefonüberwachung mit den alliierten Diensten zusammen, weshalb die Bundestagsfraktionen sich bei der Abhöraffäre 1963 darauf einigten, den BND gar nicht zu erwähnen, um keinen weiteren Unmut in der Bevölkerung aufkommen zu lassen.

Das Geheimhaltungsgebot sah drastische Strafen dafür vor, dass Informationen zur Überwachung an die Öffentlichkeit gelangten, indem Verstöße mit Landesverratsprozessen, unbegrenzt hohen Geldstrafen, Gefängnis, bis hin zur Aberkennung des aktiven und passiven Wahlrechts bedroht wurden. Kein_e Abgeordnete_r konnte etwaige Verstöße gegen das Grundgesetz auch nur erwähnen. Anträge der Alliierten auf Überwachung wurden folglich im Parlament – bis heute – einfach durchgewunken.

Es fehlte nicht an Klagen vor dem Bundesverfassungsgericht:

> *„Das Urteil des Bundesverfassungsgerichts zum G10-Gesetz war ein Urteil, das in Sachen Rechtsstaatlichkeit und Grundrechte deutlich hinter frühere Entscheidungen desselben Gerichts zurückfiel, indem es nicht mehr die Grundrechte als ‚höchstes Rechtsgut', sondern den Staatsschutz als ‚überragendes Rechtsgut' definierte, zu dessen wirksamem Schutz Grundrechte, soweit unbedingt erforderlich, eingeschränkt werden können."*[5]

1978 wurde der Europäische Gerichtshof für Menschenrechte in Straßburg wegen der G10-Gesetzgebung angerufen und 1984 erneut das Bundesverfassungsgericht in Karlsruhe, ohne Ergebnis für die Priorität der Grundrechte. „*Das Bewusstsein für die Unrechtmäßigkeit staatlichen Handelns war zwar geschärft, aber der Grundkonflikt zwischen alliiertem Vorbehaltsrecht und westdeutschem Verfassungsrecht [...] noch nicht gelöst*" (Seite 159). Der Nachrichtenaustausch mit den Alliierten ging trotz Verbesserungen in der Verwaltungspraxis des Bundesamtes für Verfassungsschutz unvermindert weiter. Im Gegenteil, die Bundesregierung war jetzt neben einer Zusatzvereinbarung zum NATO-Truppenstatut auch durch das G10-Gesetz und eine geheime Zusatzvereinbarung, die in Foschepoths Buch erstmals veröffentlicht wurde, weiterhin verpflichtet, die Überwachungswünsche der alliierten Nachrichtendienste so weit wie möglich zu erfüllen.

Die Gelegenheit, die deutsche Wiedervereinigung zur Einstellung der Überwachungspraxen zu nutzen, und einen souveräneren deutschen Staat mit der Möglichkeit einer freiheitlichen Verfassung wirklich zu etablieren, waren bei den Zwei-plus-Vier-Verhandlungen 1990 nicht durchsetzbar. Die Westmächte waren nicht bereit, die Zusatzvereinbarungen zum G10-Gesetz und zum NATO-Truppenstatut aufzuheben.

Die Überwachungspraxis der Deutschen, die Installierung der Geheimdienste und die Gegenüberstellung der DDR-Praxen, die trotz großer Ambitionen aufgrund materieller wie technischer Unterlegenheit mit der des viel effektiveren Westens nicht vergleichbar war, beenden den historischen Teil des Bandes. Ein Vergleich mit der Überwachung der DDR als gleichsam deutsch-deutsches Problem drängt sich auf und ist noch nicht erforscht.

Im Rahmen dieser Veröffentlichung gelang es in Zusammenarbeit von Bundesarchiv, Historikerverband und auf Druck der Medien, die Bundesregierung zu einer Neuregelung der sogenannten *Verschlusssachenanweisung* zu bewegen, indem die Akten nun sukzessive freigegeben werden. Es handelt sich um mehrere Regalkilometer VS-Akten.

Leider fehlen nach wie vor die Dokumente der westlichen Geheimarchive und die der westdeutschen Geheimdienste seit 1968. Wahrscheinlich sind sie nach der Gesetzgebung von 1968 frühzeitig vernichtet worden. Unterdrücken, Löschen, Schreddern sind keineswegs Pannen, sondern systemimmanent, sie gehören zum Wesen dieser Dienste. Trotzdem erhebt sich die Frage, ob die Freigabe der VS-Akten nicht das Geheimhaltungsgebot unterläuft.

Es folgt ein resümierendes Kapitel zur Überwachung als strukturbildendem Prozess, in dem Foschepoth diskutiert, was die Überwachung für den demokratischen Staat mit Verfassung und Verfassungsbruch bedeutet, welche Vorstellungen von Rechtsstaatlichkeit und welche Praxen staatlichen Handelns in Konflikt mit den machtpolitischen Ansprüchen der westlichen Siegermächte möglich waren, wie sich die fortgesetzten Umgehungen und Brüche des Grundgesetzes auf die innere Entwicklung und Verfasstheit der Bundesrepublik, auf die Bedeutung von Recht und Verfassung im politischen Prozess der Bundesrepublik ausgewirkt haben. Dies reicht von der Rolle und Bedeutung der westdeutschen Geheimdienste für die innere Entwicklung über die, auch dadurch, kaum abzuschüttelnde NS-Vergangenheit bis hin zur Vielzahl nachrichtendienstlicher Affären – und zu den nicht zu nennenden Schäden der Doppelbödigkeiten auf Rechtsverständnisse und deutsche Selbstvergewisserung. Foschepoths These ist, dass die Überwachung ein wesentlicher Struktur bildender Teil des historischen Prozesses der Weststaatsbildung der BRD war. Jedenfalls zeigt sich, wie schwierig der Weg der Bundesrepublik war, in den Westen integriert zu werden bzw. sich zu integrieren, wie hoch der Preis dafür war, und wie schwierig, um nicht zu sagen unmöglich es weiterhin ist, ein souveräner Staat zu werden, und welche Hypothek verblieben ist. Es ist ein sehr trauriges Buch.

Von Seite 274 bis 356 werden die gesamten relevanten Gesetze ausführlich aufgeführt, Besatzungrecht und Westverträge, deutsch-alliierte Verhandlungen und geheime Vereinbarungen, alliierte Post- und Telefonüberwachung, deutsche Rechtsgrundlagen, westdeutsche Post- und Telefonüberwachung, und das Bundesverfassungsgerichtsurteil 1970 zum G10-Gesetz. Die bisher unbekannten und geheim gehaltenen Quellen und ein umfassendes Literaturverzeichnis ergänzen den Band.

Dem Buch hätte eine nochmalige redaktionelle Überarbeitung gut getan. Das tut seiner Bedeutung und Wichtigkeit jedoch keinen Abbruch.

Kehren wir zur Affäre um die Überwachung von Merkels Telefon zurück:

Im Interview mit *Zeit online* antwortet Foschepoth auf die Frage, ob nun die Bundesanwaltschaft die Lauschaktion gegen die Kanzlerin rechtlich prüfen werde:

> *„Dafür gibt es keine Grundlage. Ihre Überwachung ist durch die Verträge mit den USA gedeckt. Deshalb hat sich die Kanzlerin ja auch so merkwürdig zu der NSA-Affäre verhalten. Sie hat sich ein paar Mal ausweichend dazu geäußert, aber nichts dazu, was hier eigentlich mit dem Rechtsstaat passiert. Das deutsche Recht verhindert die Überwachung nicht. Die Verträge mit den USA verpflichten die Bundesregierung vielmehr, ihre Informationen darüber für sich zu behalten."*

Und nochmals in dem Interview mit der *Süddeutschen Zeitung* antwortet Foschepoth auf die nun viel aktueller gewordene Frage, ob der NSA-Whistleblower Edward Snowden gut beraten wäre, in die Bundesrepublik zu kommen:

> *„Auf keinen Fall. Aufgrund des Zusatzvertrags zum Truppenstatut und einer weiteren geheimen Vereinbarung von 1955 hat die Bundesregierung den alliierten Mächten sogar den Eingriff in das System der Strafverfolgung gestattet. Wenn eine relevante Information im Rahmen eines Strafverfahrens an die Öffentlichkeit gelangen könnte, heißt es in Artikel 38, ‚so holt das Gericht oder die Behörde vorher die schriftliche Einwilligung der zuständigen Behörde dazu ein, dass das Amtsgeheimnis oder die Information preisgegeben werden darf.' Gemäß der geheimen Vereinbarung wurde sogar der Strafverfolgungszwang der westdeutschen Polizei bei Personen aufgehoben, die für den amerikanischen Geheimdienst von Interesse waren. Stattdessen musste die Polizei den Verfassungsschutz und dieser umgehend den amerikanischen Geheimdienst informieren. Dann hatten die Amerikaner mindestens 21 Tage lang Zeit, die betreffende Person zu verhören und gegebenenfalls außer Landes zu schaffen. Was nicht selten geschah. Im Übrigen hat natürlich die Bundesregierung keinerlei Interesse, sich auf einen neuen Kalten Krieg, dieses Mal mit den Vereinigten Staaten, einzulassen."*

Anmerkungen

1 *http://www.zeit.de/politik/deutschland/2013-10/nsa-uerberwachung-merkel-interview-foschepoth*
2 *http://www.sueddeutsche.de/politik/historiker-foschepoth-ueber-us-ueberwachung-die-nsa-darf-in-deutschland-alles-machen-1.1717216*
3 http://www.focus.de/politik/ausland/us-geheimdienst-schlaegt-zurueck-attacke-gegen-den-bnd-nsa-chef-alexander-wirft-deutschland-spionage-vor_aid_1143343.html, 30. Oktober 2013
4 BArch, NL Brentano N1239/83 BfV, Nachrichtenaustausch zwischen BfV und alliierten Nachrichtendiensten, 25.09.1963, Seite 11, nach Foschepoth Seite 265
5 BVerfGE 30 15.12.1970, S 18, Zitat Seite 199

Britta Schinzel

Britta Schinzel stieg nach ihrem Studium der Mathematik und Physik in die Compiler-Entwicklung in der deutschen Computerindustrie ein. Von dort wechselte sie in die Theoretische Informatik an der TH Darmstadt und habilitierte dort. Im Rahmen ihrer Professur für Theoretische Informatik an der RWTH Aachen arbeitete sie in verschiedenen Gebieten der Künstlichen Intelligenz, initiierte eine Reihe interdisziplinärer Projekte mit Soziologie, Linguistik, Biologie und Medizin und begann sich, zunächst nur in der Lehre, später auch in der Forschung, mit *Informatik und Gesellschaft* zu beschäftigen.

Sara Stadler

Telefon- und Internetüberwachung

Chronologie der Enthüllungen II

Die Ereignisse und Berichte um die weltweite Telefon- und Internetüberwachung reißen nicht ab und sollen auch diesmal wieder für die interessierten LeserInnen chronologisch aufbereitet werden. Schade findet die Autorin, dass sich ein großer Teil der Presseberichterstattung an der NSA abarbeitet, während die Tätigkeit anderer Geheimdienste kaum erwähnt wird. Dennoch soll die Berichterstattung hier weitgehend abgebildet werden, es wird jedoch versucht, auch immer wieder auf die Tätigkeiten europäischer Geheimdienste hinzuweisen.

August 2013

14. August 2013: Die Grünen in Mecklenburg-Vorpommern wollen gegen die großzügigen Möglichkeiten zur Datenabfrage im Bundesland eine Sammelklage beim Landesverfassungsgericht einreichen. Kritik üben sie vor allem daran, dass es den Ermittlungsbehörden, anders als im Bund und den übrigen Bundesländern, möglich ist, Verbindungsdaten und Zugangscodes von TelekommunikationsnutzerInnen abzufragen, ohne eine richterliche Zustimmung einzuholen oder die Betroffenen zu informieren (Quelle: Heise).

16. August 2013: Wie die *Washington Post* unter Berufung auf Unterlagen aus dem Snowden-Archiv berichtet, sind Verstöße gegen Datenschutzregeln und gerichtliche Anordnungen bei der NSA an der Tagesordnung. Die Rede ist von tausenden Verstößen pro Jahr, wobei ein großer Teil unabsichtlich, etwa durch Schreibfehler von AnalystInnen erfolge (Quelle: Heise, Washington Post).

21. August 2013: Wie das *Wall Street Journal* unter anderem unter Berufung auf GeheimdienstmitarbeiterInnen berichtetet, kann die NSA mit Hilfe der Telecom-Firmen auf drei Viertel des US-amerikanischen Internetverkehrs zugreifen. Auch würden die Konzerne den Traffic zunächst nach vermeintlich geheimdienstlich Relevantem durchsieben. Ebenfalls durchsucht würde der ausländische Internetverkehr; Vereinbarungen mit Providern in vielen Ländern des Nahen Osten sowie Europas seien nach wie vor in Kraft (Quelle: Heise, Wall Street Journal).

21. August 2013: Wie die Piratenpartei berichtet, wurden 2012 von der Bundesnetzagentur 36,3 Millionen Bestandsdaten über TelekommunikationsnutzerInnen bei den Anbietern abgefragt und an Behörden weitergeleitet. Die Partei prognostiziert, dass dieser Rekordwert 2013 durch die neuen Möglichkeiten, die das im Mai verabschiedete Gesetz zur Bestandsdatenauskunft bereitstellt, noch übertroffen werden wird (Quelle: Heise).

22. August 2013: Aus einem Bericht des ehemals Vorsitzenden Richters am Geheimgericht FISC, John Bates, geht hervor, das auch die E-Mail-Kommunikation von US-BürgerInnen über mehrere Jahre von der NSA gesammelt und ausgewertet wurde (Quelle: Heise, New York Times).

23. August 2013: Wie der *Guardian* unter Berufung auf Dokumente aus dem Snowden-Archiv berichtet, haben zahlreiche US-Unternehmen, unter anderem Google und Yahoo, mehrere Millionen US-Dollar von der NSA erhalten, um geänderte Anforderungen bei der Kommunikationsüberwachung umzusetzen. Damit wird ein neuer Aspekt der Zusammenarbeit zwischen Unternehmen und Geheimdiensten bei der Überwachung der TelekommunikationsnutzerInnen deutlich (Quelle: Heise, The Guardian).

23. August 2013: Der britische *Independent* berichtet, dass Großbritannien als Teil des Programms Tempora eine geheime Abhörstation im Nahen Osten betreibe, die die durch Unterseekabel geleiteten (Kommunikations-)Daten abfange und analysiere. Die so gewonnen Informationen würden dem GCHQ und der NSA zur Verfügung gestellt (Quelle: Heise, The Independent).

25. August 2013: Wie der *Spiegel* berichtet, wird auch die UNO-Zentrale in New York von der NSA abgehört. Weitere Ziele der Spionage sollen die Botschaftsräume der Europäischen Union in New York sowie die EU-Botschaft in Washington gewesen sein (Quelle: Heise, Der Spiegel).

31. August 2013: Die *Washington Post* berichtet unter Berufung auf Dokumente aus dem Fundus Edward Snowdens, dass US-Geheimdienste allein 2011 insgesamt 231 Cyberangriffe ausgeführt hätten. Die Angriffe dienten einerseits der Manipulation oder Zerstörung von Informationen in Computern oder Netzwerken. Zum größten Teil würden die Angriffe jedoch ausgeführt, um Daten zu kopieren. Möglich würden die Angriffe unter anderem durch den gezielten Kauf von Software-Schwachstellen (Quelle: Washington Post, Heise).

September 2013

1. September 2013: Wie das Nachrichtenmagazin *Der Spiegel* berichtet, wurden auch das französische Außenministerium und der arabische Sender *Al Jazeera* von der NSA überwacht. Zudem könne der Geheimdienst auf das Buchungssystem der russischen Fluglinie Aeroflot zugreifen (Quelle: Der Spiegel).

2. September 2013: Auch die PräsidentInnen Mexikos und Brasiliens, Peña Nieto und Dilma Rousseff, werden nach Angaben des Journalisten Glen Greenwald von der NSA überwacht (Quelle: Die Zeit).

6. September 2013: Neue Veröffentlichungen aus dem Snowden-Archiv zeugen von den Anstrengungen der Geheimdienste NSA und GCHQ, die Verschlüsselung von Dateien im Internet zu knacken. Da gut implementierte Kryptografie den Geheimdiensten ernsthafte Schwierigkeiten zu bereiten scheint, würden sie unter anderem in Systeme eindringen, um an die noch unverschlüsselten Daten zu gelangen. Kommerzielle Hersteller würden

jedoch auf Veranlassung der Geheimdienste hin auch Hintertüren in ihrer Crypto-Hard- und -Software bereitstellen. Auch seien Verschlüsselungs-Standards gezielt von der NSA beeinflusst worden, so etwa ein Standard für einen Pseudo-Zufallsgenerator des National Institute of Standards (NIST), welcher später von der Internationalen Organisation für Normierung (ISO) ratifiziert worden sei (Quelle: New York Times, The Guardian, Heise).

9. September 2013: Weitere Snowden-Dokumente, die dem brasilianischen Fernsehsender *Globo* vorliegen, zeugen von der Überwachung von Unternehmen und Finanzinstitutionen durch die NSA. Genannt werden unter anderem das brasilianische Erdölunternehmen Petrobras und das Netzwerk SWIFT, über das alle länderübergreifenden Finanztransaktionen abgewickelt werden. Zugriff zu den Netzen würde der Geheimdienst sich über sogenannte *Man in the Middle*-Angriffe verschaffen (Quelle: Heise).

10. September 2013: Wie der britische Journalist Duncan Campbell berichtet, wirkt auch der schwedische Geheimdienst FRA bei der weltweiten Datenausspähung mit und unterstützt den GCHQ beim Abgreifen von Daten aus Unterseekabeln (Quelle: Heise).

11. September 2013: Die *Washington Post* berichtet, dass im Rahmen des am Anfang der Späh-Affäre bekannt gewordenen Überwachungsprogramms eine Datenbank mit Verbindungsdaten aller Telefonate der größten US-Telefonanbieter in gesetzwidriger Weise durchsucht worden sei. Da in diesem Fall US-BürgerInnen von der Überwachung betroffen sind, sorgt das in den USA für besondere Aufmerksamkeit (Quelle: Heise, Washington Post).

17. September 2013: Die NSA kauft Informationen über öffentliche Software-Schwachstellen von *Vupen Security*, wie aus ihrer Antwort auf eine Anfrage im Rahmen des Freedom of Information Act (FIO) hervorgeht. Ob sie auch Informationen über Zero-Day-Lücken erhält, wird allerdings nicht erwähnt (Quelle: Heise).

18. September 2013: Laut einem Urteil des US-Geheimgerichtes FISC fallen Verbindungsdaten nicht unter den Schutz der Privatsphäre und dürfen deshalb an Behörden weitergegeben werden (Quelle: Heise).

24. September 2013: Aus einem Bericht der indischen Zeitung *The Hindu* geht hervor, dass die NSA auch in Indien die Telefon- und Internetkommunikation überwacht, um Informationen auf den Gebieten Kernkraft, Weltraum und Politik zu erhalten (Quelle: Heise).

26. September 2013: Aus der Antwort der Bundesregierung auf eine Anfrage der Bundestagsfraktion der Linken geht hervor, dass das Bundeskriminalamt (BKA) in 82 Verbund- beziehungsweise Zentraldateien mit Namen wie „Erkennungsdienst" oder „Onlineshops" millionenfach Daten von Personen sammelt, von denen angenommen wird, dass sie in Zukunft möglicherweise strafrechtlich relevant handeln. Auch das Zollkriminalamt sowie die Bundespolizei verfügen über Tausende solcher Datensätze. Mit unterschiedlicher Analysesoftware werden die Datensätze ausgewertet, um beispielsweise Beziehungsmuster zu visualisieren (Quelle: Heise).

30. September 2013: Aus neuen Snowden-Dokumenten geht hervor, dass die NSA auf Basis der von ihr gesammelten Verbindungsdaten soziale Beziehungsmuster erstellt. Dazu dürften die Daten auch aus anderen Quellen, von Facebook-Profilen bis zu GPS-Ortungsdaten, angereichert werden. Der entsprechende Bericht der *New York Times* skandalisiert, dass von dieser Praxis auch US-BürgerInnen betroffen seien, da Telefonnummern oder E-Mail-Adressen nicht jeweils einzeln überprüft würden (Quelle: New York Times, Heise).

Oktober 2013

1. Oktober 2013: Wie der *Guardian* berichtet, werden Verbindungsdaten von InternetnutzerInnen von der NSA für ein Jahr gespeichert, ungeachtet dessen, ob sie von Interesse seien oder nicht (Quelle: The Guardian, Heise).

2. Oktober 2013: Wie die *New York Times* berichtet, habe die NSA zwischen 2010 und 2011 im Rahmen eines Pilotprojektes auch Standortdaten US-amerikanischer Mobiltelefone gesammelt, sich letztendlich jedoch gegen diese Praxis entschieden (Quelle: Heise, New York Times).

6. Oktober 2013: Das Nachrichtenmagazin *Der Spiegel* berichtet, dass der Bundesnachrichtendienst (BND) mindestens seit 2011 die Leitungen von 25 Internet-Providern am Datenknotenpunkt De-CIX in Frankfurt anzapfe. Von der massenhaften Auswertung des Datenstroms nach Schlagwörtern zu Themen wie „Terrorismus" seien vor allem Telefonate und E-Mails von Personen aus Russland, Zentralasien, dem Nahen Osten und Nordafrika betroffen. Deutsche StaatsbürgerInnen dürften dagegen nur in Einzelfällen abgehört werden (Quelle: Der Spiegel).

15. Oktober 2013: Auch Daten aus Chat-Kontakten und E-Mail-Adressbüchern würden Berichten der *Washington Post* zufolge von der NSA weltweit gesammelt und ausgewertet (Quelle: Heise, Washington Post).

20. Oktober 2013: Das *c't Magazin* beleuchtet in einem Bericht Geschichte und Arbeitsweise des polizeilichen Daten-Brokers Europol, der in den letzten Jahren enorm gewachsen sei. *Europol* unterstützt die Arbeit nationaler Polizeien vor allem durch Datensammlung, -austausch und -analyse, wobei die Datenschutzbedingungen einzelner Staaten außer Acht gelassen werden können. In „Arbeitsdateien zu Analysezwecken" (AWFs) sind aktuell über 100 000 Datensätze zu Personen gespeichert,

Sara Stadler

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

die nicht zwangsläufig jemals straffällig geworden sein müssen. Auch Kontaktpersonen, ZeugInnen und Opfer werden erfasst. Gespeichert werden dabei durchaus auch sensible Daten, z. B. über den Gesundheitszustand oder das Sexualleben der erfassten Personen. Ausgewertet werden die Daten von ca. 100 Analysten, denen dafür spezielle Softwaretools zur Verfügung stehen (Quelle: c't Magazin).

21. Oktober 2013: Wie die französische Tageszeitung *Le Monde* berichtet, werden auch Telefonate und E-Mails französischer BürgerInnen und Unternehmen von der NSA überwacht (Quelle: Heise).

22. Oktober 2013: Unter Berufung auf Akten aus dem Fall *Lavabit* stellt Cryptoseal seinen VPN-Service für PrivatkundInnen ein. Aufgrund der Befugnisse der US-Regierung sei es dem Anbieter nicht möglich, ihnen den Schutz ihrer Daten zu garantieren (Quelle: Heise).

23. Oktober 2013: Dass auch das Handy der Bundeskanzlerin Angela Merkel von der NSA abgehört wurde, führt in den folgenden Tagen dazu, dass die Bundesregierung die NSA-Affäre wieder für unbeendet erklärt (Quelle: Heise).

24. Oktober 2013: Einem Bericht des *Guardian* zufolge werden in Unterlagen aus Edward Snowdens Fundus insgesamt 35 nicht namentlich genannte SpitzenpolitikerInnen und RegierungschefInnen angeführt, deren Telefon-Kommunikation die NSA in den vergangenen Jahren überwacht habe (Quelle: The Guardian, Heise).

28. Oktober 2013: Wie aus einer Studie der EU hervorgeht, gibt es in Deutschland, Frankreich, Großbritannien und Schweden groß angelegte Abhöraktionen oder Überwachung von Kommunikationsdaten durch Geheimdienste. Allein in einem der fünf untersuchten Länder, den Niederlanden, sei dies nicht der Fall. Der Studie zufolge verfügen deutsche, französische und schwedische Geheimdienste nicht über die gleichen Kapazitäten wie britische und US-amerikanische, es sei jedoch aufgrund geheimdienstlicher Verflechtungen innerhalb der EU schwierig, die Tätigkeiten der einzelnen Geheimdienste rechtlich zu prüfen. Warum die AutorInnen der Studie aus der Erkenntnis, dass die meisten europäischen Geheimdienste der NSA an Kapazität unterliegen, den Schluss ziehen, „sichere" Kommunikationswege zu schaffen, indem der Datenverkehr nur über europäische Routen läuft, leuchtet nicht ganz ein. Immerhin wird jedoch auch empfohlen, Maßnahmen zu ergreifen, um unrechtmäßige Praktiken innerhalb der EU einzuschränken (Quelle: Heise).

28. Oktober 2013: Berichten des Journalisten Glen Greenwald zufolge hat die NSA auch in Spanien in großem Umfang Telekommunikations-Datensätze gesammelt (Quelle: Heise).

30. Oktober 2013: Die *Washington Post* berichtet, dass die NSA Daten von Google und Yahoo weltweit abgreife, indem sie sich heimlich in die Leitungen von Rechenzentren einklinke. Dem Magazin *Panorama* zufolge sei schließlich auch der Papst von der NSA überwacht worden (Quelle: Washington Post, Heise).

30. Oktober 2013: In einer Kongressanhörung verteidigen der US-Geheimdienstkoordinator James Clapper und der NSA-Chef Keith Alexander die Lauschangriffe in Europa. Alexander führt an, dass Europäische Staaten ihrerseits sowohl die USA als auch die eigenen BürgerInnen ausspionieren würden. Auch hebt er hervor, dass die millionenfache Datensammlung in Europa von den nationale Geheimdiensten mit verantwortet worden sei (Quelle: Heise).

CC BY

Konferenz der Informatik-Fachschaften

KIF 41,5:
Resolution/Stellungnahme zur flächendeckenden Überwachung des Internet

Die 41,5. Konferenz der Informatikfachschaften lehnt eine flächendeckende Überwachung des Internets durch Geheimdienste ab. Das verdachtsunabhängige Mitschneiden von Kommunikation und Verbindungsdaten ist in jedem Fall unverhältnismäßig zu dem dadurch erzielten Nutzen, da ein solches Vorgehen die Grundsätze und Funktionalität einer demokratischen Gesellschaft gefährdet.

Die 41,5. Konferenz der Informatikfachschaften fordert die Regierung der Bundesrepublik Deutschland auf, geeignete Schritte auf nationaler und internationaler Ebene zu ergreifen, um gegen eine flächendeckende Überwachung vorzugehen. Außerdem ist sicherzustellen, dass Unternehmen keine (Verbindungs-) Daten oder Kommunikation Ihrer Kunden an Geheimdienste im In- und Ausland weitergeben dürfen. Die Einhaltung der gesetzlichen Datenschutzbestimmungen muss stärker kontrolliert und durchgesetzt werden.

Die 41,5. Konferenz der Informatikfachschaften empfiehlt den Fachschaften, die Studierenden bei der Nutzung von abhörsicheren Internetdiensten zu unterstützen. Zu diesem Zweck können die Fachschaften Veranstaltungen durchführen, die über die Gefahren und das Ausmaß der Überwachung informieren, und darlegen, welche Schutzmaßnahmen existieren. Weiterhin ist darauf hinzuwirken, dass an Hochschulen sichere und vertrauenswürdige Kommunikationswege zur Verfügung stehen, wobei auf Dienste von Drittanbietern verzichtet werden soll. Für den Kontakt zur Fachschaft und die Kommunikation innerhalb der Fachschaft sollen die gleichen Grundsätze eingehalten werden und, wenn erforderlich, neue, sichere Kommunikationsmöglichkeiten eingerichtet werden. Besonders die im Rahmen der Fachschaftsarbeit anfallenden Daten sollen in geeigneter Weise vor den Zugriffen Dritter geschützt werden. In gleicher Weise soll dies auch für die KIF-Orga gelten.

Vom Abschlussplenum der 41,5. KIF im Konsens verabschiedet.

Stephan Geelhaar

Ausbau der Internet-Polizei

Die Neuregelung der Bestandsdatenauskunft, betrachtet am Beispiel des Bundeslands Mecklenburg-Vorpommern. Am bisherigen Ende der Debatte steht auch hier der erleichterte Datenzugriff für Sicherheitsbehörden als vermeintlich alternativlos.

Die Auseinandersetzung um die Bestandsdatenauskunft dauert nun seit über einem Jahr. Seit das Bundesverfassungsgericht (BVerfG) in seinem viel diskutierten Urteil Anfang vergangenen Jahrs eine Neuregelung angemahnt hatte, wurde die Auseinandersetzung zunehmend kontroverser. Die bisherige Zugriffspraxis der Sicherheitsbehörden auf Bestandsdaten der Telekommunikations-Teilnehmer sah das BVerfG nicht durch die bestehenden Gesetze gedeckt. Dieser Artikel widmet sich einem kleinen Ausschnitt aus dieser weit größeren bundesweiten Debatte, der Umsetzung der Bestandsdatenauskunft in Mecklenburg-Vorpommern. Da die neuen Gesetze in den einzelnen Länderparlamenten sowie im Bundestag nahezu parallel diskutiert und verabschiedet wurden, weist die regionale Debatte große Überschneidungen zur bundesweiten Diskussion auf. Trotzdem lohnt sich ein genauer Blick auf dieses Bundesland, da die hier verabschiedeten Gesetzesänderungen aus der Perspektive des Datenschutzes weit hinter die Neuregelung auf Bundesebene zurückfallen.

Kleines Daten-ABC vorab

Bestandsdatenauskunft bezeichnet eine Sammlung spezifischer Regelungen für den Datenzugriff durch Sicherheitsbehörden auf die sogenannten Bestandsdaten. Bestandsdaten sind die Daten, die für einen Telekommunikations-Vorgang notwendig sind und während der Nutzung von Telekommunikations-Geräten anfallen. Im Weiteren werden sie in Zugangsdaten und Nutzerdaten unterschieden, um eine Differenzierung zu ermöglichen. Nutzerdaten meint die Daten, die zum Abschluss eines Vertrags zwischen Telekommunikations-Dienstleistern und Teilnehmern notwendig sind, wie Name, Anschrift, Geburtsdatum, Telefonnummer, Nutzerkennung, E-Mail-Adresse, Vertragsbeginn und –ende. Zugangsdaten sind hier Informationen wie Passwörter, PIN und PUK von SIM-Karten oder auch Zugangscodes, von denen insbesondere Innenpolitiker immer wieder reden, wenn sie eigentlich Passwörter meinen. Nutzerdaten und Zugangsdaten können zu den Bestandsdaten gezählt werden und sind von den Verkehrsdaten zu unterscheiden, die während eines Telekommunikations-Vorgangs anfallen: Art und Dauer der Verbindung, Verbindungsteilnehmer, Standortinformationen (z. B. bei Mobilfunkgeräten) und – das ist in diesem Fall besonders wichtig – IP-Adressen. Inhaltsdaten sind ebenfalls von den Bestandsdaten zu trennen (SMS, Bilder, Gespräche oder Videos etc.). Sie sind von der Bestandsdatenauskunft nicht direkt betroffen.

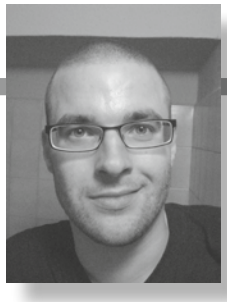
Sicherheitsbehörden fragen Nutzerdaten bereits häufig ab; im Folgenden geht es vor allem um die Abfrage von Zugangsdaten und die Identifizierung der Nutzer dynamischer IP-Adressen. Dieser Fokus ergibt sich daraus, dass sich viel Kritik am Zugriff auf Zugangsdaten entzündet. Trotz aller tatsächlichen und vermeintlichen Unterschiede stellt aber keine der im Parlament vertretenen Parteien die Datenabfrage durch Polizei und Geheimdienste grundsätzlich in Frage. Die Bemühungen richten sich vielmehr auf den Einbau (bzw. Abbau) möglichst vieler Haltelinien und größerer Hürden für den Einsatz der neuen Befugnisse.

Was bisher geschah

Ausgehend von einer Verfassungsbeschwerde gegen die im Telekommunikationsgesetz (TKG) festgeschriebenen erheblichen Speicherpflichten der Internet-Dienstanbieter einerseits und der umfassenden Erhebungsbefugnisse der Ermittlungsbehörden andererseits, kam es am 24. Januar 2012 zu einem Urteil des Bundesverfassungsgerichts. Es wies zwar die meisten Punkte der Beschwerde ab, stellte aber die Zugriffspraxis der staatlichen Stellen auf Zugangsdaten und die Ermittlung der Nutzer dynamischer IP-Adressen in Frage. Für die Kläger zumindest ein Teilerfolg.

Das BVerfG kippte die entsprechenden Regelungen und verhängte eine Übergangsfrist bis zum 30. Juni 2013. Bis dahin müsse der Gesetzgeber eine Neuregelung der einzelnen Gesetze umsetzen. Darüber hinaus formulierte das BVerfG mit dem „Doppeltürenmodell" konkrete Anforderungen darüber, wie die neu zu gestaltende Bestandsdatenauskunft aussehen müsse, wenn sie die gewünschten Datenzugriffsbefugnisse im Rahmen des Grundgesetzes ermöglichen soll. Demnach müsse das TKG die Dienstanbieter dazu ermächtigen und verpflichten, die Bestandsdaten ihrer Kunden überhaupt in vollem Umfang zu speichern und an Behörden herauszugeben. Für die Ermächtigung der Behörden zum Datenzugriff bedarf es einer weiteren juristischen Tür, einer Änderung des konkreten Behördengesetzes. Beide Gesetze – also TKG und das entsprechende Fachgesetz – sollen dann die Doppeltür ergeben.

Da aber nicht nur die Polizei sondern auch gleich alle anderen Sicherheitsbehörden den neuen Datenzugriff wünschen, steht die Politik im Zugzwang. Sie muss eine ganze Reihe von Fachgesetzen ändern, für die Behörden Bundeskriminalamt (BKA),



Stephan Geelhaar

Stephan Geelhaar studiert Informatik an der Universität Rostock und ist Neumitglied des FIfF.

Zoll und Staatsanwaltschaft sowie die verschiedenen deutschen Geheimdienste, Bundesnachrichtendienst (BND), Militärischer Abschirmdienst (MAD) und Verfassungsschutz. Im Föderalismus betrifft die Bestandsdatenauskunft auch die verschiedenen Landespolizeigesetze bzw. die Landesverfassungsschutzgesetze. Im Ganzen müssen also 16 Landesparlamente, der Bundestag und der Bundesrat über die Neuregelungen abstimmen.

Bestandsdatenauskunft in Mecklenburg-Vorpommern

Am 5. März 2013, als die Bundesgesetze noch mitten in der Diskussion in den Ausschüssen steckten, einigte sich die in Mecklenburg-Vorpommern regierende Große Koalition auf einen Gesetzentwurf zur Änderung des Sicherheits- und Ordnungsgesetzes (SOG) und des Landesverfassungsschutzgesetzes und gab ihn in das Parlament zur Verabschiedung. Das SOG ist das Polizeigesetz für die Landespolizei. In der ersten Lesung übergab der Landtag den Gesetzentwurf an den zuständigen Innenausschuss, zwei Oppositionsparteien kündigten bereits ihren Widerstand an. Der Entwurf passierte den Innenausschuss beinahe unverändert, fast alle Änderungsvorschläge wurden mit der Stimmenmehrheit von Schwarz-Rot abgewehrt. In der schriftlichen (wie auch später in der öffentlichen) Anhörung kritisierten einige Sachverständige und die Opposition das Fehlen von Richter-, Behördenleitervorbehalten sowie Mitteilungspflichten. Es zeichnete sich immer mehr ab, dass Mecklenburg-Vorpommern eine der schärfsten Länderregelungen zur Bestandsdatenauskunft bekommen würde.

In der zweiten Lesung im Landtag drückten die Regierungsparteien mit ihrer Stimmenmehrheit die Gesetzesänderung durch. Die Vertreter der Koalition sowie der Landesinnenminister Lorenz Caffier (CDU) versuchten in ihren Wortmeldungen, den Eindruck zu erwecken, es handele es sich bei der Verabschiedung des Entwurfs um eine bloße Formalität. Sie seien durch das Urteil des BVerfG zur Neuregelung angehalten und daraus ergebe sich ein unmittelbarer Sachzwang, da die Ermittlungsbehörden des Landes sonst keine Rechtssicherheit mehr hätten. Diese Argumentation behielten sie über das gesamte Gesetzgebungsverfahren bei. Zwei Zitate aus dem Landtag verdeutlichen die Geisteshaltung. Innenminister Caffier erläuterte die Notwendigkeit der Gesetzesänderung am 20. März:

> *„Die Anpassung der Gesetze ist deswegen notwendig geworden, weil vom Bundesverfassungsgericht neue Vorgaben gemacht wurden. Diese setzen wir jetzt um, nicht mehr und nicht weniger. Ich glaube, in der jetzigen Zeit ist auch jeder Landesinnenminister gut beraten, nicht mehr umzusetzen als das, was das Gesetz vorgibt, und das werden wir auch dementsprechend tun."*[1]

Der zweite Satz suggeriert, der Gesetzentwurf sei besonders zurückhaltend, tatsächlich zementiert er aber eine besonders fragwürdige Praxis der Polizeibehörden und Geheimdienste, die bisher rechtlich umstritten und alles andere als selbstverständlich war.

Im Laufe der Beratungen im Innenausschuss wie auch während der Verabschiedung im Parlament wurde der Landesregierung vorgeworfen, der Polizei einen umfassenden Zugriff auf die Bestandsdaten zu ermöglichen und ihre Befugnisse auszuweiten. Der oppositionelle Landtagsabgeordnete Peter Ritter (Die Linke) sah, vor dem Hintergrund der NSU-Affäre und der NSA-Enthüllungen, in dem Gesetzentwurf gar einen weiteren Baustein eines gesellschaftlichen Trends, der „Orwells Visionen zu Kindermärchen" machen würde. Die Vertreter der Regierungskoalition antworteten mit Beschwichtigungen, wie der Landtagsabgeordnete Heinz Müller (SPD):

> *„Rechtfertigt die Angst vor ausländischen Schnüffelagenturen, dass wir unseren Sicherheitsbehörden in ihrer berechtigten und sinnvollen Arbeit das Leben unnötig schwer machen?"*[2]

Entsprechend dieser wiederholten Argumentation zwischen Sachzwang und Bagatellisierung steht im Gesetzentwurf unter Alternativen auch schlicht *Keine*. Es ist schon kurios zu folgern, dass ein möglichst scharfes Gesetz beschlossen werden müsse, wenn das BVerfG für die bisherige Praxis keine Rechtsgrundlage sieht. Es aber noch als moderate Gesetzesanpassung zu verkaufen, ist ein politisches Kunststück.

Nichtjuristen und Bürgern ohne technisches Spezialwissen bleibt nur, den Abgeordneten ihres Vertrauens Glauben zu schenken. Eine eigenständige Lektüre der Gesetzestexte in schwer verständlicher Fachsprache ist ohne längerfristige Beschäftigung mit dem Thema zum Scheitern verurteilt. Geht man aber die einzelnen Kritikpunkte nacheinander durch, dann zeigt sich, welche Befugnisse sich für die einzelnen Behörden ergeben.

Richtervorbehalt

Damit ist gemeint, dass eine Maßnahme nur angeordnet oder eine Auskunft nur eingeholt werden darf, wenn dies vorher bei einem Gericht beantragt und durch einen Richter genehmigt wurde. Die Kritiker des Gesetzentwurfs forderten einen Richtervorbehalt für die Identifizierung von Internet-Anschlüssen über dynamische IP-Adressen. Zusätzlich müsse auch die Abfrage von Zugangsdaten einem solchen Vorbehalt unterliegen.

Es herrscht jedoch Uneinigkeit darüber, ob die Informationen über die Anschluss-Inhaber von dynamischen IP-Adressen zu den Bestandsdaten gehören, die abgefragt werden dürfen, oder ob sie zu den Verkehrsdaten gehören, die diesem Gesetz nicht unterliegen. Die Abfrage von Verkehrsdaten ist durch das Fernmeldegeheimnis eingeschränkt, dessen Schutz im Artikel 10 des Grundgesetzes festgeschrieben ist. Für Eingriffe in das Fernmeldegeheimnis gelten verschärfte Bedingungen. Das sieht auch Reinhard Dankert so, der Landesbeauftragte für Datenschutz und Informationsfreiheit. In seiner schriftlichen Stellungnahme für den Innenausschuss schreibt er:

> *„Die Zuordnung dynamischer IP-Adressen zu deren Nutzern setzt eine Analyse der Verkehrsdaten voraus und greift daher in Artikel 10 GG ein, wie das Bundesverfassungsgericht in seiner Entscheidung vom 24. Januar 2012 ausdrücklich klargestellt hat."*

Daraus ergibt sich ein Eingriff in die Privatsphäre, die unter besonderem Schutz steht. Ein Richtervorbehalt könnte ihn kompensieren – so der Vorschlag. Leider sah die große Koalition das anders. Das letztendlich verabschiedete Gesetz sieht weder für die Zuordnung von dynamischen IP-Adressen noch die Abfrage

Übersicht: Neuregelung der Bestandsdatenauskunft

	Zugriff auf Dynamische IP-Adressen & Zugangsdaten	Richtervorbehalt nur für Zugangsdaten	Mitteilungspflicht für IP-Adressen & Zugangsdaten
Staatsanwaltschaft	• Erhebung von Telekommunikationsdaten für die Erfoschung von Sachverhalten und die Ermittlung des Aufenthaltsortes einer Person	• Staatsanwalt oder Vertreter dürfen beim Richter beantragen • bei Gefahr im Verzug: Staatsanwalt oder Vertreter darf anordnen • Richterliche Entscheidung ist dann nachzuholen	• sie erfolgt wenn/sobald Zweck nicht vereitelt wird • sie unterbleibt bei schutzwürdigen Belangen Dritter
Bundeskriminalamt (BKA)	• zur Erfüllung der Aufgaben als Zentralstelle • Erhebung von Telekommunikationsdaten für die Erfoschung von Sachverhalten und die Ermittlung des Aufenthaltsortes einer Person • Erhebung/Sammlung personenbezogener Daten zur Erfüllung eigener Aufgaben	• Präsident des BKA oder sein Vertreter dürfen beim Richter beantragen • bei Gefahr im Verzug: Staatsanwalt oder Vertreter darf anordnen • Richterliche Entscheidung ist dann nachzuholen • richterliche Entscheidung nicht notwendig wenn der Betroffene bereits Kenntnis haben muss	• sie erfolgt wenn/sobald Zweck nicht vereitelt wird • sie unterbleibt bei schutzwürdigen Belangen Dritter
Bundespolizei	• Erhebung von Telekommunikationsdaten für die Erfoschung von Sachverhalten und die Ermittlung des Aufenthaltsortes einer Person	• Leiter der Bundespolizeibehörde oder sein Vertreter dürfen beim Richter beantragen • bei Gefahr im Verzug: Behördenleiter oder Vertreter darf anordnen • Richterliche Entscheidung ist dann nachzuholen • richterliche Entscheidung nicht notwendig wenn der Betroffene bereits Kenntnis haben muss	• sie erfolgt wenn/sobald Zweck nicht vereitelt wird • sie unterbleibt bei schutzwürdigen Belangen Dritter
Zoll	• zur Erfüllung der Aufgaben als Zentralstelle • Erhebung/Sammlung personenbezogener Daten zur Erfüllung eigener Aufgaben	• Leiter der Bundespolizeibehörde oder sein Vertreter dürfen beim Richter beantragen • bei Gefahr im Verzug: Behördenleiter oder Vertreter darf anordnen • Richterliche Entscheidung ist dann nachzuholen • richterliche Entscheidung nicht notwendig wenn der Betroffene bereits Kenntnis haben muss	• sie erfolgt wenn/sobald Zweck nicht vereitelt wird • sie unterbleibt bei schutzwürdigen Belangen Dritter
Bundesamt für Verfassungsschutz (BfV)	• zur Erfüllung der Aufgaben des Bundesamtes für Verfassungsschutz	• kein Richtervorbehalt vorgesehen	• sie erfolgt wenn/sobald Zweck nicht vereitelt wird • sie unterbleibt bei schutzwürdigen Belangen Dritter
Bundesnachrichtendienst (BND)	• zur Erfüllung der Aufgaben des Bundesnachrichtendienstes	• kein Richtervorbehalt vorgesehen	• keine Mitteilungspflicht vorgesehen
Militärischer Abschirmdienst (MAD)	• zur Erfüllung der Aufgaben des Militärischen Abschirmdienstes	• kein Richtervorbehalt vorgesehen	• keine Mitteilungspflicht vorgesehen
Landesamt für Verfassungsschutz MV	• zur Erfüllung der Aufgaben des Landesamt für Verfassungsschutz im Einzelfall	• kein Richtervorbehalt vorgesehen	• sie erfolgt wenn/sobald Zweck nicht vereitelt wird • sie unterbleibt bei schutzwürdigen Belangen Dritter
Landespolizei MV	• Erhebung von Telekommunikationsdaten im manuellen Auskunftsverfahren zur Abwehr einer Gefahr im Einzelfall	• kein Richtervorbehalt vorgesehen	• sie erfolgt wenn/sobald Zweck nicht vereitelt wird • sie unterbleibt bei schutzwürdigen Belangen Dritter • ist die Identifizierung von IP-Adressen nach 5 Jahren Zurückstellung nicht erfolgt, wird der Landesdatenschutzbeauftragte informiert.

von Zugangsdaten einen Richtervorbehalt vor. Aus Sicht der Hardliner sei im Falle der IP-Adressen besondere Eile geboten, das Warten auf eine richterliche Entscheidung würde den Zweck der Maßnahme untergraben. Auf Bundesebene hingegen wurde für den Zugriff auf Zugangsdaten ein Richtervorbehalt für BKA, Zoll, Bundespolizei und Staatsanwaltschaft eingeführt.

Behördenleitervorbehalt

Diese ist eine abgeschwächte Form des Richtervorbehalts. Statt eines unabhängigen Richters muss hier der jeweilige Behördenleiter vor der Datenabfrage konsultiert werden. Da der Richtervorbehalt auf Bundesebene bei Gefahr im Verzug (zur Abwehr einer konkret drohenden Gefahr) nicht gilt, wurde für diesen Fall der Behördenleitervorbehalt eingeführt, er ersetzt den Richtervorbehalt. Datenschützer und Oppositionspolitiker hatten versucht, statt des fehlenden Richtervorbehalts in den Landesgesetzen wenigstens den Behördenleitervorbehalt durchzusetzen. So wäre zumindest eine geringe Hürde für den Datenzugriff geschaffen worden. Beschlossen wurde diese Form des Vorbehalts jedoch weder für die Landespolizei noch für das Landesamt für Verfassungsschutz.

Mitteilungspflichten

Als Ausgleich für die schweren Eingriffe in die Privatsphäre der Betroffenen sehen die Gesetze eine nachträgliche Mitteilungspflicht an die Betroffenen vor. Sie ist auf Bundesebene für beide Formen der Datenabfrage durch Bundespolizei, BKA, Zoll, Staatsanwaltschaft und Verfassungsschutz vorgesehen. Mecklenburg-Vorpommern fällt aber auch in diesem Punkt deutlich hinter die Bundesebene zurück. Eine nachträgliche Mitteilungspflicht ist nur für die Identifizierung der dynamischen IP-Adressen vorgesehen, nicht jedoch für die Abfrage von Zugangsdaten.

Allerdings beruhen alle beschlossenen Mitteilungspflichten, egal in welchem Fachgesetz (und egal, ob in Bund oder Land), auf demselben ursprünglichen Gesetzentwurf. Ihr Wortlaut ist stets identisch und sie sehen eine Reihe von Einschränkungen vor. So kann die Mitteilung unterbleiben, wenn schutzwürdige Belange Dritter betroffen sind oder der Zweck der Maßnahme dadurch vereitelt werden könnte. Es ist daher zu erwarten, dass in der Praxis nicht viel von der Mitteilungspflicht übrig bleibt. Das sah die geladene Sachverständige Dr. Regina Michalke in der öffentlichen Anhörung des Innenausschusses ähnlich:

> *„[…] wenn dort die Unterrichtung und die Transparenz angesprochen ist, dann hat es nach der Formulierung zwar den Anschein, als sei die Unterrichtung der Betroffenen bei einer Datenauskunft, also über die erteilte Datenauskunft, der Normalfall, in der Praxis wird es aber gerade nicht der Fall sein. Das bedeutet aber, dass der Betroffene im Regelfall sich nicht dagegen zur Wehr setzen kann, dass seine Verkehrsdaten erhoben werden. Er wird im Regelfall zum Zeitpunkt der erteilten Auskunft hier nichts erfahren und er wird deswegen auch die Frage nicht prüfen oder überprüfen lassen können, ob die Nutzung der Daten auch tatsächlich zulässig gewesen ist. Wird, wie es in der Begründung des Entwurfes richtig, aber auch schonungslos und unverblümt heißt, der Betroffene informiert, so steht ihm allenfalls die Erlangung eines nachträglichen Rechtsschutzes offen. Ich meine aber, wenn die IP-Adresse erst einmal bekannt ist und wenn die PIN und PUK erst einmal geknackt sind, dann wird man dieses Wissen der Behörden wohl schwerlich zurückrufen können.“*[3]

Angesichts der bisherigen Praxis der Sicherheitsbehörden ist anzunehmen, dass Betroffene nicht in Kenntnis gesetzt werden und weder in der konkreten Situation noch hinterher ein Gericht anrufen können, um die Maßnahme juristisch zu überprüfen. In Kombination mit der im Telekommunikationsgesetz vorgeschriebenen Verschwiegenheit der Internet-Dienstanbieter erinnert die zu erwartende Praxis der Bestandsdatenauskunft an das FISA-Geheimgericht der USA.

Einzelfallregelung

Nur einem Änderungsvorschlag der Opposition gab die Regierungskoalition nach: bei der Einführung der Einzelfallregelung. Sie schreibt fest, dass die neuen Abfrage-Regelungen nur mit spezifischer Begründung für jeden einzelnen Fall angewandt werden dürfen. Die Koalition sah darin kein Problem, da ihrer Meinung nach die Grundlage für die Arbeit des Verfassungsschutzes bereits voraussetze, dass nur konkrete Einzelfälle bearbeitet würden.

Aushebelung des Fernmeldegeheimnisses

Das Fernmeldegeheimnis wird von zwei Seiten ausgehebelt. Einerseits betrifft das neue Gesetz die durch Artikel 10 des Grundgesetzes besonders geschützten Verkehrsdaten. Unter dem Vorwand, lediglich die Nutzerdaten durch die Bestandsdatenabfrage ermitteln zu wollen, werden die dynamischen IP-Adressen aus dem Schutzbereich des Fernmeldegeheimnis herausgezogen, da ihre Auswertung für die gewünschte Datenabfrage der Nutzer technisch erforderlich ist. Der zweite Angriff auf das Fernmeldegeheimnis ist die Abfrage der Zugangsdaten als Bestandsdaten. Ihre Herausgabe ermöglicht den Zugriff auf die geschützten Inhaltsdaten. Durch die Abfrage des PIN-Codes können die Daten auf dem zugehörigen Handy erlangt werden, beispielsweise die SMS, die während des Kommunikationsvorgangs noch unter dem Fernmeldegeheimnis stand. Kritiker werfen den Sicherheitsbehörden vor, so den Richtervorbehalt zu umgehen, der beim Abfangen von Telekommunikation (der SMS aus unserem Beispiel) besteht. Reinhard Dankert gibt zu bedenken, dass „Auskunftsersuchen zu Zugangssicherungscodes […] regelmäßig eine Vorstufe zu Maßnahmen dar[stellen], die ihrerseits den Schutzbereich des Art. 10 GG berühren können“, und empfiehlt, die parlamentarische Kontrollkommission zu unterrichten. Er sagte dazu in der öffentlichen Anhörung:

> *„Es gibt bei diesen Eingriffen, die die Polizei dann vornehmen kann, handelt es sich doch um gewichtige Grundrechtseingriffe, die wiegen schwerer als nur bloße Bestandsdatenabfragen. Wenn man erst mal die Passwörter, die PIN und die PUK hat, dann besteht die Möglichkeit, über weitere Inhalte auf Art und Weise der Kommunikation, Dauer der Kommunikation, auf frühere Kommunikation zuzugreifen, denn es ist im wahren Leben nicht davon auszugehen, dass sich der Betroffene jeden Tag die entsprechenden PIN, PUK und Passwörter ändert.“*[4]

Spätestens an diesem Punkt dürfte auch unvoreingenommenen Beobachtern deutlich werden, dass es sich nicht um harmlose Gesetzesanpassungen sondern intensive Verschärfungen handelt. Hardliner haben stets behauptet, die neuen Befugnisse seien unverzichtbar für die Arbeit der Behörden, trotzdem haben lediglich sieben weitere Bundesländer vergleichbare Gesetzesänderungen erlassen. Nur noch in Thüringen ist ein solches Gesetz auf dem Weg, in keinem der anderen Länder. Offensichtlich kommen die Länderpolizeien und Verfassungsschutz-Filialen dort ohne entsprechende Ermächtigungen aus.

Vorläufiges Fazit

Beim direkten Vergleich zwischen Bund und Land fällt auf, dass der Gesetzestext zur Bestandsdatenauskunft in Mecklenburg-Vorpommern wesentlich stärker am ursprünglichen Entwurf der Bundesregierung orientiert ist als das im Bund verabschiedete Gesetz. Während die Verhandlungen auf Bundesebene zur Einführung von Richter- und Behördenleitervorbehalten sowie zu umfangreicheren Mitteilungspflichten führten, fehlen alle diese nachträglichen Verbesserungen auf der Landesebene. Kritiker werfen der Landesregierung daher vor, dass sie den Bundesbehörden damit eine Möglichkeit zur Umgehung der Richtervorbehalte und Mitteilungspflichten schaffen würde.

Bei aller berechtigten Entrüstung bleibt Hoffnung: Der Prozess ist noch nicht abgeschlossen. Zwar wurden die Gesetze verabschiedet, entsprechende Verfassungsklagen laufen jedoch auf beiden Ebenen an. So unterschiedlich die Gegner und Befürworter, so verschieden sind auch die Erfolgsaussichten, die den Klagebemühungen eingeräumt werden.

Ein weiterer offener Punkt ist, dass die Gesetze größtenteils noch nicht in die Praxis umgesetzt sind. Den Dienstanbietern ist in der Regel noch nicht bekannt, wie die Behörden die neuen Rechtsvorschriften auslegen und welche Pflichten auf sie zukommen werden. Sehr wahrscheinlich ist, dass Dienstanbieter ab einer gewissen Größe eine elektronische Schnittstelle zur automatisierten Abfrage der Bestandsdaten durch die Bundesnetzagentur einrichten werden müssen. Für kleinere und alternative Dienstanbieter ist das noch unklar. Wir können gespannt sein auf den von der Bundesregierung für Ende 2015 angekündigten Bericht über die Auswirkungen der neuen Bestandsdatenauskunft.

Referenzen

„Datenschützer warnen: Polizei darf leichter PIN und Passwörter abfragen“ in Ostsee-Zeitung vom 8. April 2013, S. 6.

„Grüne wollen Zugriff auf private Passwörter stoppen“ in Schweriner Volkszeitung vom 16. Juli 2013, S.1.

„Datenauskunft neu geregelt“ in LandtagsNachrichten Mecklenburg-Vorpommern 6/2013 vom 18. Juli 2013, S. 10-11.

„Länder verabschieden neue Regeln zur Bestandsdatenauskunft“ auf www.heise.de (Zugriff 28.9.2013)
URL: http://www.heise.de/newsticker/meldung/Laender-verabschieden-neue-Regeln-zur-Bestandsdatenauskunft-1894865.html

„Grüne klagen wegen Datenabfrage durch Polizei in Mecklenburg-Vorpommern“ auf www.heise.de (Zugriff 28.9.2013)
URL: http://www.heise.de/newsticker/meldung/Gruene-klagen-wegen-Datenabfrage-durch-Polizei-in-Mecklenburg-Vorpommern-1935116.html

Anmerkungen

1 *Plenarprotokoll der 36. Sitzung des Landtages Mecklenburg-Vorpommern (6/36) vom 20. März 2013, S. 60-64.*

2 *Plenarprotokoll der 45. Sitzung des Landtages Mecklenburg-Vorpommern (6/45) vom 19. Juni 2013, S. 91.*

3 *Wortprotokoll der 32. Sitzung des Innenausschusses des Landtages Mecklenburg-Vorpommern vom 23. Mai 2013, S. 10.*

4 *Wortprotokoll der 32. Sitzung des Innenausschusses des Landtags Mecklenburg-Vorpommern vom 23. Mai 2013, S. 14.*

CC BY

Klaus Fuchs-Kittowski

Die Schwierigkeiten mit dem sozialen Aspekt

Zur Umprofilierung des Lehrstuhls: *Informatik in Bildung und Gesellschaft* an der Humboldt-Universität zu Berlin

Kein Geringerer als der Begründer der Kybernetik, Norbert Wiener*, hat nur zwei Jahre nach dem Erscheinen seines berühmten Buches* Kybernetik *eine Arbeit veröffentlicht:* The Human Use of Human Beings – Cybernetics and Society[1]*, in der er sich mit den sozialen und gesellschaftlichen Wirkungen der Kybernetik, speziell der Automation der Arbeitsprozesse auseinandersetzt. Wenn die Väter unserer Wissenschaft sich nicht scheuten, diese Probleme öffentlich zu diskutieren, sollte man meinen, dass dieses Vorbild aufgenommen würde. Leider war und ist dies erstaunlicherweise nicht oder nicht im erforderlichen Umfang der Fall.*

So waren z. B. schon der Gründung des Technischen Komitees *Wechselbeziehungen zwischen Computer und Gesellschaft* (TC9) der Internationalen Föderation für Informationsverarbeitung (IFIP) große Auseinandersetzungen in der Generalversammlung der IFIP vorangegangen. In der Generalversammlung war die Gründung eines Technischen Komitees für soziale Themen mehrfach auf grundsätzliche Ablehnung gestoßen. Darüber berichtet der damalige Präsident der IFIP, *Heinz Zemanek*, in einem Kapitel seines Buches, welches er überschrieben hat: Schwierigkeiten mit dem sozialen Aspekt.[2] In Organisationen in denen, wie in der IFIP, Ingenieure nur unter sich sind, neigen diese, wie Heinz Zemanek berichtet, dazu, anzunehmen, dass nur in den „Technischen Komitees“ gearbeitet und in einem „Komitee für nichttechnische Probleme“ nur geredet wird. In der Tat erlebte auch ich, wie der kanadische Computer-Pionier *C.C. Gottlieb*, der den Vorsitz einer Task Force zur Gründungsvorbereitung übernom-

men hatte, völlig verstört aus einer Sitzung der Generalversammlung kam, weil er massiv mit der Auffassung konfrontiert worden war, dass man in einem Komitee für nicht-technische Fragen „bloß reden würde". Als ich mich nach meiner Aufnahme ins TC9 und der Übernahme der Leitung der Arbeitsgruppe 1 *Computer and Work* dem sowjetischen Vertreter in der Generalversammlung vorstellte, bekam ich sofort auch entgegengehalten: „Ach das sind doch die, die immer nur reden!" Das war und ist offensichtlich eine international genutzte „Killerphrase".

Inzwischen ist viel Zeit vergangen. Viel hat sich hinsichtlich des Verständnisses des sozialen Aspekts der Informatik verändert. Vieles ist sicher besser geworden, manches anders.

Liest man heute verschiedene Beiträge z. B. im *Informatik Spektrum*, direkt vom Präsidenten der Gesellschaft für Informatik e. V.[3] oder in der *Wirtschaftsinformatik* über die Perspektive der Informatik, ihren wachsenden Einfluss auf die Gesellschaft, so könnte man sich schon fragen, ob es jemals diese Auseinandersetzungen gegeben hat. Der Gegenstand der Informatik wird weit gefasst, man kann sich nur freuen, welche Bedeutung dem sozialen Aspekt der Informatik beigemessen wird. Doch letztlich wundert man sich, warum dann die Disziplin *Informatik und Gesellschaft* nicht genannt wird. Der Tod der Disziplin wird nun erreicht, indem allgemeine Zustimmung, allgemeine Beschäftigung mit dem Thema vorgetäuscht wird. Dies ist natürlich noch gefährlicher als die offene Auseinandersetzung.

Mit Erstaunen und Erschrecken erfuhr ich von der Umprofilierung des bis zu seiner Emeritierung von *Wolfgang Coy* geleiteten, breit aufgestellten Lehrstuhls für *Informatik in Bildung und Gesellschaft*[4] hin zu einem Lehrstuhl, der ähnlich heißt, sich aber hauptsächlich mit intelligenten Tutoringsystemen, lies automatisierter Studierendenausbildung, beschäftigt. Es ist so erschreckend, da ausgerechnet an der Humboldt-Universität damit in doppelter Weise so eklatant gegen die Bildungsideale Wilhelm von Humboldts verstoßen wird. Dies, obwohl die für diese Entscheidung Verantwortlichen von verschiedenen Seiten[5] darauf hingewiesen wurden. Es ist für mich besonders erstaunlich und berührend, weil man auch wissen müsste, dass dieser Lehrstuhl auf besondere Empfehlung der internationalen Wissenschaftsgemeinschaft geschaffen wurde. So verabschiedete das TC9 der IFIP im Zusammenhang mit der Neustrukturierung der Humboldt-Universität nach der Wende einstimmig eine Resolution, in der es u. a. hieß:

> *„TC-9 considers it as essential that Social Aspects of Computing and especially the Impact of Computer on Work, to which fields Klaus Fuchs-Kittowski contributed so significantly, becomes an ordinary part of any Informatics Curriculum, as suggested by respected scientific organisations such as the Association for Computing Machinery (ACM) […]*
>
> *TC-9 therefore asks the German Informatics Society, as well as German authorities responsible for development of Informatics curricula, to ensure that education and research in Social Issues of Computing become a significant part of university education in Informatics, especially in newly established Informatics departments in East Germany, e.g. in Humboldt University."*[6]

Die Struktur- und Berufungskommission nahm diese, vom damaligen Chairman des TC9 und späteren Präsidenten der IFIP, *Klaus Brunnstein*, unterzeichnete Resolution ernst. Mit der Akzentverschiebung auf Bildung wurde der Lehrstuhl für *Informatik in Bildung und Gesellschaft* eingerichtet und mit Wolfgang Coy, einem dafür besonders engagierten und befähigten Informatiker besetzt. Wenn man sich die zuvor nur skizzierte besonders schwierige Wissenschaftentwicklung und die Notwendigkeit der Behandlung der sozialen Aspekte der Informatik auch in der heutigen Zeit verdeutlicht, kann man über die Fehlentscheidung, den Lehrstuhl umzuprofilieren, ob auf der Ebene des Fachbereichs, der Universität oder des Senats getroffen, nur entsetzt sein. Es ist der deutliche Ausdruck dessen, was der Philosoph Jürgen Habermas mit seinem neuen Buchtitel, als *Im Sog der Technokratie*[7] bezeichnet. Im Interesse der fruchtbaren Weiterentwicklung der Informatik und vor allem im Interesse der heute Studierenden ist nur zu wünschen, dass sich die Universitäten und Hochschulen für angewandte Wissenschaften diesem Sog der Technokratie entziehen können. Hierbei sollte man sich auch an die zu Recht oft beschworenen Lehren aus der Vergangenheit erinnern. Denn bekanntlich wurde das Studium Generale, aus dem sich an der Technischen Universität Berlin, auf Wunsch der Studierenden, das Fachgebiet Informatik und Gesellschaft entwickelte, durch die Alliierten eingeführt[8], da sie erkannt hatten, dass es dieses technokratische Denken war, welches dazu geführt hatte, dass sich insbesondere auch die technische Intelligenz in beiden Weltkriegen so bereitwillig zur Verfügung gestellt hatte. Die Entscheidung, Lehrstühle und Arbeitsgruppen auf dem Gebiet Informatik und Gesellschaft zu schließen oder umzuprofilieren, wie auch schon zuvor z. B. an der Universität Potsdam, der Freien Universität zu Berlin und jetzt auch an der Universität Freiburg, ist also eine Entscheidung wider die bitteren Lehren aus unserer Vergangenheit und sicher nicht gut für die weitere Entwicklung der Wissenschaft und Kultur in Deutschland. Auch der Lehrstuhl von Bernd Lutterbeck an der Technischen Universität Berlin

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.

wurde umprofiliert, jedoch so, dass die Lehre und Forschung auf den Gebieten *Mobile Security*, *Open Source* und *Intellectual Property* weitergeführt wird. Um dem Anspruch eines hohen Standards zu genügen, müssen sicher auch Spezialisierungen auf dem Gebiet *Informatik und Gesellschaft* möglich sein. Es sollten jedoch die Grundthemen von Informatik und Gesellschaft nicht soweit eingeschränkt werden, dass somit ein Lehrstuhl auf diesem Gebiet doch schrittweise eine Umwidmung erfährt.

Wir können nur hoffen, dass die Universitäten und Hochschulen dem Sog der Technokratie widerstehen, dass die Humboldt-Universität im Besonderen einen Weg findet, diese eklatante Fehlentscheidung zu bemerken und zu korrigieren. Der akademische, gesellschaftliche und politische Bedarf ist nun umfänglich vorhanden, und das nicht erst seit den Enthüllungen Edward Snowdens.

Ich danke Rainer Rehak für intensive Diskussionen zur Präzisierung verschiedener Aussagen in dieser Stellungnahme.

Anmerkungen

1 *Norbert Wiener, The Human Use of Human Beings – Cybernetics and Society, A Da Capo Paperback, New York, 1950*

2 *Heinz Zemanek, Weltmacht Computer, Weltreich der Information, Bechtle Verlag, Esslingen, München, 1991, S, 473 f.f.*

3 *http://www.gi.de/presse/detailansicht/article/auswirkungen-der-informatik-auf-die-gesellschaft-erforschen-und-diskutieren-1.html*

4 *http://waste.informatik.hu-berlin.de/*

5 *Die FIfF-Stellungnahme: http://fiff.de/stellungnahme-des-fiff-zur-besetzung-des-lehrstuhls-201einformatik-und-gesellschaft-und-didaktik-der-informatik201c-an-der-humboldt-universitaet-zu-berlin aber auch z. B. die Informatik-Studierenden der Freien Universität zu Berlin: http://fsi.spline.de/blog/2012/11/16/uber-die-professur-am-lehrstuhl-informatik-in-bildung-und-gesellschaft-der-hu-berlin/*

6 *Klaus Brunnstein, (Chairman IFIP TC-9), International Federation for Information Processing (IFIP) TC-9 Resolution, annual 1991 meeting at Tampere*

7 *Jürgen Habermas, Im Sog der Technokratie: Kleine politische Schriften XII, Edition Suhrkamp, 2013*

8 *Es ging den Alliierten natürlich nicht allein um die Einführung des Studiums Generale. Sie haben die Technische Hochschule Charlottenburg überhaupt erstmal zu einer Universität gemacht, was der General Officer der Britischen Truppen bei der Eröffnung so begründete: „Above all I think that it should be a home of true education and not of mere technology. […] All education, technical, humanistic, or what you will, is universal: that is to say it must embrace the whole of man, the whole personality, and its first aim is to produce a whole human being, capable of taking his place responsibly beside his fellows in a community. […] Science and technology can be devoted and must be devoted to advancing the peace and civilisation of man and this can only be so if they are used with responsibility. Responsibility is the cornerstone of democracy." (Speech delivered by the General Officer Commanding British Troops Berlin on the Occasion of the Opening of the Technical University Berlin-Charlottenburg on April 9th 1946.) Im Frühjahr dieses Jahres machte ich mit Besuchern aus den USA eine Bootstour durch Berlin. Als wir an der Technischen Universität vorbeikamen, berichtete die Reiseführerin in Deutsch und Englisch ausführlich über diese Entwicklung an der Technischen Universität. Sie gehört also zu den positiven Entwicklungen der Nachkriegszeit, die gerne vorgezeigt werden. Man sollte sich bei der Profilierung der Technischen Universität und insbesondere des Fachgebiets: „Informatik und Gesellschaft" dessen bewusst sein und die entscheidenden Worte des General Officer zur Gründung der Technischen Universität als Richtschnur dabei in Erinnerung rufen.*

Ursula Müller, Jürgen Kunert

Bericht von der Datenschutz-Sommerakademie 2013 in Kiel

Am 26. August 2013 fuhren wir vom FIfF Hamburg zu dritt zur Sommerakademie 2013 des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein (ULD) nach Kiel. Das ULD ist die Organisation des Schleswig-Holsteinischen Datenschutzbeauftragten Dr. Thilo Weichert, organisatorisch eine Anstalt öffentlichen Rechts.

Die Aufgaben schildert die Website *https://www.datenschutzzentrum.de/* wie folgt:

1. Das ULD geht jedem Hinweis auf Datenschutzverstöße nach und schickt den Betroffenen eine schriftliche Abschlussbewertung.

2. Das ULD kontrolliert aus eigener Initiative die Datenverarbeitung in schleswig-holsteinischen Behörden. Verstöße gegen das Datenschutzrecht werden beanstandet und die Beseitigung der Mängel wird gefordert.

3. Das ULD berät Behörden, Wirtschaftsunternehmen und Bürger in allen Fragen des Datenschutzes, z. B. bei Einrichtung neuer Computersysteme, Auslegungsfragen zum Datenschutzrecht oder in der Gesetzgebung.

Die Sommerakademie findet seit 19 Jahren jedes Jahr mit aktuellen Datenschutzthemen statt. Teilnehmer sind Datenschutz-Interessierte aus Politik, Wirtschaft – hier insbesondere Unternehmens-Datenschutzbeauftragte – und aus Lehre und Verwaltung. Auch etliche Landesdatenschutzbeauftragte sind jedes Jahr dabei, insgesamt 500 Teilnehmer, die für einen ausverkauften Tagungsbereich gesorgt haben. Dieses Jahr war das Thema: *Big Data – Informationelle Fremd- oder Selbstbestimmung?* Zielgenau hatten die Organisatoren damit auch in diesem Jahr ein Thema ausgewählt, das großes öffentliches Interesse hervorruft. Nach Wikipedia bezeichnet *Big Data* den „*Einsatz großer Datenmengen aus vielfältigen Quellen mit einer hohen Verarbeitungsgeschwindigkeit zur Erzeugung wirtschaftlichen Nutzens.*" Weiterhin sagt Wikipedia: „*Problematisch sind dabei vor allem die Erfassung, die Speicherung, die Suche, Verteilung, statistische Analyse und Visualisierung von großen Datenmengen.*" Ziel der Sommerakademie war es, eine Bestandsaufnahme zu leisten und die rechtlichen und die Aspekte des Datenschutzes aufzuzeigen.

Nach der Eröffnung durch Dr. *Thilo Weichert* war der Vormittag durch drei Vorträge von Vertreterinnen und Vertretern der Industrie geprägt.

Thilo Weichert bei der Eröffnung, Foto: Ursula Müller

Susanne Dehmel – Bereichsleiterin Datenschutz der *BITKOM e. V.* – stellte die *Big-Data*-Anwendungen in der Industrie positiv dar, zeigte den möglichen Nutzen für VerbraucherInnen und KundInnen, z. B. das leichtere Finden der richtigen Therapie für Krebspatienten, die Mitteilung von Verspätungen öffentlicher Verkehrsmittel, intelligente Stromnetze und vieles mehr. Den Datenschutz nehmen die Unternehmen der BITKOM „natürlich" sehr ernst. Der BITKOM-Leitfaden *Management von Big-Data-Projekten* enthält eine Checkliste *Privacy Impact Assessment*.

Vorstand *Stefan Noller* von der *nugg.ad* entwickelt Systeme für die Werbeindustrie auf der Basis von Big Data. Stefan Noller sprach von der Balance zwischen zielgenauer Werbung und dem Respekt vor den Nutzern und zeigte Rahmenbedingungen auf, die dazu beitragen können, diese Balance zu erreichen:

1. Vollständige Pseudonymisierung von Daten, insbesondere der IP-Adresse
2. Informationelle Gewaltenteilung, jeder sieht immer nur einen Teil der Daten
3. Transparenz und Zugriff
4. Opt-out-Widerspruchsrecht und First Steps to Opt-in
5. Keine Verwendung sensitiver Daten

Ein Produkt von nugg.ad wurde von der ULD zertifiziert (EuroPriSe-Zertifizierung), es erfüllt die datenschutzrechtlichen Kriterien. Es scheint also möglich, die Belange der VerbraucherInnen und der Anbieter in Bezug auf den Datenschutz unter einen Hut zu bringen. Als Schmankerl führte Herr Noller den „Cookie-Drucker" vor, der auf von nugg.ad betreuten Seiten die dort gespeicherten Nutzer-Informationen ausgibt.

Dr. *Günter Karjoth* vom IBM Research in Zürich stellte die Theorie hinter Anonymisierungsverfahren vor und zeigte Möglichkeiten der Renonymisierung anhand von praktischen Beispielen. Die theoretischen Hintergründe zu diesen Themen sind alle noch ziemlich neu, aus diesem Jahrtausend. Erschreckend war es, zu sehen, wie einfach in vielen Fällen die Anonymisierung aufgebrochen werden kann. Da es immer mehr Daten von uns im Netz gibt, wird es auch immer leichter, einzelne Anwender zu identifizieren.

Zum Abschluss des Vormittags gab es eine Diskussionsrunde der Vortragenden mit dem Publikum. Nach der Mittagspause wurde das Auditorium in zweimal vier Infobörsen aufgeteilt, in denen die folgenden Themen anhand eines Vortrags mit anschließender Diskussion behandelt wurden:

- *Open Data* und *Big Data*
- *Outsourcing* und *Tracking* in einer vernetzten Welt
- *Social Customer Relationship Management* und Datenschutz
- Datenschutz und IT-Sicherheitsmanagement als Grundlage für *Big Data*
- *Privacy by Design* für *Big Data*
- *Big Data* in der Medizin
- *Scoring* in Deutschland
- *@rtus*-Auswertung, PIAV & Co. – *Big Data* für die Polizei
- *Datamining*-Systeme und *Big Data*: alles böse oder bestehen Möglichkeiten zur Zertifizierung?
- Standard-Datenschutzmodell (SDM)

Im Anschluss wurden vor dem nun wieder zusammengeführten Auditorium die Kernthesen aus den Infobörsen vorgestellt.

Zum Abschluss gab es noch zwei kürzere Statements von Mitarbeitern bzw. Leitern landesnaher Organisationen und ein pointiertes Schlusswort des Leiters des zentralen Informationsmanagements (CIO) der Staatskanzlei Schleswig-Holstein, *Sven Thomsen* sowie eine Podiumsdiskussion mit Publikumsbeteiligung.

Was bleibt?

Wie bei jeder Technik zeigen sich auch bei *Big Data* positive und negative Seiten und es liegt an den AnwenderInnen, was man daraus macht. Durch die zunehmende Sammlung von Daten gibt es aber einen wachsenden Kontrollverlust für die VerbraucherInnen. Die Aufsichtsbehörden haben hier eine Menge zu tun, um den Missbrauch von Unternehmen und öffentlichen Stellen zu kontrollieren. Der Gesetzgeber ist wie immer in diesem Bereich ein Getriebener der technischen Möglichkeiten und immer „spät dran". Insgesamt gab es eine *„Wir können ja doch nicht viel tun"*-Stimmung bei allen Beteiligten. Das Erste, was wir als VerbraucherInnen tun können, ist immer noch der sparsame Umgang mit unseren Daten. Darüber hinaus können wir

1. „böse" Unternehmen boykottieren,
2. die Aufsichtsbehörden stärken,
3. Einfluss auf Politik und Behörden nehmen,
4. viele kleine Schritte in der Aufklärungsarbeit machen: *„Was hast Du zu verbergen?"*

Referenzen

Presserklärung des ULD: https://www.datenschutzzentrum.de/presse/20130827-sak-big-data.htm

Sämtliche Beiträge zur Sommerakademie 2013 können im Internet abgerufen werden unter https://www.datenschutzzentrum.de/sommerakademie/2013/

Ursula Müller und **Jürgen Kunert** sind Mitglieder des FIfF in Hamburg

Dagmar Boedicker

IT-Recht und Europa

Bericht vom 12. Bayerischen IT-Rechtstag

Am 17. Oktober 2013, nur ein paar Tage vor der Abstimmung im Innenausschuss über das Verhandlungsmandat des Europäischen Parlaments zur Datenschutzgrundverordnung[1], trafen sich um die 200 bayerische Expertinnen und Experten zum IT-Recht. Sie tauschten sich aus über verschiedene seiner europäischen Aspekte, mit den Schwerpunkten Datenschutz (vor allem zur EU-Grundverordnung), Gebrauchtsoftware und was es für deutsche Juristen bedeuten wird, dass europäisches Recht viele Bereiche durchdringt. Ort des Treffens war das Künstlerhaus am Lenbachplatz in München.

Prof. Dr. *Gerrit Hornung* von der Universität Passau ist ausgewiesener Datenschutz-Experte und hatte sich schon kurz nach Vorlage des Entwurfs der Grundverordnung (DSGVO-E) zu verschiedenen Aspekten sachkundig geäußert, beispielsweise zum Recht auf Vergessenwerden oder dem Datenschutz durch Technik. Hornung unterrichtet am Lehrstuhl für Sicherheitsrecht und Internetrecht, für seinen einführenden Vortrag hatten ihn die Veranstalter zu dem Versuch aufgefordert, europäisches IT-Recht zu strukturieren und systematisieren (in 45 Minuten). Das ist eine Pionieraufgabe, die Jura-Studierende sicher besser würdigen können als ich. Es gab aber Punkte dabei, die auch für unsereine/n spannend sind.

Kollateralregulierung

Ein Kriterium für eine Systematisierung kann der Querschnittscharakter europäischer Regulierung beim (IT-)Recht sein: So wie die Technik sämtliche Alltagsbereiche durchdringt, tut es auch das europäische Recht. Es beeinflusst fast alle Bereiche nationalen Rechts. Praktisch entstehen so Nebeneffekte aus gesetzgeberischen Handlungen, aber auch aus Entscheidungen des Europäischen Gerichtshofs (EuGH). Reguliert die EU Aspekte des elektronischen Rechtsverkehrs, so greift sie damit in den Verbraucherschutz, in Haftungsfragen und andere Gebiete ein. Mit der DSGVO-E reguliert sie die Datenverarbeitung in Wirtschaft und öffentlicher Verwaltung, die Folgen gehen sehr weit und die Bürger fragen sich, ob sie dazu legitimiert ist. Eine national gewachsene juristische Tradition erscheint auf ein Mal als Sonderweg, insbesondere dann, wenn wirtschaftliche und andere Akteure sich über lange Zeit darauf eingestellt haben. Da kann es schon passieren, dass ein für ein Unternehmen tätiger Anwalt meint, *Kollateralregulierung* sei aus Unternehmenssicht oft *Kollateralschaden*.

Widerspruch Konsistenzmechanismus

In der DSGVO-E hatte sich die EU-Kommission mit dem Instrument delegierter Rechtsakte in zahlreichen Einzelfällen die letzte Entscheidung vorbehalten, um eine weit gehende Harmonisierung des Datenschutzes in den Mitgliedstaaten durchsetzen zu können. Gleichzeitig besteht schon jetzt die Pflicht der Mitgliedstaaten, völlig unabhängige Datenschutzbehörden einzurichten. So unabhängig könnten die aber wohl nicht sein, wenn ihnen eine EU-Kommission in letzter Entscheidung das Heft aus der Hand nimmt. Hornung schlug ein unabhängiges Organ oder Gremium auf EU-Ebene vor, kontrolliert durch den EuGH. Er schloss sich damit dem Berichterstatter des Europäischen Parlaments, *Jan Phillip Albrecht* von den Grünen, an, der den europäischen Datenschutzausschuss (Nachfolger der Artikel-29 Gruppe) stärken will.

Der EuGH und andere

Hornung betonte die Rolle des EuGH als Integrationsmotor, der auf dem Wege der Vorabentscheidungen die Harmonisierung vorantreibe. (Nationale Gerichte können dem EuGH strittige Fragen des europäischen Rechts vorlegen, damit er vorab entscheidet, ob sie damit vereinbar sind.) Auch wenn diese Rolle des EuGH eine grundsätzlich sinnvolle sei, habe sie doch den Nachteil, dass Betroffene nicht direkt vor den EuGH ziehen können und beispielsweise in Deutschland den Instanzenweg bis zum BVerfG gehen müssen. Für den Datenschutz als ein Beispiel frage er sich aber, ob nicht die Zuständigkeit von Niederlassung oder verantwortlicher Stelle (gem. BDSG §1) vom EuGH entschieden werden sollte.

Da die Grundrechte fraglos Teil des europäischen IT-Rechts seien, verankert unter anderem in der Grundrechtecharta und dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV), komme auch dem Europäischen Gerichtshof für Menschenrechte (EGMR) eine wichtige Rolle zu. Dazu muss allerdings die EU der europäischen Menschenrechtskonvention beitreten, was absehbar ist und die Mitgliedstaaten bereits getan haben.

Kooperativ oder konfrontativ?

Da die Welt nun mal größer ist als nur die EU und das Internet uns mit ihr und sie mit uns verbindet – Märkte, Menschen, Rechtssysteme und Grundrechte – stellte Hornung zum Schluss

Dagmar Boedicker

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

Skulpturen von Schang Hutter im Innenhof des Künstlerhauses
Foto D. Boedicker

die Frage: „… das Universum, und der ganze Rest?" Europäisches (IT-)Recht richtet sich nach innen und ist auch nur innerhalb der EU legitimiert. Angesichts der globalen Pluralität von Werten, von Rechtssystemen und -durchsetzung, von grundrechtlichen Schutzpflichten in Deutschland und der EU, von Machtstrukturen und -ungleichgewichten ergeben sich ganz praktische Probleme. Hornung zeigte zwei Lösungsmöglichkeiten auf: In der Regel seien Konflikte im Diskurs auszutragen. Manchmal könne europäisches Recht als Vorbild sogar eine Sogwirkung entfalten. Aber manchmal gehe es eben auch nur konfrontativ. Dann sei die Verteidigung europäischer Standards Notwehr, beim Datenschutz beispielsweise durch das Aufkündigen der *Transatlantic Trade and Investment Partnership (TTIP)* wegen des Überwachungsskandals, den Edward Snowden aufdeckte. Gegenüber schwachen Partnern wäre das allerdings ein kaum zu legitimierender *Rechtsimperialismus.*

Zur Datenschutz-Grundverordnung

Die Abstimmung im Rechtsausschuss des Europäischen Parlaments über die DSGVO-E fand zwar erst am 21. Oktober statt, einige Teilnehmer/-innen am IT-Rechtstag wussten aber schon einiges über den Stand der Diskussion. So führte einer der Referenten seinen Vortrag mit der Bemerkung ein: „Es sind schon Änderungen zu meinem Manuskript eingetreten, die mir sehr angenehm sind."

Dr. *Stefan Schuppert* berichtete unter anderem über die Themen delegierte Rechtsakte, Meldung bei Datenverstößen, Recht auf Vergessenwerden, Einwilligung, *Privacy by Design*, Interessenabwägung und Zuständigkeit der Aufsichtsbehörden. Er führte die sechs Icons zur Einwilligung vor, die er nicht eben verständlich findet. Ihm war bereits bekannt, dass der Ausschluss einer wirksamen Einwilligung im Beschäftigungsverhältnis für die Verhandlungen im Innenausschuss gestrichen sei (Art. 7, Abs. 4) und auch das Koppelungsverbot unter Beschuss sei und „die Werbe-Industrie Erfolg haben" könnte.

Meldung bei Datenverstößen (Art. 31): Im Entwurf der EU-Kommission war eine Frist von 24 Stunden für die Benachrichtigung der Behörden vorgesehen, das Europäische Parlament habe sie auf realistische 72 Stunden verlängert. Die Betroffenen (Art. 32) seien immer dann zu benachrichtigen, wenn der Schutz ihrer personenbezogenen Daten oder ihrer Privatsphäre *wahrscheinlich beeinträchtigt* wird, die Aufsichtsbehörde könne eine Benachrichtigung verlangen. (Der Ministerrat empfiehlt eine Benachrichtigung nur bei drohenden *schwerwiegenden* Nachteilen.) Es werde vermutlich kein *Recht auf Vergessenwerden* geben, sondern ein Recht auf Löschung, verbunden mit der Verpflichtung, nach einer unberechtigten Veröffentlichung alle vernünftigen Schritte zur Benachrichtigung zu unternehmen. Zu Art. 23 *Privacy* (eigentlich *Data Protection*) *by Design and by Default*: aus der Vorlage sei die Verpflichtung für die Software-/Hardware-Hersteller gestrichen.

Dr. *Oliver Draf* sprach die Themen an, die für Versicherungen von besonderem Interesse sind: Gesundheitsdaten als besondere Daten[2], die Einwilligung als Hürde, die Übermittlung von personenbezogenen Daten ins Ausland, Risikomanagement und dafür wünschenswertes Profiling oder Scoring. Er zeigte sich zufrieden mit einer „komfortablen Lösung für die Bestandsdaten". Bei der Einwilligung sei zwar der Vorbehalt der Ungleichheit in Art. 7, Abs. 4 gestrichen worden, die beste Option wäre aber eine umfassende Lösung für die Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft und für das Delegieren von Aufgaben an spezialisierte Dienstleister. In eine solche Lösung wären auch die Rückversicherer einzubeziehen.

Cloud-Computing

Hierzu erläuterte Dr. *Fabian Niemann* die Entwicklung *vor und nach Snowden* und seine Einschätzung der aktuellen Situation. Er hält eine Auftragsdatenverarbeitung (ADV) auch außerhalb des europäischen Wirtschaftsraums für weiterhin rechtlich zulässig, eine Einschränkung nur auf den EWR für deutsches Sonderrecht und damit nicht für Richtlinien-konform. Anders als die deutschen Datenschutzbeauftragten (DSB) betrachtet er ADV sogar für besonders schutzwürdige (sensitive) personenbezogene Daten als möglich. Die Bewertung der DSB vom 24. Juli 2013, dass *Safe Harbor* und die Standardvertragsklauseln auszusetzen seien, weil ihre Prinzipien *mit hoher Wahrscheinlichkeit* durch die Geheimdienste verletzt würden, „müsse man nicht teilen"[3]. Schon die technischen Voraussetzungen und Inhalte, die sich im heterogenen und dezentralen Internet selbst ihre Wege suchten, machten vollständige geografische Grenzziehungen bei *public clouds* unmöglich. Niemann gab verschiedene Probleme zu bedenken: Die Grenze zwischen einer routinemäßigen bzw. nicht routinemäßigen Speicherung durch Geheimdienste sei unklar; Standardvertragsklauseln gelten mit China oder Russland weiterhin, für UK sind sie nicht einmal erforderlich. In Deutschland ist keine Genehmigung für ADV nötig, und Mitgliedstaaten könnten *Safe Harbor* und die Standardvertragsklauseln zwar aussetzen, das werde bisher aber nicht durchgesetzt. Generell sollte EU-weit beurteilt werden, ob sie mit *hoher Wahrscheinlichkeit* verletzt würden.

Niemann stellte aber einen De-facto-Effekt fest. Die Kunden zögerten noch mehr und fragten verstärkt eine *EU-Cloud* nach. Das sei ein Verkaufsargument, besonders bei Kunden, die selbst B2C-Kontakte betreiben, sowie für Geschäftsgeheimnisse, besonders schutzwürdige Daten und Arbeitnehmerdaten: „Ich erlebe immer mehr störrische Betriebsräte."

Anmerkungen

1 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)

2 Es handelt sich dabei um Daten, die in Deutschland einer besonderen Vertrauens- und Schweigepflicht nach § 203 Strafgesetzbuch unterliegen. Sie dürfen ohne Einwilligung der Betroffenen nicht von einer anderen Stelle verarbeitet werden.

3 Erfolgt mit hoher Wahrscheinlichkeit eine routinemäßige Speicherung durch Geheimdienste, sind nach Meinung der DSB Safe Harbor und die Standardvertragsklauseln auszusetzen. http://www.saechsdsb.de/oeffentlichkeitsarbeit/462-pressemitteilung-der-datenschutzkonferenz-vom-24-juli-2013 (abgerufen 7.11.13)

CC BY

Sebastian Jekutsch

Betrifft: Faire Computer

Fair wie in Faire Schokolade.

Fairness entlang der Liefer- und Wertschöpfungskette, das ist unser Wunsch. Diese regelmäßig erscheinende Kolumne mit aktuellen Entwicklungen zählt auf, wo es noch nicht so weit ist. Auch in diesem Quartal ist auf allen Ebenen etwas passiert.

Rohstoffgewinnung

Die Diskussion um *Konfliktmineralien* – bekannt ist hier vor allem die D.R. Kongo mit dem Metall Tantal – hat Fahrt aufgenommen, nachdem die EU die Absicht erklärt hat, eine Regulierung von Rohstoffgeschäften in Krisen- und Konfliktgebieten einzuführen. Die USA sind vorgeprescht mit dem Dodd-Frank-1502-Gesetz und der damit verbundenen Verpflichtung, Metallerzhandel im Kongo zu veröffentlichen. Das hat allerdings eben diesen Handel beinahe zum Erliegen gebracht, zum Nachteil der Bevölkerung. Die EU will sich nicht auf den Kongo beschränken, weil bewaffnete Milizen zum Beispiel auch in Peru (Gold) oder Kolumbien (Wolfram) vom Rohstoffhandel leben. Während NGOs gesetzliche Verpflichtungen und Sanktionsmechanismen verlangen, pochen die Unternehmen auf Freiwilligkeit und möglichst wenig Bürokratie. Freiwillig lässt sich praktisch kein EU-Unternehmen in die Karten schauen, was die Herkunft seiner Materialien angeht, das enthüllte ein NGO-Bericht.

Die Erze werden in den Krisenländern immer noch vor allem durch Tausende Schürfer in mühsamer, gefährlicher Handarbeit gefördert. Sind die Vertriebswege aber erst einmal sicher und erschlossen, so fürchten manche, kommen die großen *Rohstoffkonzerne*, hofiert von der Regierung, und beuten die Bergregionen aus. *Amnesty International* hat jüngst einen Bericht veröffentlicht, wie vor allem chinesische Unternehmen mit Unterstützung der Polizei die lokale Bevölkerung aus den friedlicheren Gebieten des Kongo vertrieben und in die Erwerbslosigkeit gezwungen haben. Das Material, meist Kupfer oder Kobalt, heißt dennoch offiziell konfliktfrei.

Gerätefertigung

Nach vielen Jahren *Foxconn* sind nun auch andere Fertiger wie *Pegatron* oder *Flextronics* regelmäßig in den Schlagzeilen. Die Branche boomt, und die Arbeitskräfte werden knapp. So rekrutierte Flextronics Malaysia Arbeiter aus fernen Ländern für die Kamerafertigung des iPhone 5. Als die Aufträge plötzlich fehlten, wurden die Arbeiter sich selbst überlassen, mit all den Schulden, die der Umzug und die Vermittlungsgebühren mit sich brachten. All dies war auch schon vor drei Jahren berichtet worden.

Die Praxis, Schüler und Studierende mittels Zwangspraktika zu billigen Arbeitskräften zu machen, wurde in den letzten Monaten mehrmals recherchiert, zum Beispiel bei der Fertigung der Playstation 4 von *Sony*.

Bei vier chinesischen Zulieferern von *Dell* und anderen haben sich nach einem aktuellen Bericht keine erkennbaren Verbesserungen eingestellt: 70-Stunden-Wochen, ungeschützte Arbeit mit Chemikalien, stupide Arbeit im Stehen, Beleidigung durch Vorgesetzte: all das widerspricht den offiziellen Grundsätzen von Dell. Wieder wurden Untersuchungen angesetzt, wieder erst nachdem investigative Recherche etwas ans Licht brachte.

Auch *Apple* hält seine Versprechungen zur Verbesserung der Situation nicht ein, wie jüngste Analysen ergaben. Zu Zeiten des bevorstehenden Markteintritts von iPhone 5S und 5C sind die Arbeitsstunden in den Fertigungsbetrieben wieder deutlich über die angestrebten 60 Stunden pro Woche gestiegen. Der Druck entsteht offensichtlich im Wesentlichen durch die Planung der Markenhersteller. Das Argument, die Arbeiter wollten gerne Überstunden machen, gilt nicht: Sie verdienen schlicht zu wenig, um ohne Mehrarbeit über die Runden zu kommen.

Gegen *Samsung* laufen weiter einige Klagen: in Brasilien wegen der Arbeitsbedingungen, in Frankreich wegen Kinderarbeitsvorwürfen und in Südkorea wegen Leukämiefällen in der Halbleiter-Fertigung. Jüngst wurde einem Opfer Entschädigungszahlungen zuerkannt, weil sich entgegen der Samsung-eigenen Untersuchungen ein Zusammenhang mit dem Arbeitsplatz nachweisen ließ.

Konsum

Fortschritte gibt es bei den beiden Projekten, bei denen Konsumenten sagen können: Ja, so will ich es. *NagerIT*, Hersteller der teilfairen Computermaus, nimmt die Arbeitsbedingungen in China in Augenschein und ergänzt die umfangreiche Dokumentation ihrer Lieferkette.

FairPhone, das Smartphone mit teilweise konfliktfreiem Tantal und Zinn, hat nun alle 25000 verfügbaren Geräte verkaufen können. Das Gerät wurde inzwischen offiziell vorgestellt, wird aber frühestens zu Weihnachten verfügbar sein. Es wurde eine Kostenaufschlüsselung veröffentlicht, aus der hervorgeht, dass 22 Euro pro Gerät für Nachhaltigkeitszwecke vorgesehen sind. Zum Zeitpunkt des Redaktionsschlusses liefen die Audits beim chinesischen Fertiger noch; der Bericht über die Arbeitsbedingungen stand also noch aus.

Die überraschendste Neuigkeit kommt aber vom gar nicht so selbstlosen *Bitkom*, dem deutschen Branchenverband von IT-Unternehmen, der zusammen mit dem Beschaffungsamt des Inneren eine Mustererklärung von Firmen für den Einkauf von IT durch die öffentliche Hand entworfen hat, und zwar mit explizitem Hinweis darauf, dass die Kernarbeitsnormen der internationalen Arbeitsorganisation ILO einzuhalten seien. Bislang wurden solche Kriterien als *vergabefremd* abgehakt.

Entsorgung

Die WEEE-Richtlinie der EU zur Behandlung von Elektroaltgeräten wurde neu geregelt. Sie verlagert nun die Nachweispflicht, ob etwas noch als reparierbar gilt und damit die EU verlassen darf, zum Exporteur. Bislang wurde unter dem Vorwand angeblicher Weiterverwendbarkeit Schrott illegal zum Beispiel nach Afrika verschifft, wo er unter meist haarsträubenden Umständen ausgeschlachtet wird. Beim Thema Entsorgung ist die EU Vorreiter, während die USA die relevante Basel-Konvention gar nicht erst unterzeichnet haben. Eine Reihe von NGOs verlangte jüngst von der EU, weiter voranzuschreiten und zu den als giftig geltenden Stoffen auch bromierte Flammschutzmittel hinzuzufügen, die in vielen Konsumprodukten bei der Herstellung und Entsorgung zwar große Probleme bereiten, für die bislang von den Herstellern aber keine geeignete Entsorgungsleistung verlangt wird.

Die Entwicklung bei den fairen Computern erscheint mir wellenartig: Vieles kommt mehrmals, wird diskutiert, angeklagt, beschwichtigt, vergessen und erscheint irgendwann wieder. Die sich wiederholenden Recherchen über die Arbeitsbedingungen in China sind so oder die Berichte über den Erzabbau in Entwicklungsländern. Manchmal aber wird dadurch etwas Wertvolles angeschwemmt und bleibt liegen, immer dann nämlich wenn ein Gesetz entsteht oder eine Firma sich den Empörungen der Öffentlichkeit beugt und einen Standard erreicht, hinter den sie nicht mehr zurück kann.

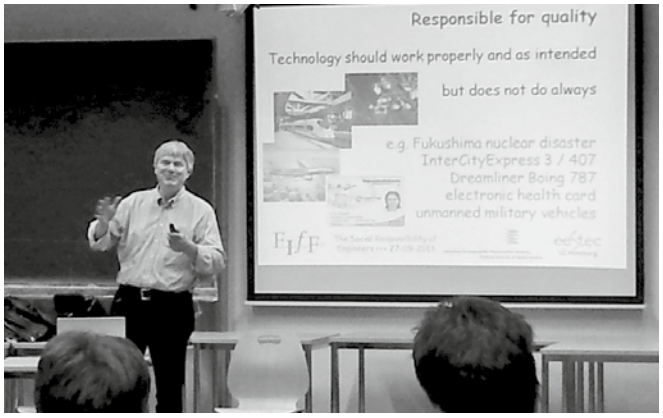
CC BY

Ursula Müller

FIfF unterstützt eine Veranstaltung über die soziale Verantwortung von Ingenieuren an der HAW Hamburg

Am 27. September nachmittags fand in den Räumen der *Hamburger Hochschule für angewandte Wissenschaften* (HAW) im Rahmen eines internationalen, einwöchigen Workshops der EESTEC[1], zu dem Elektrotechnik- und Informatik-Studierende aus ganz Europa eingeladen waren, eine vom AStA der HAW und vom FIfF organisierte Veranstaltung statt, zu der auch andere Interessierte eingeladen waren. Insgesamt kamen ca. 40 Personen zu einem sehr interessanten Event.

Den einleitenden Vortrag hielt Professor *Hans-Jörg Kreowski*, der mit gewohntem Können das Thema von vielen Seiten beleuchtete und die Standpunkte des FIfF gut rüberbrachte. Eine Gegenposition wurde von einem Studenten der HAW dargebracht, der ein Küchenmesser unter anderem mit Drohnen verglich und die Verantwortung der Ingenieure zu den „Anwendern" der Produkte schieben wollte. Die folgende angeregte Diskussion zeigte, dass sich die jungen Studenten aus ganz Europa schon vorher viele Gedanken gemacht und eine eigene Meinung gebildet hatten und sehr gut differenzieren konnten. Nach knapp drei Stunden musste der Diskussionsleiter dann die Veranstaltung beenden, da die EESTEC-Gruppe am Abend noch anderweitige Termine hatte.



1 http://eestec-hamburg.de/?page_id=22

Sara Stadler

Log 4/2013

Ereignisse, Störungen und Probleme der digitalen Gesellschaft

Immer wieder gibt es Ereignisse, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau von Rechten stehen. Wir dokumentieren hier einige davon. Die Aufzählung ist sicher nicht vollständig; mit einigen besonders gravierenden Vorkommnissen wollen wir aber auf die weiterhin besorgniserregende Entwicklung hinweisen. Wie in der vergangenen Ausgabe haben wir Ereignisse rund um die weltweite Telefon- und Internetüberwachung, die aktuell eine besondere mediale Aufmerksamkeit erfahren, in eine gesonderte Chronologie ausgelagert.

August 2013

1. August 2013: Das E-Government-Gesetz zur Förderung der elektronischen Verwaltung tritt in Kraft. Von DatenschützerInnen wurde das Gesetz unter anderem deswegen kritisiert, weil das gewählte Kommunikationsmittel De-Mail keine sichere Verschlüsselung bietet (Quelle: Heise).

10. August 2013: Mittels eines automatisch arbeitenden Überwachungssystems wertet die Deutsche Telekom die Verbindungsdaten sämtlicher Telefongespräche aus. Einer Stellungnahme der Telekom zufolge wird das System ausschließlich zur Feststellung von missbräuchlicher Nutzung eines Flatrate-Vertrags sowie zur Erkennung von Hacks auf Telefonanlagen von Firmenkunden genutzt. Das Magazin *WirtschaftsWoche* vermutet, dass das System auch eingesetzt wird, um Kunden zu erkennen, die eine Flatrate zwar legal, aber für das Unternehmen unwirtschaftlich nutzen **(**Quelle: WirtschaftsWoche, Heise)**.**

13. August 2013: Auf die im Rahmen der elektronischen Komplettüberwachung der europäischen Grenzen gewonnenen Daten sollen der Meinung zahlreicher EU-Staaten nach auch Ermittlungsbehörden zugreifen können. Die Maßnahme soll eine noch schnellere Ausweisung im Falle einer Visa-Überziehung ermöglichen (Quelle: Heise).

14. August 2013: Die brasilianische NGO *Repórter Brasil* berichtet von unzumutbaren Arbeitsbedingungen in einer Samsung-Fabrik im Norden des Landes. Die ArbeiterInnen müssten dort an bis zu 27 Tagen in Folge in Schichten von 10 bis 15 Stunden stehend Smartphone-Teile zusammensetzen. Über 2000 der insgesamt 5600 in dem Werk beschäftigten Personen hätten allein im letzten Jahr unter arbeitsbedingten gesundheitlichen Problemen zu leiden gehabt. Das Arbeitsministerium, welches in zwei Inspektionen 2011 und 2013 die schlechten Bedingungen festgestellt hätte, habe nun Anklage gegen Samsung erhoben (Quelle: Heise).

18. August 2013: Wie der *Spiegel* berichtet, verkaufen deutschen Apothekenrechenzentren Rezept- und Patientendaten an Marktforschungsinstitute, ohne dabei für eine ausreichende Anonymisierung zu sorgen (Quelle: Der Spiegel).

21. August 2013: Die Whistleblowerin Chelsea Manning wird, unter anderem wegen Verrat von Militärgeheimnissen, zu 35 Jahren Haft verurteilt (Quelle: Heise).

21. August 2013: Das Ministerium für Innere Sicherheit der Vereinigten Staaten (DHS) testet aktuell ein speziell entwickeltes System zur Videoüberwachung mit einem 3D-Verfahren, das Gesichter aus bis zu 100 Meter Entfernung erkennen und eine Foto-Fahndung erlauben soll. In Deutschland wird dieses Verfahren im Rahmen des Projekts GES-3D vom BKA vorangetrieben (Quelle: Heise).

22. August 2013: Zur Leistungssteigerung der Grenzkontrollen werden noch 2014 an zahlreichen deutschen Flughäfen automatische Grenzkontrollsysteme installiert. Den Zuschlag dafür haben nun die Berliner Bundesdruckerei und die Essener Secunet erhalten (Quelle: Heise).

30. August 2013: Die Bundesregierung beteiligt sich nicht nur als einer der größten Geldgeber am NATO-Programm *Advanced Ground Survelliance* (AGS), sondern plant auch die Anschaffung von vier Drohnen als „nationale Beistellung", so ihre Antwort auf eine kleine Anfrage der Linksfraktion. Anders als *Eurohawk* sind die AGS-Drohnen nicht mit dem ISIS-System zur Suche nach Funksignalen ausgestattet, sondern mit einem SAR/GMTI-Sensor, der bewegliche Ziele erkennen soll (Quelle: Heise).

30. August 2013: Um die Überwachung an deutschen Bahnhöfen noch weiter auszubauen, wollen das Bundesinnenministerium und die Deutsche Bahn AG gemeinsam 60 Millionen Euro investieren (Quelle: Heise).

31. August 2013: Mit einem neuen Verordnungsentwurf für einen gemeinsamen Telekommunikationsmarkt bewegt sich die EU-Kommission vordergründig auf KritikerInnen des Zwei-Klassen-Netzes zu. Dienste mit einem besonderen Service dürfen dem Entwurf zufolge nur dann angeboten werden, wenn traditionelle Dienste dadurch nicht „substantiell beeinträchtigt" werden. Die Bürgerrechtsorganisation *La Quadrature du Net* hebt hervor, dass auch in diesem Entwurf die bevorzugte Behandlung großer Netzbetreiber angelegt sei (Quelle: Heise).

September 2013

5. September 2013: Nach dem Skandal um Foxconn benennt die Organisation *China Labor Watch* (CLW) einen weiteren Apple-Zulieferer, in dessen Werk untragbare Arbeitsbedingungen herrschen. Der Elektronikhersteller *Jabil Circuit* lasse in Wuxi ein günstiges iPhone fertigen, dass bislang noch nicht auf dem Markt ist. Gefertigt wird es in Schichten von 11,5 Stunden, die die ArbeiterInnen im Stehen ableisten müssen. Als Pause sind lediglich 30 Minuten vorgesehen. Überstunden machen die ArbeiterInnen pro Monat etwa 110 – elf davon unbezahlt (Quelle: Heise).

5. September 2013: Gemeinsam mit anderen Organisationen veröffentlicht Wikileaks unter dem Namen *Spy Files 3* eine Datensammlung zum Handel mit Überwachungssoftware. Aus den insgesamt 249 Verkaufsbroschüren und Präsentationen geht hervor, wie europäische und US-amerikanische Unternehmen intensive und lukrative Geschäftsbeziehungen mit autoritären Staaten pflegen (Quelle: Heise).

15. September 2013: Der Hamburger Datenschutzbeauftragte Dr. Johannes Caspar kritisiert gegenüber dem Nachrichtenmagazin *Der Spiegel* Apples kommendes iPhone, das die Identität der BenutzerInnen mittels eines Fingerabdruck-Sensors feststellen soll. Auch wenn die Fingerabdruck-Daten dem Unternehmen zufolge nicht auf Cloud-Server übertragen würden, seien biometrische Daten auf einem iPhone nicht vor Zugriffen geschützt und sollten nicht leichtfertig abgegeben werden (Quelle: Der Spiegel).

18. September 2013: Die *Deutsche Polizeigewerkschaft* fordert ein Drohnen-Flugverbot – allerdings nur bei inländischen Veranstaltungen mit „Schutzpersonen". Anlass war eine Aktion der Piratenpartei während einer CDU-Wahlkampfveranstaltung, die mit dem Absturz einer etwa 40 Zentimeter großen Drohne endete. Die Piraten hatten die Drohne eingesetzt, um den anwesenden PolitikerInnen deutlich zu machen, wie es sich anfühlt, überwacht zu werden (Quelle: Heise).

19. September 2013: Der niedersächsische Verfassungsschutz räumt ein, seit 2006 in mindestens sieben Fällen JournalistInnen überwacht zu haben, die sich im Kontext ihrer Arbeit mit sogenanntem Extremismus beschäftigen (Quelle: Heise).

24. September 2013: Einundzwanzig Schweizerische Nationalräte wollen „Schwerverbrechern" künftig elektronische Chips zur Aufenthaltsfeststellung implantieren lassen. Die Parlamentarier aus der SVP-Fraktion, der Christdemokratischen Volkspartei (CVP) und der FDP Schweiz haben die Schweizer Bundesregierung aufgefordert, entsprechende gesetzliche Maßnahmen zu ergreifen (Quelle: Heise).

Oktober 2013

1. Oktober 2013: Der GKV-Spitzenverband gibt in einer Pressemitteilung bekannt, dass die herkömmlichen Krankenversicherungskarten zum 1.1.2014 ihre Gültigkeit verlieren. Dies sei gemeinsam mit der Kassenärztlichen Bundesvereinigung beschlossen worden. PatientInnen, die ab Januar ohne eine elektronische Gesundheitskarte behandelt werden möchten, können diese innerhalb von 10 Tagen nachreichen, bevor sie die Behandlung erstmal selbst in Rechnung gestellt bekommen. Die Kassenärztliche Vereinigung Hamburg spricht allerdings bereits am Folgetag von einer unbefristeten Übergangsregelung (Quelle: Pressemitteilung des GKV-Spitzenverbandes, Heise).

4. Oktober 2013: Auch die Arbeitsbedingungen bei Foxconn in Tschechien geraten über eine Reportage der c't in die Kritik. Im böhmischen Pardubice arbeiten Angestellte aus Vietnam, Bulgarien und der Mongolei zu Niedriglöhnen in Zwölf-Stunden-Schichten ohne Pausen am Fließband (Quelle: Heise).

10. Oktober 2013: Einem Report von *Games in Asia* zufolge werden Studierende des *Xi'an Institute of Technology* im Rahmen eines vermeintlichen Praktikums und unter der Androhung des Verlustes von Credit-Punkten gezwungen, in einem Foxconn-Werk in Yantei Spielkonsolen für Sony zu montieren. Die Arbeitsbedingungen seien die gleichen, für die Foxconn bereits mehrfach in die Kritik geraten ist (Quelle: Games in Asia, Heise).

17. Oktober 2013: Der Europäische Gerichtshof bekräftigt, dass die Speicherung digitaler Fingerabdrücke auf den deutschen Reisepässen zulässig sei. Das Urteil, das auf die Klage eines Bochumer Rechtsanwalts vor dem Verwaltungsgericht Bochum zurückgeht, wird mit der rassistischen Einreisepolitik der Europäischen Union begründet: Nur so könne die Einreise „Unbefugter" verhindert werden. Eine Gefahr für den Schutz persönlicher Daten kann das Gericht in der Speicherung biometrischer Daten nicht erkennen (Quelle: Heise).

21. Oktober 2013: Die drei Tage zuvor von den EU-InnenpolitikerInnen verabschiedete Kompromissfassung des Entwurfs für eine neue Datenschutzgrundverordnung wird vom Innenausschuss des EU-Parlamentes angenommen. Sie wird nun ohne eine 1. Lesung im Plenum direkt in Verhandlungen mit dem EU-Rat und der EU-Kommission eingebracht. Auch wenn an dem Entwurf einiges nachgebessert wurde, wird er von Bürgerrechtsorganisationen nach wie vor kritisiert, da er es in zahlreichen Fällen eben doch ermögliche, persönliche Daten ohne die Zustimmung der Betroffenen zu erheben und auszuwerten (Quelle: Heise).

21. Oktober 2013: Nach Amazon gerät nun auch der Online-Händler Zalando für die Arbeitsbedingungen in seinen Logistikzentren in die Kritik. Aus einem Bericht des Nachrichtenmagazins *Der Spiegel* geht hervor, dass die Angestellten in einem Verteilzentrum des Unternehmens überwacht und massiv unter Druck gesetzt werden (Quelle: Der Spiegel).

23. Oktober 2013: Aus einem Sachstandsbericht des Verteidigungsministeriums zum Thema *Eurohawk* geht hervor, dass die Entwicklung des ISIS-Systems zum Abhören von Funksignalen erfolgreich beendet worden sei. Offen sei noch, in welches Flugsystem ISIS eingebaut werde. Zur Integration von Drohnen im deutschen Luftraum werde das Verteidigungsministerium ein Luftfahrtamt der Bundeswehr (LufABw) gründen (Quelle: Heise).

29. Oktober 2013: Über eine Anfrage nach dem Informationsfreiheitsgesetz gelangt das „Handbuch zur Kampagne ‚Deutschland wird einfacher – neuer Personalausweis'" an die Öffentlichkeit. Der elektronische Ausweis, der nicht nur wegen eklatanter Sicherheitslücken, sondern auch wegen seiner Funktionalität als Überwachungsinstrument in der Kritik steht, soll den BürgerInnen über die Kampagne schmackhaft gemacht werden. Dafür soll unter anderem auch an ihren Nationalismus appelliert werden: geplant ist es, den Ausweis in allen Medien des Springer-Verlags als ‚Volksausweis' zu bewerben (Quelle: Heise).

CC BY

Christian Wölbert

Faire Computer: schwieriger als Kaffee, aber machbar

Gasteditorial zum Schwerpunktthema

Seit 2004 hat sich der Umsatz mit Fairtrade-Produkten in Deutschland verzehnfacht: von 50 auf 500 Millionen Euro. In Großbritannien liegt der Jahresumsatz sogar schon bei zwei Milliarden Euro. Immer mehr Menschen geben für Kaffee, Süßigkeiten und T-Shirts gerne mehr Geld aus, weil sie wissen, dass sie damit zu besseren Arbeitsbedingungen beitragen. Es liegt auf der Hand, dass viele von ihnen das auch bei Elektronik tun würden.

Fraglich ist nur, ob es jemals faire Elektronik geben wird, also zum Beispiel Laptops und Smartphones mit Fairtrade-Zertifikat. In diesen Geräten stecken hunderte Komponenten, die wiederum aus Dutzenden Rohstoffen bestehen, über deren Herkunft oft sogar der Hersteller selbst nichts weiß. Schwer vorstellbar, dass auf einem Smartphone irgendwann dasselbe Fairtrade-Logo klebt wie heute auf einer Banane oder einem Pfund Kaffee.

Ich glaube trotzdem, dass es einen fairen Elektronik-Sektor geben wird. Er entsteht zurzeit. Und ich finde es unglaublich spannend, diese Entwicklung zu beobachten. Seit ein paar Jahren arbeiten Forscher, NGOs und Unternehmen daran, die bislang kaum durchschaubare Lieferkette der Industrie offenzulegen und die Arbeitsbedingungen Schritt für Schritt zu verbessern.

Ganz am Anfang, bei den Rohstoffen, setzen die Industrie-Initiativen *Solutions for Hope* und *CFTI* an: Sie handeln mit Tantal und Zinn aus dem Kongo und stellen sicher, dass Bürgerkriegsmilizen nicht mitverdienen. Viele Hersteller nutzen diese Rohstoffe schon. Von der Konfliktfreiheit ist es nur noch ein kleiner Schritt zur Zahlung eines Aufpreises für bessere Arbeitsbedingungen. Fairtrade-Gold gibt es bereits, es muss nur noch in die Elektronik-Lieferkette eingespeist werden.

Susanne Jordan von *Nager IT* setzt am anderen Ende der Lieferkette an: bei den Bedingungen für die Arbeiter, die Komponenten zu fertigen Geräten zusammensetzen. Im Alleingang hat sie eine Maus entwickelt, die seit einem Jahr in Deutschland montiert wird. Die Arbeitsbedingungen sind überdurchschnittlich gut, die Lieferkette ist transparent, die Verkaufszahlen können sich sehen lassen. Nun versucht sie, bessere Bedingungen für die Arbeiter ihres chinesischen Kabel-Lieferanten zu erreichen. Und hofft, dass andere Hersteller ihre Strategie kopieren.

Das schwedische Unternehmen *TCO Development* hat sich ebenfalls zum Ziel gesetzt, die Arbeitsbedingungen in Elektronikfabriken zu verbessern. Seit einem Jahr überwacht *TCO*, wie ausgewählte Produkte von 15 großen Herstellern in China, Südkorea und weiteren Ländern montiert werden. Die *TCO*-Anforderungen sind noch gering, aber im Drei-Jahres-Rhythmus sollen sie in Zukunft verschärft werden – so wie zuvor die Umwelt-Anforderungen stetig hochgeschraubt wurden. Wenn die Hersteller das *TCO*-Siegel behalten wollen, müssen sie die Arbeitsbedingungen Schritt für Schritt verbessern, auch bei ihren Auftragsfertigern.

Das niederländische Unternehmen *Fairphone* setzt an beiden Enden der Lieferkette an: Es verwendet konfliktfreies Zinn und Tantal in einem Smartphone. Außerdem zahlen die über 20 000 Fairphone-Kunden einen Aufpreis für ein Programm zu Verbesserung der Arbeitsbedingungen bei der Montage in China, für einen Arbeiter-Sozialfonds und für die Überwachung dieser Maßnahmen.

Die konfliktfreien Rohstoffe aus dem Kongo, die faire Maus, das *TCO*-Siegel und das *Fairphone* sind die prominentesten Projekte für faire Elektronik. Es gibt Dutzende weitere: Studien vom Öko-Institut, Sozialkriterien beim *Blauen Engel* und Kampagnen von

Christian Wölbert

Christian Wölbert ist Redakteur bei c't und heise online. Zu seinen Schwerpunkten gehören Nachhaltigkeit, Verbraucherschutz, Mobilgeräte und Apps. Er veröffentlicht regelmäßig zu Themen der fairen IT, zum Beispiel recherchierte er in Tschechien zu den Arbeitsbedingungen bei Foxconn. Siehe auch *http://blog.ct.de/fairgreenit*

NGOs wie *Sacom* und *China Labor Watch*. Sie befragen chinesische Arbeiter und schaffen damit die Grundlage der meisten Medienberichte. Die Medien wiederum setzen die großen Hersteller wie HP, Apple und Samsung unter Druck.

Einige Hersteller igeln sich ein, einige haben aber auch Teile ihrer Lieferketten offengelegt, die Verhaltensregeln für Zulieferer verschärft und unabhängige Kontrollen zugelassen. Unwahrscheinlich ist, dass sie ausgewählte Produkte als „fair" vermarkten, weil sie damit den Rest ihres Sortiments abwerten würden.

Substanzielle Verbesserungen der Arbeitsbedingungen wird es deshalb nur dann geben, wenn die Politik die Regeln verschärft. Da muss noch mehr passieren. Bislang haben die USA die *Blutmineralien* aus der Lieferkette der Industrie gekegelt (leider mit unerwünschten Nebenwirkungen). In Deutschland müssen Behörden seit einiger Zeit nicht mehr zwingend die billigsten Computer kaufen, sondern können Sozialkriterien berücksichtigen. Aber EU-Gesetze für transparentere Lieferketten und bessere Arbeitsbedingungen sind überfällig – auch in EU-Staaten wie Tschechien werden Wanderarbeiter in Elektronikfabriken ausgebeutet.

Es gibt also noch viel zu tun. Ob auf den Produkten am Ende dasselbe Logo klebt wie auf dem Kaffee, ist unerheblich. Es kommt darauf an, dass Einzelne ihre Lieferketten offenlegen, einen überdurchschnittlich hohen Sozialstandard garantieren, die Machbarkeit demonstrieren und damit die gesamte Branche und die Politik antreiben – zusammen mit einer kritischen und immer besser informierten Öffentlichkeit.

CC BY

Sebastian Jekutsch

Sind faire Computer möglich?

Wir thematisieren in diesem Schwerpunkt nur nebenbei, dass unsere Computer, Smartphones, IT-Infrastruktur, eigentlich alle Elektronik unfair hergestellt werden. Es genügt, die aktuellen Entwicklungen in der regelmäßigen Kolumne Betrifft: Faire Computer *zu beobachten. Aber warum gibt es zum Beispiel fairen Kaffee, aber keine faire Kaffeemaschine? Ist faire Elektronik, sind faire Computer überhaupt realistisch?*

Die Antwort ist: Ja, selbstverständlich, aber einfach ist es nicht, denn:

Die Produkte sind komplex: Hardware besteht aus zig Rohstoffen und Hunderten von Bauteilen, die alle fair gewonnen bzw. produziert werden müssten, um das ganze Gerät fair nennen zu können. Aus diesem Grund gibt es zwar schon lange faire Bananen oder Fußbälle, bei fairer Kleidung wird es aber schon schwieriger (oft ist *nur* die Baumwolle selbst fair) und faire Elektronik steht noch lange nicht in den Verkaufsregalen.

Die Lieferkette ist lang: Über die Rohstoffe (meist aus Südamerika oder Afrika), die Bauteilefertigung (meist in Fernost), zur Fertigung (ebenfalls in Fernost, aber auch Osteuropa oder Mittelamerika), Transport, Vertrieb und Verkauf, bis schließlich zur Entsorgung beschäftigt die so genannte Wertschöpfungskette eine große Anzahl von Firmen in vielen Ländern mit unterschiedlichen Gesetzen und (De-)Regulierungen. Das erschwert die Chance auf eine hinreichende Zulieferertransparenz und damit die Durchsetzung, ja schon die reine Beurteilung der Fairness sehr.

Abhängigkeit von der Industrie: Um einen Computer fair herzustellen, müssten beispielsweise die Chips fair sein, und um diese fair herzustellen, sind enorme Investitionen nötig. Graswurzel-Aktivisten, aus deren Idealismus in der Vergangenheit oft die ersten fairen Produkte entstanden sind, können das schlicht nicht aufbringen. Die Großindustrie, die klassischen Hersteller müssen mitmachen, sonst klappt es nicht.

Hoher Innovationsdruck: Neue Elektronikprodukte setzen sich von der Konkurrenz vor allem durch neue Funktionen, besseres Design oder höhere Leistung ab. Reine Qualitätsmerkmale, wie etwa Umweltfreundlichkeit, Haltbarkeit oder eben Fairness in der Produktion, sind nachrangig. Während Fairness eine langfristige, planbare Investition voraussetzt, zwingt der Marktdruck die Hersteller zu Flexibilität und kurzen Produktionszyklen.

Bewusstsein der Konsumenten: Faire Nahrungsmittel, insbesondere mit Bioqualität, sind Käuferinnen und Käufern bekannt. Dass Elektronik fair sein könnte, aber unfair ist, der Gedanke ist neu. Niemand fordert es, daher fehlt auch der Nachfragedruck bei den Markenherstellern. Selbst die Green-IT, die sich lediglich um die Entsorgungsmöglichkeiten und den möglichst geringen Stromverbrauch beim Betrieb kümmert, ökologische Aspekte bei der Herstellung aber weitgehend ignoriert, ist als relevanter Kaufgrund kaum angekommen und in Werbung oder Vergleichstests wenig präsent.

Sebastian Jekutsch

Sebastian Jekutsch, FIfF-Mitglied aus Hamburg, ist Schwerpunktredakteur dieser Ausgabe der FIfF-Kommunikation. Er ist aktiv beim AK *Faire Computer* und betreut den Twitter-Account *@FaireComputer* und das *blog.faire-computer.de*. Unter *www.faire-computer.de* hat das FIfF weitere Quellen verlinkt. Wer beim AK mitmachen möchte, schreibt einfach an *FairIT@fiff.de*.

Ein realistisches Ziel kann also nur sein, Computer immer weiter ein Stück fairer zu machen, Rohstoff für Rohstoff, Bauteil für Bauteil, Gerät für Gerät. In diesem Schwerpunkt werden eine Reihe Strategien vorgestellt, die diese kleinen Schritte auslösen können.

Der Begriff *Fair* definiert sich in der Praxis oft dadurch, dass wir das als unfair Empfundene abgestellt haben wollen und nicht unterstützen möchten. Konkret soll Fair hier bedeuten, dass, wer für mich arbeitet – und sei es indirekt für mich als Konsumenten des von ihm hergestellten Produkts –, von mir fair behandelt wird. Dazu gehört, dass sie oder er einen guten (auch für eine Familie ausreichenden) Lohn bekommt, seine Würde bewahrt sowie seine körperliche und geistige Gesundheit nicht gefährdet wird, dass er nicht betrogen sondern angemessen beteiligt wird, sich auf die Arbeit verlassen kann und nicht der Willkür von Vorgesetzten und Auftraggebern ausgesetzt ist, einen (gegebenenfalls aus Kollektivverhandlungen hervorgegangenen) einklagbaren Vertrag hat, abgesichert ist gegen Krankheit und Alter und Perspektiven für eine Verbesserung seiner Situation sieht statt drohende Verschlechterung.

CC BY

Andrea Ben Lassoued

Kampagnen für „faire Computer“ – ein Überblick

Seit 2010 eine Reihe von Selbstmorden beim Gerätefertiger Foxconn internationales Aufsehen in den Medien erregte, sind die menschenunwürdigen Arbeitsbedingungen in der Elektronikindustrie ein heiß diskutiertes Thema. Schon seit 2004 gibt es Kampagnen verschiedenster europäischer Organisationen, die die skandalösen Arbeitsbedingungen in der Produktion von Hardware kritisieren. Dieser Artikel versucht einen Überblick zu schaffen, konzentriert sich aber auf Kampagnen und Organisationen, die sich für Arbeits- und Menschenrechte einsetzen.[1]

Im Januar 2004 startete die Entwicklungshilfeorganisation *CAFOD* mit Hilfe einiger Nichtregierungsorganisationen (*Non-governmental organisations*, NGOs) aus Mexiko, Thailand und Hong Kong die *Clean up your Computer*-Kampagne mit dem Ziel, mit Dell, IBM und HP einen einheitlichen Branchenverhaltenskodex zu verhandeln.[2] Schon im April 2004 hatten HP und IBM unternehmenseigene Verhaltenskodizes. Durch den großen öffentlichen Druck der Kampagne zog auch Dell bald nach. Wesentlich war dabei vor allem die Publikation eines Reports[3], der auf Basis von Interviews mit ArbeiterInnen die Arbeitsrechtsverletzungen bei den Zulieferern der drei Markenfirmen darstellte.[4] Inhaltlich waren die erwähnten Verhaltenskodizes der Firmen jedoch schwach, sie blieben alle hinter den ILO-Kernarbeitsnormen zurück. Ungewöhnlich schnell, würde ich aus heutiger Sicht sagen, einigten sich die drei Markenfirmen Dell, HP und IBM sowie fünf ihrer Kontraktfertiger im Oktober 2004 auf einen branchenweiten Verhaltenskodex, den noch immer bestehenden *Electronics Industry Code of Conduct (EICC)*. Heute, neun Jahre später, haben 89 Unternehmen den EICC unterzeichnet. Doch den Forderungen von CAFOD vor neun Jahren, nämlich die ILO-Kernarbeitsnormen einzuschließen, ist man noch immer nicht nachgekommen.[5]

Die deutsche NGO *WEED (Weltwirtschaft, Ökologie & Entwicklung)* beschäftigt sich seit 2004 mit dem Thema Produktionsbedingungen in der Computerindustrie. Unter dem Kampagne-Namen *PC Global*[6] fordert man Arbeitsrechte und Umweltgerechtigkeit in der Computerindustrie ein. WEED erstellt Bildungsmaterialien, gestaltet an zahlreichen deutschen Gymnasien, Berufsschulen und Universitäten Unterrichtseinheiten und führt Fortbildungen für Lehrerinnen und Lehrer durch. Spannendes Material für die entwicklungspolitische Bildungsarbeit bietet die von WEED gestaltete Bildungs-CD „Der Weg eines Computers“[7] sowie die DVD „Digitale Handarbeit – Chinas Weltmarktfabrik für Computer“.[8] Im Bereich sozial verantwortlicher öffentlicher Beschaffung ist WEED gemeinsam mit anderen

Abb.1: Die CAFOD-Kampgane Clean up your Computer *fand auch auf der Straße statt. Foto: CAFOD (cafod.org.uk)*

deutschen Organisationen höchst aktiv. So holte das Bundesbeschaffungsamt des BMI die Expertise von WEED und anderen NGOs ein, bevor es sich mit dem Branchenverband BITKOM an einen Tisch setzte, um eine IT-Mustererklärung zu verhandeln. Es bewegt sich also was in Deutschland in Richtung faire öffentliche IT-Beschaffung, und das nicht zuletzt aufgrund der langjährigen Bildungs- und Öffentlichkeitsarbeit von WEED.

Über aufklärende Berichte zur Bildungsarbeit

Eine weitere deutsche NGO, die schon länger zum Thema „faire Computer“ arbeitet, ist *Germanwatch*. Von 2007 bis 2012 war *Germanwatch* Mitglied der *makeITfair*-Kampagne[9]. Diese wurde von der holländischen Organisation *SOMO* geleitet. SOMO wird in der entwicklungspolitischen Szene für seine fundierten Reports und Studien geschätzt. Im Rahmen von *makeIT-*

fair beschränkten sich die NGOs nicht mehr auf die Publikation von Reports und anschließende Medienarbeit, sondern erweiterten ihr Tätigkeitsfeld in Richtung Bildungsarbeit. Neben dem Dialog mit Markenfirmen standen vor allem die Arbeit mit Universitäten und Schulen und die Publikation verschiedenster Studien[10] und kurzer, informativer Factsheets im Zentrum der Arbeit. Inhaltlich argumentierte die Kampagne für faire und grüne Elektronikgeräte. Dabei konzentrierte man sich nicht nur auf die Produktionsbedingungen, sondern bezog die gesamte Entstehungskette von Handys, PCs und mp3-Playern ein, von der Rohstoffbeschaffung bis zum Recycling. Laut *Irene Schippers*, Mitarbeiterin bei SOMO, war es zu Beginn der Kampagne für die meisten Markenfirmen neu, auf das Thema soziale Verantwortung angesprochen zu werden. Im Lauf der Kampagne begannen dann einige, Verantwortung für den Abbau der Metalle, die in ihren Geräten verarbeitet werden, zu übernehmen, indem sie untersuchten, woher die Metalle für ihre Produkte kamen. Beim zweiten Teil der Kampagne konzentrierte man sich vor allem auf Apple – mit dem Erfolg, dass Apple der *Fair Labor Association* beitrat, einer aus der Bekleidungsbranche bekannten Audit-Organisation für Arbeitsrecht. Die Ergebnisse dieses Schritts sind umstritten, doch steht außer Frage, dass es für die Firma selbst ein großer Schritt war.

In der Schweiz arbeiten die beiden Organisationen *Brot für alle* und *Fastenopfer* seit 2007 unter dem Slogan *High Tech – No Rights?* gemeinsam an einer *Kampagne für fair hergestellte Computer*.[11] Zwei Zielgruppen will man erreichen: KonsumentInnen einerseits und Marktführer in der Schweiz andererseits. Zu Beginn der Kampagne stand – wie so oft – die Publikation eines Reports. Berichtet wurde darin über die fünf Firmen mit dem größten Marktanteil in der Schweiz. Die Beteiligung der KonsumentInnen war groß: Über 5000 Personen unterzeichneten Postkarten, E-Cards und Briefe an das Management von Acer, Apple, Dell, HP und Fujitsu-Siemens, um Auskunft über Herstellungsbedingungen zu erhalten. Die Firmen reagierten sehr unterschiedlich. Eine Folgestudie wurde ein Jahr später in Auftrag gegeben[12], um Arbeitsbedingungen bei Zulieferfirmen in China zu überprüfen. Die Missstände hatten sich jedoch kaum verbessert.

Als konkreten Erfolg der Kampagne sieht *Brot für Alle*[13], dass die Firmen den Diskurs über ArbeiterInnen-Ausbildung aufnahmen und Verhaltenskodizes annahmen. Zwei Pilotprojekte zur Schulung von ArbeiterInnen bezüglich ihrer Rechte wurden gemeinsam mit HP in China gestartet und dort durch zivilgesellschaftliche Organisationen durchgeführt. Es war dies das erste Mal, dass im Elektroniksektor ArbeiterInnen-Trainings mit unabhängigen Organisationen durchgeführt wurden. Im September 2009 wurden abschließende Berichte über die Erfahrungen der Organisationen bei den Schulungen publiziert[14] und in einem ExpertInnen-Seminar wurden, gemeinsam mit Good Electronics, Guidelines für ArbeiterInnen-Trainings erarbeitet[15].

Im Bereich der öffentlichen Beschaffung gelang es der Kampagne *High Tech – No Rights?,* politische Vorstöße in verschiedenen Kommunen zu erreichen. Seit 2009 zum Beispiel werden Sozial- und Umweltkriterien im Kanton Waadt mit 20 % bei der Beurteilung einer Ausschreibung gewertet.[16]

Abb.2: makeITfair Aktionstag in Dresden, 2007
Foto: (c) www.makeitfair.org

Von Schulung der ArbeiterInnen bis zu Urgent Actions

Auch in Österreich beschäftigt man sich mit der sozial-fairen Beschaffung von IT. Seit 2008 läuft bei der österreichischen NGO *Südwind* die *Clean-IT*-Kampagne für faire Arbeitsbedingungen in der Computerindustrie.[17] Südwind arbeitet mit unterschiedlichen Ansätzen am Thema. Ein Konzept, das gut funktioniert, da es großes Medienecho erzeugt, sind Reisen in Länder des Südens. *Südwind*-MitarbeiterInnen besuchen Opfer von Arbeitsunfällen, ArbeiterInnen, die Fabriken besetzen, oder dokumentieren die Lebens- und Arbeitsbedingungen auf Elektromüllhalden. Durch eine anschließende Pressekonferenz und Straßenaktionen in Österreich macht Südwind der österreichischen Öffentlichkeit Erfahrungen zugänglich. Man verfolgt dabei das Ziel, Arbeitskämpfen in Ländern des Südens durch internationale Vernetzung mehr Druck zu verleihen.

Ein anderer Ansatz ist, Partner aus Ländern des Südens nach Europa einzuladen. GewerkschafterInnen, NGO-AktivistInnen und ArbeiterInnen berichten bei Pressekonferenzen oder Vortragsreihen[18] über ihr Engagement für Arbeitsrechte. Auch dieses Format erfährt meist breites Medienecho.

Um neben der oberflächlichen Medienberichterstattung eine tiefer gehende Auseinandersetzung mit dem Thema zu ermöglichen, publiziert Südwind gemeinsam mit Partnerorganisationen verschiedene Berichte, die Arbeitsrechtsverletzungen und den Widerstand der ArbeiterInnen dokumentieren.[19]

Ein weiterer Ansatz sind Petitionen. Südwind hat mit *Urgent Actions* (Eilaktionen) hinreichend Erfahrung. Zum Thema IT arbeitete Südwind mit diesem Ansatz, indem eine E-Mail-Petition für faire Arbeitsbedingungen in der Handy-Produktion 2012 durchgeführt wurde. Schon im Jahr 2010 versuchte man diese Herangehensweise mit dem Thema der sozial-fairen öffentlichen Beschaffung zu verknüpfen, indem in einer Postkartenaktion soziale Kriterien beim Computereinkauf an Fachhochschulen und Universitäten gefordert wurden.

Zwei Werkzeuge, die meist ohne großes Medienecho eingesetzt werden, dennoch aber langfristig sehr wirksam sind, sind Lobbying für sozial-faire öffentliche Beschaffung[20] einerseits und die Produktion von Materialien für die Bildungsarbeit[21] andererseits. Eine neue und sehr ambitionierte Zielsetzung, die Südwind mit sechs anderen europäischen NGOs und internationalen Partnern derzeit verfolgt, ist der Aufbau von *Electronics Watch*, der ersten internationalen Monitoring-Organisation für die Überprüfung der Arbeitsbedingungen in der Elektronikindustrie.[22]

Die Konzentration auf Marktführer und das Veröffentlichen von Recherchen über deren Zulieferer, das Stellen von öffentlichen Forderungen und eine möglichst breite Medienarbeit: Neben dem direkten Dialog mit Firmen, Bildungsarbeit und Lobbying, sind das die meist genutzten Instrumente in den dargestellten Organisationen. Die dahinter stehende Logik: Je breiter das Medienecho, umso schneller reagieren die Markenfirmen. In Gesprächen mit den Kampagnen-Leiterinnen (ja, es waren wirklich ausschließlich Frauen) versuchte ich auch greifbare Erfolge herauszufinden. Schnell wurde klar: Kampagnenarbeit braucht einen langen Atem – es ist ein mühsames, kleinteiliges Geschäft und die Firmen bewegen sich nur langsam.

Anmerkungen

1 *Nicht näher ausgeführt werden daher die Aktivitäten von* Greenpeace *zu E-Waste sowie die* Make IT Better-Kampagne *von* Friends of the Earth.

2 *High-Tech-Sweatshops in China. Arbeitsrechte im internationalen Standortwettbewerb und die Perspektiven von Corporate Social Responsibility. Weed, 2007: http://www2.weed-online.org/uploads/hightech_sweatshops.pdf*

3 *Vor dem* CEREAL-*Report gab es nur eine Studie zu Arbeitsbedingungen in Chinas Computerindustrie, die in den Jahren 2002 und 2003 entstanden war. Sie kam zu dem Schluss, dass es sich bei den meisten Fabriken, in denen für* HP, Compaq, IBM, Dell, Sony *und* Samsung *produziert wurde, um nichts anderes als High-Tech-Sweatshops handelte: Wong, Monina (2004): What difference does ‚Corporate Social Responsibility' make to improve labour standards in China? In: AMRC (Hg.): A critical guide to corporate codes of conduct: Voices from the South. Hong Kong. S. 59-69. http://www.amrc.org.hk/system/files/critical-guide-to-codeof-conduct.pdf*

4 *Clean Up Your Computer. Working conditions in the electronics sector.* CAFOD*, 2004: http://www.catholiclabor.org/gen-art/cafod-computers.pdf*

5 *Vom Erfolg zivilgesellschaftlicher Akteure: http://blog.faire-computer.de/vom-erfolg-zivilgesellschaftlicher-akteure/#more-270*

6 *http://www.pcglobal.org*

7 *http://www.weed-online.org/themen/wk/799849*

8 *http://pcglobal.org/index.php?option=com_content&view=article&id=93*

9 *http://makeitfair.org/de?set_language=de*

10 *Eine Fülle von Reports und Factsheets, die in Zusammenarbeit mit Partnern aus Ländern des Südens entstanden, können unter http://makeitfair.org/de/die-fakten/studien abgerufen werden.*

11 *http://www.fair-computer.ch/*

12 *Durchgeführt wurde diese von* Students and Scholars Against Corporate Misbehaviour *(SACOM), einer NGO mit Sitz in Hongkong.*

13 *Persönliches Telefonat mit Chantal Peyer, ehem. Leiterin der Kampagne bei* Brot für Alle *(27.9.2013)*

14 *SACOM produzierte für die High Tech – No Rights-Kampagne zwei Berichte. Beide stellten die Arbeitsbedingungen bei Zulieferfirmen von* HP *in Dongguan, China dar. Die Studie über* Chicony Electronics *ist unter http://www.fair-computer.ch/cms/fileadmin/user_upload/computer-Kampagne/Pilotprojekt_09/ChiconyAUG2009.pdf abrufbar, jene zu* Delta Electronics *findet sich unter: http://www.fair-computer.ch/cms/fileadmin/user_upload/computer-Kampagne/Pilotprojekt_09/DeltaAUG2009.pdf*

15 *http://goodelectronics.org/publications-en/Publication_3690*

16 *Siehe dazu auch: http://www.fair-computer.ch/cms/index.php?id=370*

17 *http://www.clean-it.at/*

18 *Diese sind oft Teil eines EU-Projektes. Die Gäste reisen dabei meist nicht nur quer durch Österreich, sondern vielmehr quer durch Europa. Eine belastende, aber sehr lohnende Art, das Thema bekannt(er) zu machen.* Kevin Li*, Mitarbeiter der chin esischen NGO* Globalization Monitor*, hielt im November 2009 vier Vorträge in Wien, der Steiermark und Oberösterreich.* Rubenia Guadalupe Delgado Figueroa *und* Merejilda Peñaloza Mora *reisten von April bis Mai 2010 durch Österreich, Deutschland, Tschechien und Malta.*

19 Handys Made-in-India*. Arbeits- und Lebensbedingungen in der Handy-Produktion in Südindien am Beispiel der Nokia-Sonderwirtschaftszone,* Südwind, Arbeiterkammer Wien und Cividep-India*, 2012 http://doku.cac.at/bericht_indien_handy_bsp_indien_120831.pdf ,* Arbeitsrecht in Zeiten der Krise, Südwind & CEREAL *2009: http://doku.cac.at/report_cereal.pdf*

20 *Gemeinsam mit den NGOs* EAP *(Tschechien),* WEED *(Deutschland),* CES *(Ungarn),* Karat *(Polen),* Setem *(Spanien),* SOMO *(Holland) arbeitete Südwind in einem EU-Projekt namens „Procure IT fair" über 3 Jahre zum Thema „Faire Beschaffung von IT": http://makeitfair.org/en/about-us/en/procure-it-fair*

21 *2012 erstellte* Südwind *die Publikation: „Die Welt im Handy. Materialien für die Bildungsarbeit. http://www.suedwind-agentur.at/start.asp?ID=250686, an Handreichungen zum Thema Elektroschrott arbeiten wir derzeit.*

22 *Weitere Informationen dazu im Artikel von* Annelie Evermann *bzw. unter: http://electronicswatch.org/de/*

CC BY

Andrea Ben Lassoued

Andrea Ben Lassoued leitet die Clean-IT-Kampagne für faire Arbeitsbedingungen in der Computerindustrie bei der entwicklungspolitischen Organisation Südwind. Sie beschäftigt sich schwerpunktmäßig mit sozial-fairer Beschaffung von IT und arbeitet mit anderen Organisationen am Aufbau der ersten internationalen Monitoring-Organisation für die Elektronikindustrie.

Sebastian Beschke

Die Abstimmung über den Geldbeutel

Konsumalternativen für eine fairere Elektronik

Die Berichte über die schlechten Arbeitsbedingungen bei der Elektronikherstellung und beim damit verbundenen Rohstoffabbau stellen unser Konsumverhalten in Frage. Bei vielen Menschen lautet der Reflex, auf den Kauf von Geräten, die unter solchen Bedingungen hergestellt wurden, fortan zu verzichten. Doch ein Boykott verbessert erst einmal nicht die Lebensbedingungen der betroffenen Arbeiter und Arbeiterinnen, gegebenenfalls macht er sie stattdessen arbeitslos. Gibt es einen Weg, diese Bedingungen – analog zur Fair-Trade-Bewegung – über einen bewussten Konsum zu verbessern? Zwei Projekte, die diese Möglichkeit ausloten und salonfähig machen möchten, werden hier vorgestellt.

Susanne Jordan kann von sich sagen, das erste Elektronikprodukt auf den Markt gebracht zu haben, bei dessen Herstellung explizit auf die Arbeitsbedingungen geachtet wurde. Das Produkt ist bewusst unspektakulär: es handelt sich um eine Computermaus. Dennoch flossen mehrere Jahre Arbeit in dieses Projekt namens *NagerIT*, vom Entwurf über die Beschaffung von Komponenten bis hin zum Zusammenbau.[1]

Maus von NagerIT. Foto: www.nager-it.de/maus

Wo bei der Herstellung der Maus welche Arbeitsschritte durchgeführt werden, ist online genau nachvollziehbar: Die komplette Lieferkette ist einsehbar, soweit sie überhaupt nachvollzogen werden konnte. Wo immer möglich, wurde dabei darauf geachtet, dass menschenwürdige Arbeitsstandards eingehalten werden – oft heißt dies: Produktion nicht in Fernost, sondern in Europa. Die Bestückung der Platine findet zum Beispiel in einer Werkstatt für psychisch kranke und behinderte Menschen in Regensburg statt.

Wer sich die Lieferkette anschaut, dem fallen aber auch zwei große Lücken auf. Zum einen sind dies spezialisierte Komponenten wie der Sensor-Chip oder auch – überraschenderweise – die Füße. Für sie konnte schlicht kein Zulieferer gefunden werden, der für menschenwürdige Arbeitsbedingungen garantieren wollte. Der Chip kommt von den Philippinen, die Füßchen aus China.

Ein dichter Nebel liegt zudem über der Rohstoffkette. Denn mit den Herstellern von Komponenten kann man noch telefonieren, sie ggf. besuchen und sich von den Bedingungen vor Ort überzeugen. Wo deren Rohstoffe herkommen, lässt sich jedoch im Allgemeinen nicht sicherstellen, und je nach Bezugsweg ist es selbst dem Hersteller nicht bekannt. Sie werden über Rohstoffhändler bezogen, welche einen Rückschluss auf die Ursprungsorte nicht ermöglichen. Die Grafik der weit verzweigten Lieferkette[2] schafft auf jeden Fall eine Vorstellung von der Größenordnung der Aufgabe, tatsächlich jeden einzelnen Schritt bei der Herstellung eines Produkts in Betracht ziehen zu wollen.

Der Herstellung von Smartphones widmet sich hingegen das Projekt *Fairphone* der niederländischen *Waag Society*.[3] Das gleichnamige Produkt lässt sich seit Frühjahr 2013 vorbestellen, und die Auslieferung soll im Dezember beginnen. Zu haben ist ein Smartphone der Mittelklasse, das eben nicht durch seine technische Spezifikation, sondern durch ein durchdachtes, auf Nachhaltigkeit ausgerichtetes Design seine Käufer finden soll.

Fragt man danach, was beim Fairphone denn jetzt konkret fair ist, findet man erstaunlich wenig: Am sichtbarsten ist noch die Beteiligung an der *Conflict-Free Tin* Initiative sowie *Solutions for Hope*, welche konfliktfreies Zinn aus der Demokratischen Republik Kongo zertifizieren. Mit Fairness hat das aber noch nichts zu tun; Kinderarbeit und gefährliche Arbeitsbedingungen kommen auch hier zum Einsatz. Von Fair-Trade-zertifiziertem Gold ist die Rede, und mit der Fabrik in China, die das Handy zusammenbaut, steht man immerhin in einem Assessment-Prozess. Einen umfassenden Überblick über die verwendeten Rohstoffe hatte Fairphone im November noch nicht veröffentlicht, jedoch für die Zukunft versprochen.

Sebastian Beschke

Sebastian Beschke ist Doktorand in Informatik an der Universität Hamburg. Seit dessen Gründung ist er im Arbeitskreis *Faire IT Hamburg* aktiv.

Betrachtet man demgegenüber die fast unüberschaubare Menge von Rohstoffen und Komponenten, die ein Smartphone ausmachen, wird klar, dass Fairphone hier noch ganz am Anfang steht. Kein Wunder, dass sich Fairphone nicht in erster Linie als Smartphone-Hersteller versteht, sondern eine Plattform bereitstellen möchte: Verschiedene in der Elektronikherstellung involvierte Akteure sollen zusammenkommen und kooperieren. Das Telefon dient vor allem dem Beweis, dass dieser Markt für nachhaltige Elektronik tatsächlich vorhanden ist.

Smartphone von Fairphone.
Foto: http://www.flickr.com/photos/fairphone

Diesen Beweis scheinen die beiden erwähnten Projekte erbracht zu haben: NagerIT wurde vom Medieninteresse geradezu überrannt, und Fairphone konnte seine erste Fertigungscharge von 25 000 Stück durch Vorbestellungen finanzieren. Betrachtet man, dass es sich nicht um Weltkonzerne, sondern um personell sehr überschaubare Initiativen handelt, ist das ein beachtlicher Erfolg. Letztlich könnte er – so das Ziel beider Projekte – größere Hersteller davon überzeugen, faire(re) Produkte in ihr Sortiment aufzunehmen.

Wie könnte und sollte die Entwicklung nun weitergehen? Um fairere Produkte effektiv und glaubhaft als solche bewerben zu können, braucht es standardisierte Prozesse und Siegel, wie es die ebenfalls in diesem Heft vorgestellte *TCO*-Zertifizierung im Ansatz demonstriert. Diese, gemeinsam mit der von den Pionierprojekten geleisteten Vorarbeit, erleichtert Herstellern den Einstieg in die fairere Produktion.

NagerIT und Fairphone werden beide ihre jeweiligen Plattformen voranbringen. NagerIT versucht weiterhin unermüdlich, weitere fair hergestellte Komponenten für die Maus aufzutreiben – aktuell geht es zum Beispiel um USB-Kabel. Längerfristig soll daraus eine Komponentendatenbank entstehen, die es anderen Projekten ermöglicht, an fair hergestellte Bauteile zu kommen. Ebenso will Fairphone weitestmöglich Informationen über seine Lieferkette veröffentlichen und es so anderen Herstellern ermöglichen, von den Erfahrungen Fairphones zu profitieren.

Diese Transparenz, die im völligen Gegensatz zum sonst üblichen Betrieb in der IT-Branche steht, ist essenziell, da sie genau die Synergien schafft, die das faire Produzieren erst möglich machen. Wollte jeder Hersteller seine eigene Lieferkette bis ins Detail untersuchen, wäre dies teuer und aufwändig. Teilt man diese Informationen, statt sie als Geschäftsgeheimnis zu behandeln, schafft man nicht nur Glaubwürdigkeit, sondern erhöht auch die Effizienz. Es ist zu wünschen, dass die Projekte zur fairen IT dazu beitragen, dass diese Transparenz zunehmend von den Unternehmen als nützlich empfunden und von den Verbrauchern und Verbraucherinnen eingefordert wird.

Anmerkungen

1 *Mehr Informationen zur fairen Maus, inklusive Bestellung, gibt es unter https://www.nager-it.de/. Die Maus kostet 29,90 Euro plus Versand (Stand September 2013). Zu empfehlen ist auch ein Blick auf die Lieferkette: https://www.nager-it.de/static/pdf/lieferkette.pdf.*

2 *https://www.nager-it.de/static/pdf/lieferkette.pdf"*

3 *Mehr Informationen zu Fairphone gibt es unter http://www.fairphone.com/. Das Telefon ist für 325,00 € vorzubestellen und soll im Dezember 2013 ausgeliefert werden (Stand September 2013).*

CC BY

Susanne Brügelmann

„Es gibt Möglichkeiten andere Wege zu gehen"

Interview mit Fujitsu Deutschland

FIfF: Sehr geehrte Frau Brügelmann, erkennen Sie eine Nachfrage nach fairer hergestellten Geräten? Spüren Sie die zunehmende Medienpräsenz dieses Themas?

Susanne Brügelmann: Generell nehmen wir folgenden Paradigmenwechsel wahr: Im Umfeld von Green IT fließt die soziale Komponente zunehmend in die Kaufentscheidung mit ein, zuzüglich zu Fragen nach der Energieeffizienz und der Reduktion des CO_2-Ausstoßes. Damit sind nun auch Produktions- und Arbeitsbedingungen in Bezug auf unsere eigenen Werke und auch auf unsere Lieferketten ein wichtiges Thema.

Keine der Markenfirmen hat die Herkunft der Rohstoffe in den Geräten veröffentlicht. Was sind die Probleme, und wie könnte man sie Ihrer Meinung nach überwinden?

Das hängt mit der Komplexität eines Produktlebenszyklus zusammen. Nehmen wir als Beispiel einen Computer: Auf den ersten Blick scheint dieser sich aus einer übersichtlichen Zahl von Komponenten zusammenzusetzen – der Anschein trügt jedoch. So setzt sich ein PC aus unterschiedlichen Komponentengruppen zusammen, die ihrerseits aus einer Vielzahl von Kleinteilen bestehen. Noch komplexer ist die Situation bei Servern. Daher sind *Lifecycle Assessment Analysen* selbst innerhalb einer Pro-

duktfamilie sehr aufwändig. Bei Fujitsu kommt zudem noch ein sehr breites Portfolio hinzu, das gemäß unserem Prinzip *Think Global – Act Local* geographisch divergieren kann. Konkret heißt das, dass man je nach Marktanforderung unterschiedliche Produktlinien vorfindet.

Meiner Einschätzung nach lässt sich dieses Thema nur im Rahmen eines integrierten Reportings, gestützt auf internationale Standards, angehen.

Man sagt immer, alle Hersteller wären gleich, weil sowieso jeder in China bei Foxconn oder ähnlichen Kontraktherstellern fertigen lässt. Sehen Sie das auch so? Gibt es Möglichkeiten, sich von der Konkurrenz positiv abzusetzen?

Nein, das sehen wir nicht so. Mit Sicherheit hat die Kommodifzierung Einzug in die IT-Industrie gehalten und die Lieferantenlandschaft weltweit verschlankt. Dennoch gibt es nach wie vor Möglichkeiten, andere Wege zu gehen – und genau das machen wir. So haben wir beispielsweise viele eigene Werke. Allen voran unser Werk in Augsburg. Oder unser Forschungs- und Entwicklungsstandort Paderborn mit eigenem Recycling-Center. Zudem gibt es in Japan eigene Werke, in denen Fujitsu-Produkte und Komponenten hergestellt werden.

Von der Fertigung in Deutschland ist wenig bekannt. Welche Produktionsschritte finden in Augsburg statt und welchen Anteil hat dies innerhalb Ihrer gesamten Produktion von PCs? Wäre es in China nicht günstiger?

Fujitsu setzt stark auf den Standort Deutschland und das Werk in Augsburg. Wir sind das einzige IT-Unternehmen dieser Größe, das noch in Deutschland fertigt. So wird beispielsweise die Produktlinie ESPRIMO PC mit Mainboard komplett in Augsburg gefertigt. Das garantiert kurze Wege.

Darüber informieren wir auch regelmäßig und bieten zudem Werksführungen an. Diese werden beispielsweise von unseren Partnern gerne wahrgenommen, aber auch von Schulen oder Universitäten. Zudem informieren wir im Internet darüber.[1] Dass über die Fertigung wenig bekannt ist, stimmt so also nicht.

Haben Sie eine Erklärung, warum keiner der großen Hersteller, Fujitsu eingeschlossen, tut, was FairPhone oder Nager-IT vormachen? Warum nutzt niemand die vorhandenen Möglichkeiten zur faireren Herstellung offensiv als Verkaufsargument?

Fujitsu stellt sich immer wieder neuen Herausforderungen mit alternativen Designkonzepten, durch die natürliche Materialien und bio-basierte Kunststoffe zum Einsatz kommen – und das kommunizieren wir auch.

Fujitsu Recycling-Center in Paderborn
Quelle: Fujitsu Technology Solutions (FTS)

Erstes Beispiel: Das Öko-Keyboard. Das Fujitsu KBPC PX ECO Keyboard besteht zu 45 Prozent aus Biokunststoff, verfügt über ein PVC-freies USB-Kabel und eine halogenfreie Platine. Die Basis der Handauflage ist ARBOFORM® (Lignin), ein Abfallprodukt der Papierindustrie. Das Unterteil besteht aus BIOGRADE®, einem Grundmaterial der Papierindustrie. Damit hilft es, auf Öl basierende Produkte wie Plastik und PVC aus der Fabrikproduktion zu entfernen.

Zweites Beispiel: Die Öko-Maus. Das Gehäuse der Fujitsu-Maus M440 ECO besteht aus BIOGRADE®. Weiterhin verfügt diese Maus über ein PVC-freies USB-Kabel sowie eine halogenfreie Platine. Weiterer Pluspunkt: Durch den Einsatz biologisch abbaubarer Materialen treibt Fujitsu seine umweltverträgliche Produktion weiter voran und reduziert den CO2-Ausstoß während der Herstellung. Hinzu kommt, dass das Mausgehäuse zu 100 Prozent biologisch abbaubar ist und somit für deutlich weniger Müll sorgt. Das Beste dabei, die Öko-Maus kostet nicht mehr als herkömmliche Computermäuse.

Was ist Ihr nächster Schritt in Richtung einer faireren Herstellung der Geräte?

Die Fujitsu Group ist Mitglied des Netzwerks *United Nations Global Compact*. Durch das Einhalten der Prinzipien des Global Compact in den Bereichen Menschenrechte, Arbeitsnormen, Umweltschutz und Korruptionsbekämpfung sowie die aktive Umsetzung von CSR-Initiativen fördert Fujitsu als globales Unternehmen verantwortungsbewusstes Management und trägt so zu einer nachhaltigen Gesellschaft bei. Aus diesem Grund hat FTS einen Verhaltenskodex für Zulieferer eingeführt, den Sup-

Susanne Brügelmann

Susanne Brügelmann ist Senior Product Marketing Manager Green IT & Corporate Social Responsibility bei Fujitsu Technology Solutions (FTS).

plier Code of Conduct. Dieser verdeutlicht unser Engagement für ethisches und verantwortungsvolles Handeln und die damit verbunden Verpflichtungen, die wir unseren Zulieferern auferlegen.

Zudem sind wir derzeit dabei, ein umfassendes globales Compliance-Programm auszurollen, das faire Betriebs- und Geschäftspraktiken einschließt.[2]

Das ist leider etwas undurchsichtig. Ich persönlich würde gerne das fairere Produkt von dem verantwortungsvolleren Hersteller kaufen, aber ein Vergleich ist schwierig. Wie können wir gemeinsam zu mehr Transparenz kommen, die für die Einkäufer und Konsumenten nützlich ist?

Mit unserem Siegel *proGREEN Selection* kennzeichnen wir besonders umweltfreundliche und energieeffiziente Produkte von Fujitsu. Damit sind sie auf einen Blick zu erkennen. Auf unserer Website finden Interessierte außerdem zu jedem unserer Produkte detaillierte Informationen – über Produktbeschreibungen mit technischen Details, bis hin zu Datenblättern und Zertifikaten. Im Internet finden Einkäufer und Konsumenten also wichtige Informationen, um unterschiedliche Produkte und Hersteller zu vergleichen.

Was können aus Ihrer Sicht die kritischen Konsumenten tun?

Ganz klar: Sie müssen im Einklang mit ihren Vorstellungen handeln und die Kaufentscheidung danach richten, nicht nur nach dem Preis. Das zeigt dann auch den Unternehmen, dass sozial- und umweltverträgliche Produktion von den Konsumenten gewünscht ist und ein entsprechender Markt existiert – und führt hoffentlich langfristig zu einem Umdenken.

Anmerkungen

1 *Siehe http://www.fujitsu.com/de/about/fts/environment-care/, http://www.fujitsu.com/de/about/fts/environment-care/production/, http://www.fujitsu.com/de/about/fts/environment-care/products/*

2 *Weiterführende Informationen unter: http://www.fujitsu.com/global/about/responsibility/*

Michael Kaminski-Nissen

„Letztendlich entscheiden die Kunden"

Interview mit Hewlett-Packard Deutschland

FIfF: Sehr geehrter Herr Kaminski-Nissen, erkennen Sie eine Nachfrage nach fairer hergestellten Geräten? Spüren Sie die zunehmende Medienpräsenz dieses Themas?

Michael Kaminski-Nissen: Seit einigen Jahren verzeichnet die Diskussion um fair hergestellte ITK-Geräte in der Tat eine Zunahme. Dies resultiert sicher nicht zuletzt auch aus einem wachsenden Interesse der Medien, Aktionen von NGOs und ähnlichem. Ungeachtet dessen berichtet HP bereits seit Jahren regelmäßig in seinem *Global Citizenship Report*[1] unter dem Titel *Supply Chain Responsibility* proaktiv und detailliert über Maßnahmen, Ziele und Erreichtes bezüglich Lieferketten und Sozialverträglichkeit.[2]

Allerdings muss man realistischerweise auch sehen, dass bei der Beschaffung von ITK-Geräten sowohl für den privaten wie auch für den geschäftlichen Gebrauch eine Vielzahl von Kriterien eine Rolle spielen, beginnend bei den technischen und nutzungsrelevanten Eigenschaften über den Preis bis hin zu Aspekten der Umweltverträglichkeit und eben auch sozialverträglichen Lieferketten etc. Letztendlich entscheiden dann aber die Kunden über die Priorisierung dieser Kriterien bei ihrer jeweils individuellen Kaufentscheidung. Und daran orientieren sich wiederum die Schwerpunkte und der Umfang einer produktbezogenen und auch mengenmäßig durch die Kunden verarbeitbaren Kommunikation durch Hersteller wie HP. Das spiegelt sich auch in den individuellen Anfragen zu Umwelt und Nachhaltigkeit wider.[3]

Keine der Markenfirmen hat die Herkunft der Rohstoffe in den Geräten veröffentlicht. Was sind die Probleme, und wie könnte man sie Ihrer Meinung nach überwinden?

HP hat im April 2013 als erstes IT-Unternehmen weltweit die *3TG smelter list*[2] der in seinen Lieferketten aktiven 195 Schmelzhütten veröffentlicht, die die so genannten *Critical Minerals* Gold, Tantal, Wolfram und Zinn verarbeiten und ganz am Beginn der Produktlieferkette stehen.[4]

HP hat eine Liste der Schmelzereien in der eigenen Lieferkette veröffentlicht. Quelle: Hewlett Packard

Aber wissen Sie auch, woher die Schmelzhütten ihre Mineralien und Erze beziehen?

Diese Informationen sind für die Schmelzhütten wettbewerbs- bzw. geschäftskritisch und werden daher nicht öffentlich publiziert.

Man sagt immer, alle Hersteller wären gleich, weil sowieso jeder in China bei Foxconn oder ähnlichen Kontraktherstellern fertigen lässt. Sehen Sie das auch so? Gibt es Möglichkeiten, sich von den Mitbewerbern positiv abzusetzen?

HP arbeitet seit mehr als 12 Jahren bei und mit seinen Lieferanten an einer kontinuierlichen Verbesserung von Sozial- und Umweltstandards. Diese sind bereits vor vielen Jahren eine wesentliche Grundlage für den inzwischen weltweit anerkannten, branchenspezifischen Verhaltenskodex *Electronics Industry Code of Conduct* der *Electronic Industry Citizenship Coalition*[5] gewesen.

Eine Überprüfung dieser Sozial- und Umweltstandards erfolgt seit Jahren durch proaktive, regelmäßige Audits, die falls notwendig auch aktive Verbesserungsmaßnahmen nach sich ziehen. Darüber hinaus werden konkrete, z. B. über die Medien oder durch NGOs bekannt gemachte kritische Vorkommnisse bei Kontraktherstellern, die auch für HP relevant sind, kurzfristig analysiert. Es folgen bei Bedarf durch HP auch individuelle Maßnahmen zur Behebung möglicher Missstände. HP schafft zu dem Thema seit Jahren eine hohe Transparenz und macht eine detaillierte Liste seiner wichtigsten Lieferanten sowie die zusammengefassten Auditergebnisse und entsprechend umgesetzte Maßnahmen für jeden Interessierten öffentlich zugänglich.[2]

Haben Sie eine Erklärung, warum niemand der großen Hersteller tut, was FairPhone oder Nager-IT vormachen? Warum nutzt niemand die vorhandenen Möglichkeiten zur faireren Herstellung offensiv als Verkaufsargument?

Kleinere, eher lokal produzierende und verkaufende Unternehmen, deren Produktportfolio sich auf ein oder zwei Produkte beschränkt und deren wesentliche Produktbotschaft die faire Herstellung ist, verfolgen einen interessanten und guten Ansatz. Allerdings sind diese lokalen Initiativen schwerlich mit den komplexen Lieferketten globaler Hersteller wie HP mit über 10 000 aktiven Produkten für Kunden in rund 170 Ländern weltweit zu vergleichen. Während die Klientel dieser lokalen Hersteller sehr spezifisch ist und mit dem einen Verkaufsargument der fairen Herstellung adressiert wird, erwarten die privaten und geschäftlichen Kunden von HP für ihre Kaufentscheidung, wie oben bereits erläutert, eine Vielzahl von Kriterien, beginnend bei den technischen und nutzungsrelevanten Eigenschaften über den Preis bis hin zu Aspekten der Umwelt- und Sozialverträglichkeit. Mit anderen Worten: Auch ein Anbieter wie HP nutzt das Verkaufsargument der fairen Herstellung durchaus, muss dies aber entsprechend den aktuellen Anforderungen aller seiner Kunden angemessen im umfangreichen und vielschichtigen Kriterienkatalog platzieren.

Übrigens müssen im ITK-Bereich auch lokal produzierende Unternehmen die wesentlichen Elektronikkomponenten ihrer Produkte meist von den großen Lieferanten z. B. in Asien beschaffen. Dabei ist der Druck, den sie auf die Lieferanten ausüben können, um wirklich fair produzierte Ware zu bekommen, sicher kaum vergleichbar mit den Möglichkeiten, wie sie oben beispielsweise für HP dargestellt worden sind.

Was ist Ihr nächster Schritt in Richtung einer faireren Herstellung der Geräte?

Es gibt zahlreiche und vielfältige Schritte, mit denen HP eine fairere Herstellung seiner Produkte vorantreibt. Zielvorgaben für 2013 sind beispielsweise eine intensivere und häufigere Prüfung der Einhaltung von Arbeitszeitmesskriterien sowie die Schulung von 90 Prozent der Endfertigungslieferanten in China bezüglich der HP-Arbeitsrichtlinien. Im *HP 2012 Global Citizenship Report* gibt es am Ende des Kapitels *Supply Chain Responsibility* eine Übersicht sowohl über nächste Schritte und Ziele wie auch über Ergebnisse.[6]

Was können aus Ihrer Sicht die kritischen Konsumenten tun?

Grundsätzlich ist hier zu unterscheiden zwischen dem privaten Konsumenten und der Beschaffung, die für geschäftliche Zwecke erfolgt.

Der private Konsument, also jeder von uns, sollte für seinen Kauf Informationsquellen nutzen, wie sie z. B. oben für HP genannt wurden, und so auf Anwender- wie auf Herstellerseite den Einsatz fairer hergestellter Produkte vorantreiben.

Für die Beschaffung im geschäftlichen Bereich gelten einerseits dieselben Informationsquellen zur Vorbereitung. Andererseits werden heute bereits zunehmend im Rahmen von Ausschreibungen auch Fragen zu den Lieferketten, sozialen Kriterien etc. gestellt.

Darüber hinaus gibt es für den Bereich der öffentlichen Beschaffung seit August 2013 eine zwischen BITKOM und dem Beschaffungsamt im Bundesministerium des Inneren erarbeitete Mustererklärung, die sich an den so genannten Kernarbeitsnormen der Internationalen Arbeitsorganisation ILO orientiert.[7]

Anmerkungen

1 *Siehe www.hp.com/globalcitizenship*

2 *Zu Themen der Zuliefererverantwortung siehe www.hp.com/go/supplychain*

Michael Kaminski-Nissen

Michael Kaminski-Nissen ist seit Ende 2007 bei Hewlett-Packard als Umwelt-Manager für Deutschland und die Schweiz tätig und in dieser Funktion intern wie extern in Deutschland der zentrale Ansprechpartner für alle umweltrelevanten Fragen zum Produkt- und Lösungsportfolio von HP.

3 *Anfragen zu Umwelt und Nachhaltigkeit können bei HP an folgende eMail-Adresse geschickt werden: umwelt@hp.com*

4 *Siehe die Presseerklärung vom April diesen Jahres, mit der bekanntgegeben wurde, dass HP erstmals eine Liste mit allen Schmelzhütten in seiner Lieferkette veröffentlicht: http://www8.hp.com/us/en/hp-news/press-release.html?id=1391397*

5 *Siehe www.eicc.info*

6 *Zu finden ab Seite 101 im Report, der unter www.hp.com/go/report verfügbar ist.*

7 *Die Mustererklärung kann unter http://www.nachhaltige-beschaffung.info/SharedDocs/Kurzmeldungen/DE/2013/BITKOM_Bescha_Soziale-Nachhaltigkeit_ITK.html abgerufen werden.*

Cornelia Heydenreich

Freiwilligkeit und Verbindlichkeit: Unternehmensverantwortung am Beispiel der IT-Industrie

Sorgen Computerproduzenten freiwillig dafür, dass in ihren Geräten keine Rohstoffe verbaut werden, deren Abbau kriegerische Konflikte anheizt oder müssen Staaten durch Gesetze dafür Sorge tragen? Funktioniert es, wenn Mobiltelefonhersteller über freiwillige Verhaltenskodizes ihren Zulieferern vorschreiben, dass die ArbeiterInnen nicht unter ausbeuterischen Bedingungen ihre Handys zusammenbauen sollen oder müssen sie über Gesetze in den Produktionsländern und in ihren Heimatstaaten dazu verpflichtet werden? Seit vielen Jahren gibt es eine Diskussion darum, was Unternehmen freiwillig tun und was ihnen durch Gesetze vorgeschrieben werden muss.

Unternehmensverbände setzen traditionellerweise auf Freiwilligkeit und wollen zusätzliche Regelwerke vermeiden. Und auch die bisherige Bundesregierung unterstützte vor allem freiwillige Ansätze im Rahmen der sogenannten *Corporate Social Responsibility, CSR*.

Umfassende Studie zeigt Grenzen der Freiwilligkeit

Allerdings reicht das freiwillige Engagement allein nicht aus, um den bestehenden gesellschaftlichen Herausforderungen angemessen zu begegnen. Dies ist das Ergebnis einer Studie, deren Ergebnisse 17 europäische Forschungsinstitute im September 2013 vorgestellt haben[1]. Unter der Leitung des Öko-Institutes hatten sie fast vier Jahre lang die Auswirkungen von *CSR* auf die Gesellschaft untersucht. Ihr Projekt *IMPACT* kam zu dem Ergebnis, dass die Auswirkungen von *CSR* nicht groß genug sind, um die gesetzten politischen Nachhaltigkeitsziele zu erreichen. Die Forscher stellten zwar Verbesserungen fest, allerdings nur von unter einem Prozent. Ihre Schlussfolgerung ist deshalb, dass der Effekt von CSR nicht ausreicht, um bei Arbeitsbedingungen und der Umweltsituation substanzielle Verbesserungen herbeizuführen.

Interessant ist zudem das Ergebnis, dass eine gesetzliche Rahmensetzung nicht das freiwillige Engagement einschränkt. Derart argumentieren insbesondere Unternehmensverbände immer wieder, die gesetzliche Regelungen u. a. mit der Begründung ablehnen, dass Unternehmen dann nur noch so viel wie gefordert und nicht mehr machen würden. Die Forscher entdeckten jedoch gerade in stark regulierten Themenfeldern wie bei gefährlichen Chemikalien oder bei Gesundheit und Arbeitsschutz, dass Unternehmen freiwillig über die gesetzlichen Regelungen hinausgehen. Ebenso stellten sie fest, dass Unternehmen in Erwartung von zukünftigen Gesetzgebungen aktiv werden. In nicht regulierten Bereichen tun Unternehmen dagegen mitunter gar nichts.

Diese Ergebnisse decken sich auch mit Erfahrungen aus dem IT-Sektor. So betonten die führenden Elektronikfirmen im Jahr 2007 auf Anfrage von *makeITfair*, einem europäischen Projekt zur gesellschaftlichen Verantwortung der IT-Industrie, dass sie für den Abbau der Rohstoffe, die in ihren Computern und Han-

Vom Kontrollieren und Einpacken der Microsoft-Mäuse erschöpfte jugendliche Arbeiterinnen der Firma NYE (China) in der Pause
Foto: © Institute for Global Labour and Human Rights, 2010

dys verarbeitet werden, nicht verantwortlich seien. Nach mehreren Rohstoffstudien von *makeITfair* und einem Dialogprozess mit der Industrie begann ein Umdenken und erste Pilotprojekte entstanden. Wirkliche Dynamik kam aber erst auf, nachdem die USA im Jahr 2010 den sogenannten *Dodd-Frank-Act* verabschiedet hatten.

Handyproduktion: Verbesserungen sichtbar, aber unzureichend

Auch bei den Arbeitsbedingungen im Produktionsprozess sind Veränderungen aufgrund von unternehmerischen Initiativen festzustellen, die jedoch bei weitem nicht ausreichen. Im Jahr 2008 veröffentlichte *makeITfair* eine Studie über die schlechten Arbeitsbedingungen in Zulieferfabriken von Handyfirmen in China und den Philippinen. Junge Frauen arbeiteten ohne Gesichtsschutz oder Handschuhe in den Fabriken und atmeten gefährliche Dämpfe an den schlecht gelüfteten Arbeitsplätzen ein. Seitdem hat sich einiges verändert, wie eine Folgestudie bei einigen der untersuchten Firmen in China, die Ladegeräte an Nokia, Motorola, Samsung und LG liefern, im Jahr darauf zeigte. Ein neuer Besitzer übernahm die Fabriken und investierte 2,5 Millionen US-Dollar, vor allem in angemessene Sicherheitsausrüstung sowie Trainings zur Arbeitssicherheit, um die Gesundheit der ArbeiterInnen zu schützen.

In einer anderen Studie untersuchte *makeITfair* die Produktion von Spielekonsolen, MP3-Playern und Smartphones bei vier Zulieferfirmen in China im Jahr 2009 und veröffentliche Anfang 2011 eine Folgestudie. In den Fabriken sind die Löhne seit der ersten Studie zumindest geringfügig erhöht worden und es werden weniger Schülerpraktikanten beschäftigt. Die diskriminierenden Hepatitis-B-Tests, nach denen erkrankte BewerberInnen gar nicht erst eingestellt wurden, sind inzwischen abgeschafft. Aber gravierende Probleme bestehen auch weiterhin: Die Löhne liegen trotz der Lohnerhöhungen immer noch unter dem Existenzminimum, die ArbeiterInnen müssen massive Überstunden leisten und sie haben weiterhin keine gewerkschaftliche Vertretung.

Die beiden Beispiele zeigen, dass Verbesserungen bei den Arbeitsbedingungen durch Initiativen auf Unternehmensebene möglich sind – allerdings sind sie häufig begrenzt auf Arbeitssicherheit und Gesundheitsschutz. Viel zu oft gibt es zudem nur dort Fortschritte, wo Initiativen wie *makeITfair* zuvor den Finger in die Wunde legten. Grundlegende Veränderungen wie Gewerkschaftsfreiheit und faire Einkaufspraktiken, also zum Beispiel eine gerechte Preisgestaltung der Markenunternehmen bei der Auftragsvergabe, fehlen dagegen. Aber erst damit könnten wesentliche strukturelle Probleme wie die extrem hohen Überstunden und die zu geringen Löhne behoben werden. Der Wettbewerb im IT-Sektor ist extrem hoch und ein einzelnes Unternehmen kommt bei preisrelevanten Themen an seine Grenzen. Selbst einige Unternehmensvertreter unterstützen daher, dass für bestimmte Fragen wie Existenz-sichernde Löhne gesetzliche Rahmensetzungen erforderlich sind.

Intelligenter Mix

Das *Ob* von politischen Rahmensetzungen für die gesellschaftlichen Auswirkungen des weltweiten Handelns von Unternehmen steht also zunehmend nicht mehr in Frage, nun geht es jedoch um das *Wie*. Was konkret sollte geregelt werden, auf welcher Ebene und wie sollte die Regelung konkret aussehen? Der große Wurf, alles in einem umfassenden Dokument auf UN-Ebene zu regeln, ist seit den 2003 gescheiterten *UN-Normen für die Verantwortlichkeit transnationaler Konzerne und anderer Wirtschaftsunternehmen im Hinblick auf die Menschenrechte* zunächst aus dem Blickfeld geraten. Mit den UN-Leitprinzipien für Wirtschaft und Menschenrechte aus dem Jahr 2011 hat der Menschenrechtsrat der Vereinten Nationen jedoch ein Rahmenwerk verabschiedet, das einerseits die staatlichen Schutzpflichten betont und andererseits die unternehmerische Verantwortung herausstellt. Es geht um den sogenannten „intelligenten Mix" aus freiwilligen und verbindlichen Rahmensetzungen. Auf nationaler und regionaler Ebene, z. B. im Rahmen der europäischen Union, kommt es nun auf eine Umsetzung der UN-Leitprinzipien an. Bei den *Staatenpflichten* geht es um Fragen wie die Offenlegung der Auswirkungen unternehmerischen Handelns, um öffentliche Beschaffung oder um Außenwirtschaftsförderung, aber auch um Zugang zu Beschwerdemöglichkeiten über Gerichte oder über die OECD-Leitsätze für multinationale Unternehmen. Bezüglich der *unternehmerischen Verantwortung* etablieren die UN-Leitprinzipien ein neues Konzept, die menschenrechtliche Sorgfaltspflicht (*Due Diligence*). Anstatt für die angerichteten menschenrechtlichen Schäden im Nachhinein an den Pranger gestellt zu werden, sollen Unternehmen diesen frühzeitig vorbeugen.

Allerdings versäumen es die UN-Leitprinzipien, eine staatliche Rahmensetzung für die menschenrechtliche Sorgfaltspflicht der Unternehmen zu verankern. Hier müssen die UN-Leitprinzipien aus Sicht von Nichtregierungsorganisationen weiterentwickelt werden, zumindest in der Umsetzung. Eine umfangreiche Studie[2]

Cornelia Heydenreich

Cornelia Heydenreich ist seit 2001 bei Germanwatch im Bereich Unternehmensverantwortung tätig. Sie ist Mitbegründerin des CorA-Netzwerkes (Netzwerk für Unternehmensverantwortung in Deutschland) und dort u. a. im Koordinationskreis aktiv. Seit 2007 koordiniert sie die Aktivitäten in Deutschland des europäischen Projektes makeITfair zu menschenrechtlichen, sozialen und ökologischen Auswirkungen der IT-Industrie auf Entwicklungsländer.

im Auftrag des europäischen Netzwerkes für Unternehmensverantwortung, *ECCJ*, und des amerikanischen Pendants *ICAR*, entwickelt zahlreiche Vorschläge, wie diese menschenrechtlichen Sorgfaltspflichten gesetzlich verankert werden könnten.

Auf EU-Ebene gibt es derzeit eine konkrete Initiative, menschenrechtliche Sorgfaltspflichten zu regulieren. Im Dezember wird ein Vorschlag der EU-Kommission erwartet, wie Unternehmen ihre menschenrechtliche Sorgfaltspflicht walten lassen sollen, wenn sie Rohstoffe aus Konfliktgebieten beziehen. Dies würde auch die IT-Industrie betreffen, die zum Beispiel Tantal und Zinn verbaut, die in der DR Kongo seit Jahren einen kriegerischen Konflikt anheizen. Hier eine intelligente Rahmensetzung zu schaffen, würde bedeuten, dass sie einerseits eine Lösung für die Probleme vor Ort schafft, ohne gravierende Nebeneffekte zu haben, und andererseits keine unrealistische Last für Unternehmen darstellt. Aber nicht alles, was Unternehmen oder ihre Verbandsvertreter als Unmöglichkeit darstellen, ist in der Praxis wirklich nicht zu leisten. So behaupteten die Elektronikunternehmen noch vor wenigen Jahren, sie könnten die Herkunft ihrer Rohstoffe nicht zurückverfolgen. Mit dem Dodd-Frank-Act sind sie nun dazu verpflichtet und die Praxis zeigt: es ist möglich, wenn auch mit zusätzlichem Aufwand verbunden.

Anmerkungen

1 Öko-Institut e. V.: Freiwilliges CSR-Engagement von Unternehmen reicht nicht aus, Pressemitteilung 17.9.2013 (*http://www.oeko.de/presse/pressemitteilungen/dok/1573.php*)

2 *http://www.corporatejustice.org/IMG/pdf/human_rights_due_diligence-the_role_of_states-2.pdf*

CC BY

Annelie Evermann

Geht nicht – ist nicht?

Neue Ansätze für eine sozial verantwortliche öffentliche Beschaffung von IT-Produkten

Öffentliche Verwaltungseinheiten sind Großabnehmer von IT-Hardware. Daher setzen sich WEED e. V. *und andere zivilgesellschaftliche Organisationen schon lange dafür ein, dass Länder, Gemeinden, Universitäten und andere öffentliche Beschaffungsstellen ihre Einkaufsmacht nutzen, um die ausbeuterischen Arbeitsbedingungen in der IT-Produktion zu verändern. Doch wie fordert man soziale Bedingungen, wenn es noch kein IKT-Produkt gibt, das diese Kriterien erfüllt? Der Artikel geht verschiedenen neuen Ansätzen für eine sozial verantwortliche öffentliche IT-Beschaffung nach und stellt eine neue Monitoring-Organisation,* Electronics Watch*, vor.*

Die Produktion von Hardware in der Informations- und Kommunikationstechnologie (IKT) ist entlang der gesamten Lieferkette von ausbeuterischen Arbeitsbedingungen geprägt. Seit *Apple* 2010 durch eine Reihe von Selbstmorden überlasteter ArbeiterInnen beim chinesischen Zulieferer *Foxconn* in die Schlagzeilen geriet, ist das inzwischen jedenfalls der politisch interessierten Öffentlichkeit bekannt.

Längst steht nicht mehr nur Apple im Fokus der Kritik. Davon abgesehen, dass der als Apple-Zulieferer bekannte Konzern *HonHai/Foxconn* ebenso *Dell*, *HP*, *IBM* und andere beliefert: Die Arbeitsbedingungen sind in den Produktionshallen der anderen Zulieferer und Sublieferanten nicht weniger kritisch.

Die Probleme in der Computerindustrie variieren zwar je nach Standort; weltweit verbreitet sind jedoch die hohe Jobunsicherheit, niedrige Löhne, extensive Arbeitszeiten und unbezahlte Überstunden sowie ein höchst gewerkschaftsfeindliches Verhalten vieler Unternehmen. Die Arbeitsschutzmaßnahmen sind oft unzureichend, obwohl die ArbeiterInnen in der Produktion mit teils hochgiftigen Stoffen in Kontakt kommen. Hier nur einige aktuelle Beispiele:

Samsung wurde jüngst von der brasilianischen Regierung verklagt: Die Arbeitsbedingungen in einem Samsung-Werk in Manaus/Brasilien seien gesundheitsschädlich und würden z. B. mit Schichten bis zu 15 Stunden am Tag gegen bestehendes Arbeitsrecht verstoßen.

Auch der chinesische Zulieferer *Pegatron*, der für eine große Zahl namhafter Elektronikkonzerne wie Dell, Apple, Microsoft und HP produziert, steht in der Kritik. Laut *China Labor Watch* verstößt Pegatron massiv gegen internationales und chinesisches Arbeitsrecht. Die 70 000 ArbeiterInnen, darunter auch PraktikantInnen und Minderjährige, arbeiten unter gesundheitsgefährdenden Bedingungen, leisten permanent Überstunden und werden unzureichend bezahlt.

China Labor Watch deckte auch auf, dass der *SHARP*, *TCL* und *HTC* beliefernde chinesisch-taiwanesische Zulieferer *Jiangxi Lianchuang Electronics* Kinder im Alter von 12 bis 14 Jahren beschäftigt. Laut ihrem Bericht leisten sie die gleiche Arbeit wie Erwachsene, was in diesem Fall Schichten bis zu elf Stunden mit nur wenigen Pausen und niedriger Vergütung bedeutet.[1]

All diese Berichte stehen im direkten Zusammenhang mit unserem Kauf von Laptops, Smartphones, Desktops oder anderen IKT-Geräten. Doch anders als bei Kleidung, Kaffee oder Schokolade gibt es bislang keine echte Kaufalternative im IKT-Bereich. Alle Markenhersteller kaufen über wenige zentrale Hauptzuliefererfirmen (Kontraktfertiger) ein, die die Arbeitsrechte in der eigenen und der Sublieferanten-Produktion missachten. Bislang

Wohnheim für Arbeiterinnen: Schlafen zu zwölft – verhängte Betten als einzige Privatssphäre, China. Foto: SACOM 2007

ist daher noch kein *faires* IKT-Produkt auf dem Markt. Sogar die beiden aus NGO-Kreisen stammenden Produkt-Initiativen, die sich auf den Weg zur sozial verantwortlich produzierten Computermaus (*Nager IT*) bzw. Smartphone (*Fairphone*) gemacht haben, zeigen – erfreulich transparent – die Schwierigkeiten, entlang der gesamten Lieferkette soziale Rechte von Zulieferern und Sublieferanten einzufordern und zu kontrollieren.

Die Einkaufsmacht der öffentlichen Beschaffungsstellen

Gerade wegen dieser aussichtslos scheinenden Situation können Großeinkäufer wie öffentliche Beschaffungsbehörden bei der Verbesserung der Bedingungen in diesem Sektor eine Schlüsselrolle spielen. In Europa kaufen öffentliche Einrichtungen IKT-Produkte mit einem enormen Gesamtbetrag ein, oft mit mehrjährigen Rahmenverträgen und hohen Einkaufsvolumina pro Ausschreibung. Zwischen 2013 und 2015 wird sogar ein jährliches Wachstum von sieben Prozent erwartet.[2] Damit verfügen sie über eine enorme Marktmacht, die sie sozial verantwortlich einsetzen können und sollten.

Doch leider versagen in Deutschland die meisten politisch Verantwortlichen beim Thema IT-Einkauf. Bislang haben so gut wie alle Bundesländer, die soziale Kriterien in ihren Vergabegesetzen fordern, IKT-Produkte von der Liste der verpflichtend sozial einzukaufenden Produkte gestrichen. Eine rühmliche Ausnahme ist bislang nur Nordrhein-Westfalen.

Dabei gibt es gerade jetzt mehrere neue Ansätze und auch Initiativen, die Beschaffungsstellen mit praktischen Hilfestellungen zur Seite stehen können.

WEED und andere NGOs schlagen schon länger vor, von den Bietern statt eines fairen Produkts die Umsetzung sogenannter zielführender Maßnahmen zu fordern, die für den Auftraggeber überprüfbar sind. Dies kann z. B. eine möglichst weit reichende Transparenz der Lieferkette, die Aushändigung von Arbeitsverträgen und nationalen Arbeitsgesetzen an die ArbeiterInnen, eine Schulung des Managements zu den geforderten sozialen Rechten, die Durchführung von Arbeitsrechts-Trainings oder im besten Falle eine unabhängige Beschwerdestelle sein. Eine Musterausschreibung hierzu ist auf WEEDs Website zu finden.[3]

In Schweden gibt es außerdem den Ansatz, den dort bewährten Fragenkatalog zur Verlaufskontrolle auch beim IKT-Einkauf einzusetzen: Der Bieter, der den Zuschlag erhalten hat, ist verpflichtet, nach einer gewissen Zeit nach Vertragsunterzeichnung diesen Fragenkatalog zu sozialen Rechten auszufüllen. Mithilfe eines Auswertungsbogens nach dem Ampelsystem können die Behörden dann ermitteln, ob der Vertragspartner die vereinbarten sozialen Kriterien eingehalten hat. Die schwedischen Bezirksgemeinden schließen bei denjenigen Vertragspartnern, deren Antworten nicht zufriedenstellend sind, an dieses Verfahren sogar ein externes Auditing vor Ort an. Das Konzept hat WEED im Rahmen des europäischen *LANDMARK*-Projekts zu sozial verantwortlicher Beschaffung vorgestellt.[4]

Dieses schwedische Modell des Fragenkatalogs hat auch *TCO Development* übernommen, die das erste Zertifikat zu sozialen Kriterien bei IT-Hardware vergeben. Auch wenn hier bislang leider nur die letzte Stufe in der Produktion kontrolliert wird, leistet TCO doch wichtige Pionierarbeit. Weil TCO die Einhaltung sozialer Kriterien in der Lieferkette fordert, aber nur die letzte Stufe in der Produktion kontrolliert, kam es vor kurzem zum Eklat: NGOs zeigten auf, dass in der Produktion des TCO-zertifizierten Samsung-Smartphones *Galaxy S4* in koreanischen Werken der unteren Lieferkette Arbeitsschutzmaßnahmen schwerwiegend missachtet wurden. Die Konsequenzen, die TCO in diesem Fall Samsung gegenüber ziehen wird, werden hoffentlich zeigen, wie unabhängig und transparent TCO auch im Ernstfall ist.

Auch in Deutschland übernehmen manche öffentliche Beschaffungsverantwortliche mit neuen Ansätzen freiwillig Verantwortung. So hat die zentrale IT-Beschaffungsstelle im Norden, *Dataport*, in ihrer jüngsten Hardware-Ausschreibung mit einem Gesamtvolumen von etwa 70 Millionen Euro und einer Laufzeit von vier Jahren von den Bietern ein Konzept zur Einhaltung umfangreicher sozialer Rechte gefordert und dies im Rahmen der Zuschlagskriterien gewertet.[5] Und das *Bundesbeschaffungsamt des BMI* hat eine IT-Mustererklärung mit dem IT-Branchenverband *BITKOM* vereinbart, die zwar diverse Schwächen hat, aber doch ein erster Schritt in die richtige Richtung ist.[6]

Vertrauen ist gut – Kontrolle ist besser

All dies sind wichtige Schritte, um ein Umdenken bei den Bietern anzustoßen. Angesichts fehlender personeller und zeitlicher Ressourcen bei vielen öffentlichen Beschaffungsstellen einerseits

und intransparenter Lieferketten andererseits bleibt bei den meisten Ansätzen jedoch der wichtige Aspekt der Kontrolle problematisch.

Hier setzt ein neues Projekt an, an dem auch WEED beteiligt ist. Gemeinsam mit mehreren europäischen Organisationen haben wir begonnen, ein Konsortium namens *Electronics Watch*[7] aufzubauen. Electronics Watch wird eine unabhängige Monitoring-Organisation, die mithilfe sozial verantwortlicher öffentlicher Beschaffung in Europa die Einhaltung der ArbeitnehmerInnenrechte in der globalen Elektronikbranche erreichen will.

Das Modell von Electronics Watch lehnt sich eng an das für den Bekleidungssektor bewährte Modell des *Worker Rights Consortium*[8] aus den USA an. Die Mitglieder dieses Konsortiums fordern von ihren Lieferanten die Einhaltung internationaler Arbeitsrechte und schaffen durch ihre kumulierte Kaufkraft seit 2000 Anreize für nachhaltige und sozial verantwortliche Arbeitsbedingungen entlang der Lieferkette.

Arbeit in einer chinesischen Computerfabrik
Foto: SACOM 2008

Auch bei Electronics Watch werden NGOs und Gewerkschaften aus dem Süden ebenso wie europäische öffentliche Beschaffungsstellen in der Führung der neuen Organisation gleiches Mitspracherecht haben. Gegen Zahlung einer Gebühr sollen die beteiligten öffentlichen Einrichtungen und Institutionen mit aktuellen Informationen über ihre Lieferanten versorgt, die Arbeitsbedingungen vor Ort überprüft und Verfahren bereitgestellt werden, um auf Nichteinhaltungen zu reagieren. Dies wird durch Kontakte und Kontrolleure vor Ort in Kombination mit einem Whistleblower-System möglich. Die Finanzierung durch Beschaffungsbehörden statt durch die zu kontrollierenden Unternehmen gewährleistet die unerlässliche Unabhängigkeit von den IKT-Unternehmen. Electronics Watch soll bis Mitte 2015 mit einer ersten Gruppe von 50 öffentlichen Beschaffungsstellen aus ganz Europa beginnen.

Dass das eigene Einkaufsverhalten direktes politisches Handeln bedeutet, haben die über 18000 Einzelpersonen verstanden, die *Fairphone* durch den Kauf dieses Produkts unterstützen. Angesichts der vielversprechenden Ansätze ist zu hoffen, dass auch mehr öffentliche Beschaffungsstellen und politische EntscheidungsträgerInnen in Europa ihre Verantwortung beim IKT-Einkauf wahrnehmen.

Anmerkungen

1 *Links zu diesen und weiteren Berichten auf www.pcglobal.org*
2 *Global Consumer Electronics Market Forecast von RNCOS, http://www.reportlinker.com/ci02060/Consumer-Electronics.html*
3 *WEED u. a.: „Buy IT Fair– Leitfaden zur Beschaffung von Computern nach sozialen und ökologischen Kriterien", http://www2.weed-online.org/uploads/leitfaden.pdf sowie „Quo Vadis, Beschaffung?", http://www2.weed-online.org/uploads/quo_vadis_beschaffung.pdf*
4 *Vgl. http://www.landmark-project.eu/de/leitfaeden-instrumente*
5 *Vgl. www.dataport.de/ueber-uns/presseservice/pressemitteilungen/Seiten/Dataport2013/130801-Kooperation-IT-Beschaffung.aspx . Die Ausschreibung wird demnächst auf www.landmark-project.eu vorgestellt.*
6 *Vgl. das vorab veröffentlichte Forderungspapier des CorA-Netzwerks unter www2.weed-online.org/uploads/forderungen_cora_it_beschaffung_2012.pdf*
7 *Siehe www.electronicswatch.org/de*
8 *Siehe www.workersrights.org*

Annelie Evermann

Annelie Evermann ist Juristin und Referentin für nachhaltige Produktion und öffentliche Beschaffung bei WEED – Weltwirtschaft, Ökologie und Entwicklung e. V. *(www.weed-online.org).* Sie beschäftigt sich derzeit schwerpunktmäßig mit Produktionsbedingungen in der IT-Branche.

TCO Development

Zertifizierung von IT-Produkten als Katalysator für eine nachhaltigere IT-Industrie

Die schlechten Arbeitsbedingungen in der IT-Industrie haben in den vergangen Jahren immer mehr Aufmerksamkeit erfahren. Organisationen, deren Strategien auch von Fragen der Nachhaltigkeit abhängen, müssen die Bedeutung und die Auswirkungen dieser Probleme bei der Auswahl von IT-Produkten berücksichtigen. Unabhängige Produktzertifizierungen sind dabei ein nützliches Werkzeug für Einkäufer, die Nachhaltigkeitsanforderungen in ihre Produktspezifikationen einbeziehen möchten. Das globale Zertifikat TCO Certified *wird von* TCO Development *vergeben, einer Organisation mit einer langen Geschichte, Einfluss auf das Design von IT-Produkten in den Bereichen Ergonomie, Energieeffizienz und verbesserte Umweltverträglichkeit zu nehmen. Jetzt konzentriert sich* TCO Development *darauf, Fortschritte bei der sozial verantwortlichen Herstellung von IT-Produkten herbeizuführen.*

Nur wenige von uns können sich einen Tag ohne unseren Computer oder unser Smartphone vorstellen. Aber wie viel wissen wir darüber, wie diese Geräte hergestellt werden? Dank einer zunehmenden Anzahl von Berichten in den Medien, die mangelhafte Arbeitsbedingungen in der IT-Industrie aufdecken, wird dieses Problem immer mehr Menschen bewusst. Sie machten die damit verbundenen Probleme weltweit bekannt, nämlich illegale Überstunden, Erkrankungen von Arbeitern durch toxische Substanzen sowie Einschränkungen des Rechts der Arbeiter, sich zu organisieren. Die Belastungen werden in der Lieferkette verstärkt durch den wachsenden Zwang zu Kostensenkungen und kürzeren Produktzyklen.

Die Bedingungen, die bei einem der größten Zulieferer in China herrschen, wurden im vergangenen Jahr weltweit von den Medien berichtet. Eine Welle von Selbstmorden hat die Industrie und Verbraucher aufgerüttelt und die betroffene Firma so gezwungen, Ermittlungen einzuleiten, Prüfungen durchzuführen und einen Aktionsplan zu veröffentlichen.

Für IT-Einkäufer sind soziale und ökologische Verantwortung wichtiger denn je. Je mehr sich Organisationen der Nachhaltigkeit widmen, desto genauerer Beobachtung unterliegen auch die Herstellung von IT-Produkten und Probleme in der Lieferkette. Die Herstellung eines einzigen Computers kann bis zu 60 Vorgänge bei einer Anzahl unterschiedlicher Zulieferer auf der ganzen Welt erfordern.

Der sozialen Verantwortung in einer solchen Lieferkette, die durch Komplexität und Intransparenz gekennzeichnet ist, kann man nicht durch eine Einzellösung gerecht werden. Neben einschlägiger Gesetzgebung und der Lobbyarbeit der Nichtregierungsorganisationen hat sich die Nachfrage von Einkäufern nach bestimmten Zertifizierungen als effektiv erwiesen. Beispiele solcher Third-Party-Zertifikate sind *TCO Certified*, der *Blaue Engel*, *Nordic Swan* und das *EU Ecolabel*.

TCO – bekannt durch die Zertifizierung von Monitoren

TCO Development, Besitzerin des globalen Zertifikats *TCO Certified*, arbeitet ausschließlich im IT-Bereich und ist Tochter von *TCO*, der *Swedish Confederation for Professional Employees*. Die Zertifizierung stattet hauptamtliche Beschaffer mit einem strategischen Werkzeug aus, um Nachhaltigkeitsanforderungen beim IT-Einkauf mit einzubeziehen. Durch ihre großen Einkaufsmengen können öffentliche und private Organisationen so Verbesserungen in der Industrie herbeiführen. Gleichzeitig bietet *TCO Certified* Produzenten ein industrieweites Rahmenwerk, um ihren Fortschritt im Hinblick auf verantwortungsvolleres Handeln zu messen.

Die Geschichte von *TCO Certified* geht bis in die 1980er Jahre zurück, als sich die Verwendung von Computern auszubreiten begann. Zu Anfang bezog sich die Zertifizierung auf einige Anforderungen bezüglich Gesundheit, Sicherheit und Qualität für Computermonitore. Später wuchs sie dann zum De-Facto-Standard für Monitorqualität auf der ganzen Welt heran. Etwa die Hälfte aller Computermonitore sind *TCO-zertifiziert*, was dazu beiträgt, die negativen ökologischen und sozialen Auswirkungen von IT-Produkten zu vermindern. Die Abbildung 2 auf der nächsten Seite zeigt das Siegel.

TCO Development

TCO Development setzt sich auf internationaler Ebene dafür ein, dass bei IT-Produkten und deren Produktion ökologische, soziale und wirtschaftliche Belange berücksichtigt werden. 1992 wurde das TCO-Gütesiegel eingeführt. Ab dem Jahr 2000 wurden die Umweltkriterien schrittweise verschärft. 2009 wurde das Kriterium der unternehmerischen Sozialverantwortung in der Produktion eingeführt. Die Liste der aktuell zertifizierten Produkte findet man unter http://www.tcodevelopment.de/tco-certified/zertifiziertes-produkt-suchen/. Die Firmenzentrale von TCO Development befindet sich in Stockholm, Schweden.

Abbildung 1: Die Kriterien der sozialen Verantwortung für die TCO Zertifizierung

Der Fokus von *TCO Development* hat sich, ausgehend von Gesundheit, Sicherheit und Energieeffizienz, weiter entwickelt und umfasst nun ökologische Nachhaltigkeit und soziale Verantwortung. Insgesamt wurden durch TCO Development über 4 000 Produktmodelle zertifiziert. Wichtige Aspekte von *TCO Certified* sind die rigorose Methodologie und die Qualitätssicherung des Zertifizierungsprozesses. Die Einhaltung von Anforderungen bezüglich Ergonomie, Umweltverträglichkeit und sozialer Verantwortung wird in jedem dieser Bereiche von bereichsspezifisch akkreditierten Testeinrichtungen kontrolliert.

Wird ein Markenhersteller *TCO-zertifiziert*, bedeutet das, dass er eine für die gesamte Gültigkeit des Zertifikats andauernde Verpflichtung eingeht, auch in Zukunft alle Anforderungen bezüglich Produkt und Herstellung für das zertifizierte Modell zu erfüllen. Die Kriterien sind so gewählt, dass sie sowohl eine Herausforderung darstellen als auch erreichbar sind, um möglichst effektiv Änderungen herbeizuführen. Die Anforderungen werden in Zusammenarbeit mit einer international zusammengesetzten Interessensgruppe ständig überarbeitet und aktualisiert.

Zertifiziert werden einzelne Produkte anhand von Sozialkriterien

Die meisten Anforderungen von *TCO Certified* beziehen sich auf Produkteigenschaften, welche von einer unabhängigen Testorganisation überprüft werden. Die Testberichte werden anschließend durch einen weiteren Drittspezialisten überprüft. Weitere Kriterien beziehen sich auf die Herstellungsprozesse des jeweiligen Produkts. Hier gibt es einen Verifikationsprozess, bei dem die Einhaltung der Bestimmungen der acht *Kernarbeitsnormen* der ILO, der UN-Kinderrechtskonvention sowie der Gesetze des Produktionslandes bezüglich Gesundheit und Sicherheit, Lohn, sozialer Absicherung und dem Recht der Arbeiter, sich zu organisieren, überprüft werden. Für China kommen gesonderte Regeln zum Einsatz, da das Recht, sich zu organisieren, dort gesetzlich eingeschränkt ist.

Im Zentrum der Arbeit von *TCO Development* stehen sich die gründliche Überprüfung und Nachkontrolle der Einhaltung der Kriterien. Die Kriterien sind in Abbildung 1 dargelegt. Ob ein Hersteller, sie bezogen auf die zu zertifizierenden Produkte, erfüllt, wird in sechs Punkten überprüft:

- Rechtlich bindende Vereinbarungen
- Kompetenz in der Umsetzung
- Transparenz in der Produktion
- Inspektionen der betroffenen Fabriken
- Jährliche stichprobenartige Überprüfungen
- Eine Kontaktperson für den fortlaufenden Dialog

Die Mission von *TCO Development* ist es, zur nachhaltigen Entwicklung in der IT-Industrie beizutragen. Sie wird von ihrer Eigentümerin nicht dazu verpflichtet, Profit abzuwerfen. *TCO Development* arbeitet mit den großen IT-Markenherstellern auf der Grundlage zusammen, dass Fortschritte zu mehr Nachhaltigkeit im IT-Bereich durch diese Zusammenarbeit effektiver geschehen können.

Abbildung 2: Achten Sie auf dieses Siegel

Übersetzung aus dem Englischen: **Sebastian Beschke**

CC BY

Friedel Hütz-Adams

Zertifizierungen: ein Baustein zu mehr Transparenz

Beim Abbau von Rohstoffen und deren Weiterverarbeitung kommt es in vielen Staaten zu massiven Menschenrechtsverletzungen. Dies beginnt in einigen Abbauländern mit der Vertreibung der Menschen, die auf den Flächen leben, auf denen der Bergbau stattfinden soll, führt über die Verschmutzung von Luft und Wasser in den Minengebieten und deren Umland über miserable Arbeitsbedingungen bis hin zu Verseuchungen durch Chemikalien. Besonders eklatant sind die Probleme beim Abbau der metallischen Rohstoffe durch Kleinschürfer. Diese arbeiten häufig unter äußerst schlechten Bedingungen, sind gesetzlich nicht geschützt und mit Arbeitsschutz sowie Umweltbestimmungen entweder nicht vertraut oder nicht in der Lage, diese umzusetzen. Betroffen davon sind hunderttausende Menschen, die weltweit beispielsweise nach Gold, Tantal, Zinn oder Kobalt graben, lauter Rohstoffe, die auch in der Elektronikindustrie sehr wichtig sind.

Dabei gibt es eine Vielzahl von Regulierungen auf internationaler Ebene, die solche Missstände verhindern sollten. Dies reicht von der *Allgemeinen Erklärung der Menschenrechte* bis hin zu Konventionen von Unterorganisationen der Vereinten Nationen, die beispielsweise den Umweltsektor, den Schutz der Arbeitnehmer oder die Rechte indigener Völker umfassen. Allen diesen Bestimmungen gemein ist, dass es bei Verstößen an Sanktionsmechanismen mangelt.

Auch nationale Regierungen haben eine Vielzahl von Gesetzen erlassen, die soziale und ökologische Mindeststandards festlegen. Doch vielen Regierungen mangelt es entweder an der Fähigkeit, die eigenen Gesetze durchzusetzen, oder an dem Willen dazu. Dabei kann der Versuch eine Rolle spielen, Investoren anzulocken und Arbeitsplätze zu schaffen. Doch häufig genug gibt es gerade bei Rohstoffprojekten Korruptionsvorwürfe.

Kassiterit (Zinnerz) in der Hand eines Kongolesischen Minenarbeiters, Foto: Enough Project/Laura Heaton 2011

UN und OECD zur Verantwortung der Unternehmen

Um die Debatte über Wege zur Beseitigung von Missständen voranzutreiben, wurde vom Generalsekretär der Vereinten Nationen mit *John Ruggie* ein Sonderbeauftragter für Wirtschaft und Menschenrechte eingesetzt. Ruggie, dessen Forderung nach einer Sorgfaltspflicht (*due diligence*) der Unternehmen im Juni des Jahres 2011 durch eine im Menschenrechtsrat der Vereinten Nationen verabschiedete Richtlinie zu einer weltweiten Leitlinie wurde, sieht zwar an erster Stelle die Regierungen in der Pflicht, die Einhaltung der Menschenrechte in der Wirtschaft durchzusetzen. Geschieht dies nicht, tragen seiner Meinung nach Unternehmen eine Verantwortung für Missstände in der eigenen Produktion sowie bei den Zulieferern.

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (*OECD* – ein Zusammenschluss von derzeit 34 Industrie- und Schwellenländern) hat in Anlehnung an die Thesen von John Ruggie in ihrer im Mai 2011 verabschiedeten Neufassung der *OECD-Leitsätze für multinationale Unternehmen* den Begriff der *due diligence* übernommen und die Unternehmen dazu aufgefordert, die Durchsetzung der Menschenrechte in ihren Geschäftsbeziehungen zu garantieren. Darüber hinaus hat die OECD weitere Richtlinien für Rohstoffe aus Konfliktgebieten sowie eigene Richtlinien für einzelne Rohstoffe erlassen.

Die Vorgaben wurden unter Beteiligung von Unternehmen und Gewerkschaften entwickelt und umfassen neben menschenrechtlichen Bestimmungen auch Arbeitsbeziehungen, Umweltstandards und Regelungen zu Bestechung, Wettbewerb und Besteuerung. Die Mitgliedsstaaten der OECD haben nationale Kontaktpunkte eingerichtet, bei denen Beschwerden über Verstöße gegen die Leitlinien eingereicht werden können.

Die OECD benennt die an den verschiedensten Stellen der Wertschöpfungskette vorhandenen Risiken und schlägt zu deren Ausschluss die Durchführung regelmäßiger Audits durch unabhängige Dritte vor, für deren Ablauf konkrete Schritte erarbeitet wurden.

Dreh- und Angelpunkt dieser Argumentation ist die Möglichkeit, den Weg der Metalle von der Mine bis zum Endprodukt transparent zu machen. Dies würde den Druck auf die Unternehmen schaffen, flächendeckend Missstände, Umweltzerstörungen und Korruption bei ihren Lieferanten zu bekämpfen. Freiwillige Verpflichtungen haben dies bisher nicht geschafft.

Gesetze bringen Debatte voran

Im Juli 2010 wurde in den USA ein umfassendes Gesetzespaket in mit dem Namen *Dodd-Frank Wall Street Reform and Consumer Protection Act*, kurz *Dodd-Frank-Act*, unterzeichnet. Dieses enthält zwei Absätze, die großen Einfluss auf die Debatten über den Handel mit metallischen Rohstoffen haben. Einer dreht sich um die Offenlegung von Zahlungen an Regierungen im Rahmen

von Rohstoffgeschäften, die nun für an den Börsen der USA notierte Unternehmen vorgeschrieben ist, wobei die Umsetzung des Gesetzes noch sehr umstritten ist.

Der zweite Absatz schreibt allen an US-Börsen notierten Unternehmen vor, dass die von ihnen verwendeten Metalle Gold, Zinn, Tantal und Wolfram nachweislich keine Milizen im Osten der Demokratischen Republik Kongo finanzieren dürfen: Eine Reihe der Milizen, doch auch Teile der Regierungsarmee waren und sind in die Ausbeutung und den Handel mit metallischen Rohstoffen verwickelt. Um Schmuggel aus dem Kongo zu unterbinden, muss laut Dodd-Frank-Act auch über die genaue Herkunft der aus der Zentralafrikanischen Republik, dem Sudan, Sambia, Angola, der Republik Kongo, Tansania, Burundi, Ruanda und Uganda importierten Rohstoffe Auskunft gegeben werden. Nach langen Debatten über die konkrete Umsetzung trat die Regelung im Januar 2013 in Kraft.

Die EU plant, ähnliche Bestimmungen zu erlassen. Offen ist, ob das Gesetz wie in den USA auf Rohstoffe aus der Demokratischen Republik Kongo beschränkt bleibt. Möglich ist auch, dass die EU berücksichtigt, dass es auch in vielen anderen Rohstoffgebieten und bei weit mehr als den vier im Dodd-Frank-Act genannten Rohstoffen erhebliche Konflikte gibt. Dies würde für eine deutliche Erweiterung der Zahl der Länder und der betroffenen Metalle sprechen.

Bislang geht es dabei allerdings im Wesentlichen um Konfliktfreiheit. Darüber hinaus muss eine Debatte darüber geführt werden, welche Preise, Löhne, Umweltschutzbestimmungen und Verbesserungen bei den Arbeitsbedingungen notwendig sind, um den Beschäftigten ein menschenwürdiges Leben zu ermöglichen.

Zertifizierungen im Aufbau

Die Debatten über den Beitrag des Handels mit Rohstoffen an der Konfliktfinanzierung im Kongo laufen seit dem Jahr 2001, als ein erster Bericht der Vereinten Nationen diesen Zusammenhang nachwies. Passiert ist viele Jahre lang wenig. Erst als sich ab 2010 abzeichnete, dass in den USA ein Gesetz kommt, kam es zu hektischen Aktivitäten in der Elektronikbranche. Eine Angestellte eines großen Konzerns hat die Entwicklung in einem internen Gespräch so zusammengefasst: „Da ist in einem Jahr mehr passiert als in den zehn Jahren zuvor."

Eine erste Reaktion vieler Unternehmen war, ihren Lieferanten vorzuschreiben, gar keine Rohstoffe mehr aus den Staaten Zentralafrikas zu kaufen. Dies hatte verheerende Folgen für hunderttausende Kleinschürfer, die ihren Broterwerb verloren. Dies ist einer der Gründe dafür, warum viele Beobachter den Dodd-Frank-Act als Fehlschlag bezeichnen.

Andererseits gibt es nun eine Reihe von Initiativen, den Handel mit Erzen aus dem Osten des Kongo transparent zu machen und so Arbeitsplätze zu sichern, was letztendlich zur Schaffung von Frieden beitragen würde. Ein Ansatz ist dabei, bereits in den Minen die Rohstoffe in Säcke zu verpacken und diese dann mit einer Plombe mit einer Nummer zu verschließen. Die Erze werden dann an Schmelzen geliefert, die sich verpflichtet haben, ausschließlich Ware mit Herkunftsnachweis zu verarbeiten. So arbeitet beispielsweise die *Tin Supply Chain Initiative (iTSCi)*, die bereits Zinnminen erfasst hat und den Ansatz auf Tantal und Wolfram ausbaut. Hierbei steht bislang allerdings lediglich die Verhinderung der Finanzierung von Milizen im Mittelpunkt.

Mit Unterstützung der deutschen Entwicklungszusammenarbeit werden ebenfalls zertifizierte Handelsketten (*Certified Trading Chains – CTC*) für Zinn, Tantal und Wolfram aufgebaut, wobei bislang hauptsächlich in Ruanda und der Demokratischen Republik Kongo gearbeitet wird. Kontrolliert werden hier nicht nur die Finanzierung von Milizen, sondern auch Umwelt- und Arbeitsschutzstandards. Darüber hinaus kooperiert das Projekt mit einem Zusammenschluss der Regierungen der zentralafrikanischen Region (*International Conference on the Great Lakes Region – ICGLR*), der ein einheitliches Zertifizierungssystemen für alle Länder Zentralafrikas aufbauen will. Weitere Initiativen gibt es im Goldsektor sowie durch einzelne Unternehmen und Nichtregierungsorganisationen.

Umfassender Ansatz nötig

Diese Auflistung, die sich noch deutlich verlängern ließe, zeigt einen Teil des Problems: Unter dem Druck der drohenden Gesetze wird an den verschiedensten Stellen an Teillösungen gearbeitet, die jeweils nur einzelne Metalle und einzelne Probleme umfassen. Notwendig wäre dagegen ein umfassender Ansatz, bei dem die Elektronikindustrie ihre Lieferketten bis hin zu den Minen transparent macht und damit eine Kontrolle auf mögliche Missstände entlang der gesamten Kette ermöglicht. Noch vor wenigen Jahren haben Unternehmen gesagt, es sei unmöglich, ihre Lieferanten zu kontrollieren. Bei Qualitätsfra-

Friedel Hütz-Adams

Friedel Hütz-Adams (*1966) ist seit 1993 wissenschaftlicher Mitarbeiter des SÜDWIND e. V., Institut für Ökonomie und Ökumene. Zuvor studierte er in Köln Geschichte, Philosophie und Volkswirtschaftslehre. Bei SÜDWIND beschäftigt er sich hauptsächlich mit den Zusammenhängen zwischen Armut und Missständen in Entwicklungsländern einerseits und dem Verhalten von Wirtschaft, Politik, Verbraucherinnen und Verbrauchern in Deutschland andererseits.

gen wird dies dagegen schon immer praktiziert, was die Frage aufwirft, warum dies bei Sozial- und Umweltstandards nicht möglich sein soll.

Das Unternehmen HP hat beispielsweise kürzlich mit der Veröffentlichung einer Liste von mehr als 190 weltweit verstreuten Schmelzen, die ihre Zulieferer beliefern, gezeigt, dass es geht. Auch der Versuch von Fairphone, ein transparenter hergestelltes Mobiltelefon zu bauen und dabei zumindest für einige Metalle Herkunftsnachweise mitzuliefern, zeigt, dass vieles möglich ist.

Insellösungen durch Zertifizierungen können allerdings nur Teilaspekte abdecken. Zu hoffen ist daher, dass die Zusammenschlüsse der Branche – hier insbesondere die im Jahr 2001 gegründete *Global e-Sustainability Initiative (GeSI)* sowie die 2004 gegründete *Electronic Industry Citizenship Coalition (EICC)* – in einem konzertierten Ansatz die notwendigen Investitionen bereitstellen, um die sozialen, ökonomischen und ökologischen Bedingungen bei der Produktion von elektronischen Produkten zu verbessern. Dies muss dann für alle Rohstoffe gelten, nicht nur für die aus der Demokratischen Republik Kongo – schließlich gibt es auch bei der Förderung von Erzen in anderen Ländern massive Missstände.

CC BY

Andreas Manhart

Berichtspflicht zu Konfliktmineralien in den USA

Was können wir daraus für Europa lernen?

Der Dodd-Frank-Act 1502 *verlangt von US-Börsennotierten Firmen, die Herkunft ausgewählter Rohstoffe offen zu legen. Betroffen sind dabei die Erze und Metalle, die teilweise im Osten der Demokratischen Republik Kongo abgebaut werden und zum Teil für die Finanzierung bewaffneter Konflikte missbraucht werden.[1] Sobald eine Firma als Herkunftsland Kongo oder eines der Nachbarländer angibt, sind umfängliche Nachweise erforderlich, die belegen sollen, dass diese Materialien nicht im Zusammenhang mit Konflikten gewonnen wurden. Dabei ist die IT-Industrie besonders betroffen, denn alle der vier Konfliktmetalle Zinn, Tantal, Wolfram und Gold (auch* 3TG *genannt) kommen in modernen Elektronikgeräten vor. Dieses Gesetz wirkte zunächst wie ein Embargo, weil sich die Hersteller die Mineralien in der Folge aus anderen Gegenden besorgt haben. Dennoch will die EU nun eine eigene, ähnliche Richtlinie verabschieden, „on responsible sourcing of minerals originating from conflict-affected and high-risk areas", wobei die Lehren aus 1502 einfließen sollen.[2]*

Das *Öko-Institut* veröffentlichte Ende August die viel beachtete Studie *Conflict minerals – An evaluation of the Dodd-Frank Act and other resource-related measures*.[3] Wir sprachen mit *Andreas Manhart*, einem der Autoren, über die Konsequenzen daraus.

FIfF: Herr Manhart, die von Ihnen mitverfasste Studie ist sehr kritisch gegenüber dem Dodd-Frank-Act 1502, der in den U.S.A. vor allem durch zivilgesellschaftliche Organisationen vorangetrieben wurde. War hier „gut gemeint" das Gegenteil von gut?

Andreas Manhart: Der *Dodd-Frank Act* hat vieles bewirkt, das wollen wir den USA gar nicht abstreiten. Aber letztendlich zeigt sich auch, dass es zu unerwünschten Nebeneffekten gekommen ist, die man nicht ignorieren darf. So haben die Auflagen eine stark abschreckende Wirkung für alle, die Erze aus dem Kongo beziehen wollen – selbst wenn die Förderung unter verantwortungsvollen Rahmenbedingungen geschieht.

Abb. 1: Goldmine in Süd-Kivu, Kongo. Foto: Sasha Lezhnev/ Enoughproject.org 2011, CC-BY-NC-ND

Zwar fordern Sie Verbesserungen und weniger aufwändige Prozesse, Sie lehnen in Ihren Empfehlungen eine EU-Regelung zur Offenlegung von Rohstoffgeschäften aus Risiko- und Konfliktgebieten aber nicht grundsätzlich ab. Glauben Sie, dass der Auftraggeber der Studie, der BDI (Bundesverband der Deutschen Industrie e. V.), Ihre Empfehlungen übernehmen wird? Bislang lehnte er eine Regulierung dieser Art immer ab.

Zuallererst fordern wir – wie Sie ja sagen – keine grundsätzliche Abkehr vom Transparenzgedanken. Man sollte aber nicht glauben, dass ein positiver Zusammenhang zwischen möglichst ambitionierten Berichtspflichten und der Verbesserung der Situation vor Ort bestünde. Es gilt, eine ausgewogene Balance zwischen Transparenzanforderungen und verantwortungsvollem Direktengagement vor Ort zu finden.

Als *Öko-Institut* können wir natürlich nicht für die Industrie sprechen. Wir hatten aber in unserer Arbeit mit dem BDI sowie auch mit vielen Leuten in Unternehmen den Eindruck, dass das Problem nicht ignoriert wird. Wir sehen auf Seiten der Industrie auf alle Fälle Gesprächsbereitschaft und das Interesse zur Suche eines tragfähigen europäischen Lösungsbeitrages. Letztendlich hängen aber die Richtungsentscheidungen für einen europäischen Beitrag nicht alleine von der Industrie ab, sondern ebenso von der EU Kommission, dem Parlament sowie vom Einfluss der Nichtregierungsorganisationen. Letztendlich sind wir der Überzeugung, dass es nun zeitnah einen Dialogprozess geben sollte, der die verschiedenen Vorschläge ergebnisoffen diskutiert. Dabei sollten natürlich auch kongolesische Stimmen nicht fehlen.

Können Sie kurz erzählen, wie die Zertifizierung konfliktfreier Rohstoffquellen in der Praxis abläuft? Ist sie vertrauenswürdig?

Fast alle Industriezweige sehen die Schmelzen und Raffinerien als Schlüssel zum Erfolg. Hier gibt es verschiedene Programme, die mit Hilfe von Auditierungen einen Nachweis ausstellen, dass ein Schmelzbetrieb garantiert „konfliktfrei" ist. Die Schmelzen müssen für alle ihre Lieferungen im zurückliegenden Jahr die genaue Herkunft nachweisen. Das Problem ist, dass fast alle als „konfliktfrei" gelisteten Schmelzen de facto „Kongo-frei" sind, ihren Status also dadurch erreichen, dass sie gar nicht mehr aus der Region beziehen. Aus meiner Sicht führt man hier einen eigentlich guten Gedanken ad absurdum: Man steckt unglaublich viel Geld in die Zertifizierung konfliktfreier Lieferketten, dieses Geld wird aber überhaupt nicht für die Lösung der Probleme vor Ort verwendet. Hauptprofiteure sind derzeit die großen Wirtschaftsprüfungsunternehmen, die sehr viel Geld mit der Nachweisführung verdienen.

Und dann kommt noch hinzu, dass die Rohstoffe aus dem Kongo dann doch über dunkle Kanäle auf den Weltmarkt kommen. Und ein Hersteller eines sehr komplexen Produkts kann sich letztendlich doch nicht sicher sein, ob die vielen tausend Papiernachweise für alle Einzelteile wirklich der Realität entsprechen.

Gilt dies auch für die Vorzeigeprojekte, *Solutions for Hope* für Tantal und *Conflict Free Tin Initiative* für Zinn?

Nein, bei diesen beiden Projekten kann man sich tatsächlich sicher sein, dass sie nicht im Zusammenhang mit Konflikten stehen. Das Problem besteht eher darin, dass unter den vielen Akteuren in komplexen Lieferketten immer auch schwarze Schafe zu finden sind, die Zertifikate und Herkunftsangaben bewusst fälschen. Leider kann man solche Betrüger analytisch nicht überführen, denn die existierenden Labormethoden sind nur im Bereich der Erze und Konzentrate anwendbar – nicht bei standardisierten Metallen und Legierungen.

Es gibt viele Gegenden wo Tantal- und Zinnerze abgebaut werden, auch weniger risikoreiche wie Brasilien oder Australien. Warum werden dennoch Rohstoffe aus der D.R. Kongo bezogen, warum machen sich die Firmen sogar die Mühe, einen konfliktfreien Zugang zu schaffen? Da scheint doch ein ökonomischer Vorteil zu liegen.

Offiziell werden aus dem Kongo nur sehr kleine Mengen an Konfliktrohstoffen ausgeführt. Hier wird die Wahrnehmung noch oft von der Situation vergangener Jahre geprägt, als z. B. Australien vorübergehend kein Tantal mehr produziert hat und der Kongo diese Lücke aufgefüllt hat. Aber natürlich spielt der Schmuggel über die Nachbarländer eine wichtige Rolle. Gerade Gold lässt sich wegen seines hohen Materialwerts und der Tatsache, dass es vielerorts als Zahlungsmittel akzeptiert ist, sehr leicht schmuggeln. Bei den Industrierohstoffen – insbesondere Tantal und Zinn – hat der Kongo zwar durchaus große Vorkommen, diese werden aber derzeit nur oberflächlich angekratzt. Es ist nicht so, dass die wenigen Projekte der westlichen Industrie im Kongo große Mengen fördern würden. Die Hauptmotivation der Unternehmen die an den Projekten *Solutions for Hope* und *Conflict Free Tin Initiative* beteiligt sind, liegt derzeit wohl eher im Imagegewinn. Für ein größeres Engagement ist die Region für verantwortungsvolle Investoren einfach zu riskant. Diese Lücke füllen derzeit dubiose Händler und „Abenteurer".

Wen meinen Sie?

Dies sind in der Regel Geschäftsleute, die die hohen Risiken nicht scheuen, dafür aber auch keinerlei Investitionen tätigen. Sie agieren nach der Formel *high risks, high profits, no standards*. Oft sitzen diese Akteure auch gar nicht im Kongo selbst, sondern irgendwo in der Schmuggelkette über Nachbarländer in den Mittleren Osten oder nach Asien. Leider wird man diese Spezies weder mit dem *Dodd-Frank Act*, noch mit einer europäischen Regulierung vollständig verbannen können. Man darf solche Akteure nicht mit seriös arbeitenden Firmen gleich setzen.

Die EU will in Ihrem Richtlinienvorschlag vom Kongo und den 3TG-Rohstoffen abstrahieren und allgemein riskante Rohstoffgeschäfte regulieren. Kennen Sie andere Risiko- und Konfliktgebiete als den Kongo und seine Nachbarländer, die für die IT-Industrie wichtige Rohstoffe liefern?

Andreas Manhart

Andreas Manhart ist wissenschaftlicher Mitarbeiter beim Öko-Institut und beschäftigt sich mit der Frage, wie Sozial- und Umweltstandards auch in weit verzweigten und globalisierten Produktionsketten sichergestellt werden können. In der Vergangenheit hat er unter anderem zu der Fairness in der IT-Produktion gearbeitet.

Ich halte es für gut, wenn der EU-Vorschlag einen offenen Rahmen setzt, in dem sich auch andere Rohstoffkonflikte integrieren lassen. Es ist sicherlich so, dass Rohstoffe in vielen Konflikten eine Rolle spielen. Insbesondere wird immer wieder die *FARC* in Kolumbien genannt, die sich ebenfalls teilweise über den Goldabbau und -handel finanziert. Und auch bei Edelsteinen und fossilen Energieträgern liegt einiges im Argen.

Allerdings müssen wir auch sehen, dass der Osten der Demokratischen Republik Kongo derzeit eine Sonderrolle einnimmt. Nirgends auf der Welt sind bewaffnete Konflikte dieser Größenordnung so eng mit der Ausbeutung von Erzen und Metallen verknüpft. Und vor allem ist dieser Zusammenhang sehr gut und lückenlos dokumentiert. Denn für den Kongo erhält die Welt nun seit über 10 Jahren alle sechs Monate den Bericht einer UN Expertengruppe. Und diese Berichte gehen jedes Mal auf den Rohstoffabbau und dessen Verwickelung in die dortigen Konflikte ein.

Deshalb sind wir der Meinung, dass man neben den Nachweispflichten auch Positivanreize für verantwortungsvolles Engagement im Bergbau des Kongos schaffen muss. Zudem sollte man auch die Angebote der Industrie ernst nehmen. Bei einer vernünftigen Einbindung der Industrie wäre es aus meiner Sicht durchaus denkbar, dass diese in substanzieller Weise Vor-Ort-Projekte unterstützt und vorantreibt.

Was sind Ihre wichtigsten drei Empfehlungen an die EU-Gesetzgebung?

Zuallererst begrüßen wir die EU-Initiative zu Konfliktrohstoffen. Das ist ein lange überfälliger Schritt. Insofern wollen wir die EU-Kommission ermutigen, den eingeschlagenen Weg auch gegen Widerstände fort zu setzen.

In der konkreten Ausgestaltung halten wir es für sehr wichtig, eine Balance zwischen Transparenzanforderungen und Anreizen für verantwortungsvollen Bergbau vor Ort zu finden. Wenn wir all unsere Aufmerksamkeit darauf lenken, dass ja keine Konfliktrohstoffe mehr in unsere Produkte gelangen, dann erlangen wir vielleicht ein reines Gewissen, nützen tut es aber zuallererst einmal den global tätigen Wirtschaftsprüfungsunternehmen, die viel Geld mit der Nachweisführung verdienen.

Zudem würden wir es begrüßen, wenn die Angebote der Industrie zumindest gehört werden würden. Das sollte nicht im Hinterzimmer geschehen, sondern unter Einbezug von NGOs, den kirchlichen Hilfswerken und auch Akteuren aus der Region.

Zudem denke ich, dass sich bei diesem Thema viele Akteure von alten Denkmustern verabschieden müssen. So ist das oft kommunizierte Täter-Opfer-Schema (z. B. *„… die Industrie ist an einer Fortsetzung des Konfliktes interessiert um an billige Rohstoffe zu gelangen …“*) am Beispiel des Kongos einfach nicht haltbar. Umgekehrt muss natürlich auch stärker anerkannt werden, dass viele NGOs schon seit langer Zeit auf das Thema hinweisen und bislang nur wenig Gehör gefunden haben.

Anmerkungen

1 *Siehe genauer unter http://de.wikipedia.org/wiki/Konfliktrohstoff*
2 *Siehe http://trade.ec.europa.eu/consultations/?consul_id=174*
3 *Als PDF erhältlich unter http://www.oeko.de/files/forschungsergebnisse/application/octet-stream/download.php?id=1809*

CC BY

Dieser Text erschien im September 2013 im Blog *Faire Computer* des FIfF unter *http://blog.faire-computer.de/interview-manhart-oeko-institut/*. Der Blog thematisiert regelmäßig neue Entwicklungen im Bereich Faire Computer und ist empfehlenswert für alle, die am Ball bleiben wollen. Begleitend twittern wir Neuigkeiten per *@FaireComputer*. Siehe auch *www.faire-computer.de* für eine Übersicht unserer Aktivitäten.

Peter Pawlicki

Arbeiter_innen verlassen die Fabrik

Arbeitskämpfe in der chinesischen Elektronikindustrie

Arbeitskämpfe in China sind zahlreich und werden in den entwickelten Industrienationen kaum wahrgenommen. Seit 2010 werden vermehrt offensive Forderungen von den Arbeiter_innen formuliert. Wanderarbeiter_innen spielen eine entscheidende Rolle bei diesen Veränderungsprozessen.

Am 17. Mai 2010 verlassen Arbeiter_innen einer Getriebefabrik von *Honda* ihre Arbeitsplätze und gehen auf die Straße von Nanhai (Provinz Guangdong): sie streiken und fordern substanzielle Lohnerhöhungen.[1] Mehr als 1.800 Arbeiter_innen beteiligen sich und legen die gesamte chinesische Produktion von Honda tagelang lahm. Gleichzeitig lösen sie damit eine landesweite Streikwelle in der Automobilindustrie aus, in deren Verlauf Fabriken von *Hyundai*, *Chrysler* und *Toyota* bestreikt werden und für kurze Zeit schließen müssen. Selbst eine Begrenzung der Berichterstattung kann die Streiks nicht eindämmen, die sich bis Ende Juli hinziehen. Die Streiks werden größtenteils von Wanderarbeiter_innen organisiert und durchgeführt.

Der Streik bei Honda in Nanhai wird als Wendepunkt der Arbeiterkämpfe in China wahrgenommen, der den Beginn einer offensiveren Phase markiert. Statt wie bisher Arbeitskämpfe auf defensive Ziele wie die Verteidigung oder den Erhalt grundlegender Rechte zu beschränken, werden nunmehr weitergehende Forderungen formuliert. Lohnerhöhungen, die über den rechtlich zugestandenen Rahmen hinausgehen, sind dabei zen-

Abbildung 1: Streik bei Nokia in Dongguan, China
Foto: China Labour Watch 2013

trale Forderungen. Aber auch der Ruf, eigene Gewerkschaften wählen zu dürfen, wird stärker.

Diese Veränderungen sind auch in der Elektronikindustrie in China zu beobachten, und sie gehen, wie im gesamten Produktionssektor des Landes, mit einem Anstieg der Arbeitskämpfe insgesamt einher. Obwohl Streiks in China nicht grundsätzlich verboten sind, ist ihre Rechtmäßigkeit unklar. So hängen staatliche Sanktionen gegen betriebliche Arbeitskämpfe immer stark von der lokalen und nationalen politischen Gemengelage ab. Offizielle Zahlen zu Streiks sind in China nicht vorhanden, da sie in der Kategorie sogenannter Massenzwischenfälle untergehen, deren Zahl landesweit von 9000 in 1994 auf 18000 in 2010 angestiegen ist. Die Arbeitskämpfe in China sind meist von kurzer Dauer und hoher Militanz.

Der seit einiger Zeit immer weiter zunehmende Arbeitskräftemangel, ausgelöst u. a. durch die *Ein-Kind-Politik*, hilft die strukturelle Macht der Arbeiter_innen zu erhöhen. Gleichzeitig ist ein kultureller Wandel bei den Wanderarbeiter_innen festzustellen. Die Rückkehr in das Heimatdorf nach ein paar Jahren der harten und entbehrungsreichen Arbeit hat als Lebensentwurf ausgedient. Die jungen Wanderarbeiter_innen wollen heute in den Metropolen bleiben und die dort gebotenen Möglichkeiten auskosten. Die sich so formierenden Anspruchshaltungen werden von rechtlichen Entwicklungen, wie z. B. dem Arbeitsvertragsgesetz von 2008, flankiert, die den Schutz der Arbeiter_innen erweitert haben. Das von der Kommunistischen Partei Chinas verfolgte Ziel der „harmonischen Gesellschaft" führt zu einem teilweise veränderten Umgang mit sozialen Konflikten, die nicht mehr vollständig eliminiert werden. Kontrolle findet heute vermehrt durch die Bereitstellung legitimer Kanäle statt, etwa des Rechtsweges. Das schließt brutale Sanktionen jedoch in keiner Weise aus.

Die Wanderarbeiter_innen sind das Fundament, auf dem die Produktion in den chinesischen Standorten der global organisierten Elektronikindustrie fußt. Ihr durch das *Hukou-System* regulierter sozio-ökonomischer Status hat erst die viel gerühmten Flexibilitäts- und Lohnkostenvorteile ermöglicht. Das Hukou-System entstammt der frühen chinesischen Kommandowirtschaft und bindet Sozialrechte an einen bestimmten Ort, meist den der Geburt. In dem sie sich auf der Suche nach Arbeit in eine andere Stadt aufmachen, lassen die Wanderarbeiter_innen ihre Sozialrechte zurück. Öffentliche Dienstleistungen wie Schulen, Krankenhäuser, Kranken- und Rentenversicherung stehen ihnen am neuen Wohnort nicht mehr zu. Die Situation der Arbeiter_innen im Betrieb wird durch das Hukou-System weiter prekarisiert, das sich auch negativ auf die Möglichkeiten von Arbeitskämpfen auswirkt.

Aktivisten wichtiger als der Gewerkschaftsbund

Von den staatlichen Gewerkschaften können die Arbeiter_innen meist keine Hilfe erwarten.[2] Sie verhalten sich bei betrieblichen Auseinandersetzungen meist passiv, bzw. stehen auf der Seite des Managements. Auch bei privaten und ausländischen Unternehmen, wo Gewerkschaften durchaus anzutreffen sind, ist dies der Fall. Regelmäßig werden Gewerkschaften von der Unternehmensleitung eingesetzt und nicht von den Arbeiter_innen gewählt. Selbst bei gewählten betrieblichen Gewerkschaften ist Vorsicht geboten. So ist die Ankündigung von *Foxconn*, in seinen Betrieben die Gewerkschaften wählen zu lassen, von Aktivisten mit Hinweis auf die problematische Kandidatenfindung nicht mit Begeisterung aufgenommen worden. Die Aktion hat die klare Stoßrichtung, gutes Marketing für die Nachhaltigkeitsberichte der belieferten Großkunden von Foxconn zu bieten. Trotz der problematischen Lage wird von einigen Beobachtern festgestellt, dass es im Allchinesischen Gewerkschaftsbund Anzeichen von Veränderung gibt und sich Vertreter kritischer Fraktionen in einigen lokalen Strukturen durchsetzen können.

Viel wichtiger als die Gewerkschaften sind die verschiedenen organisierten und unorganisierten Aktivist_innen in China, die an der Verbesserung der Situation der Arbeiter_innen arbeiten. Schulungen, juristische Hilfe und die Unterstützung bei sozialen Krisensituationen sind wichtige Momente dieser Arbeit. Die von Organisationen wie *SACOM* und *China Labor Watch*, unter oft schwierigen Umständen, angefertigten Berichte und Fallstudien zu den Arbeitsbedingungen in den Produktionsstätten in China helfen, die globale Öffentlichkeit über die wirkliche Lage der Arbeiter_innen zu informieren. Sie setzen damit den meist rosig gehaltenen Berichten der Hersteller etwas entgegen.

Streiks in der Elektronikindustrie

Von den Wanderarbeiter_innen in der Elektronikindustrie werden vergleichsweise offensive Forderungen formuliert. Am 29. März 2012 gehen mehr als 700 Wanderarbeiter_innen von *Ohms Electronics*, einem Tochterunternehmen von Panasonic, das elektrische Schalter fertigt, in Shenzhen auf die Straße. Sie sitzen drei Tage lang relativ friedlich auf Plastikstühlen vor der Fabrik. Neben Forderungen nach einem höheren Einkommen und der Möglichkeit, Urlaubsanträge stellen zu können, verlangen sie auch demokratische Wahlen ihrer Gewerkschaft im Betrieb. Viele der Beschäftigten haben erst kurz zuvor erfahren, dass es eine Gewerkschaft in ihrem Betrieb gibt, welche jedoch vom Management eingesetzt wurde. Trotz einiger Widerstände versteht der lokale Gewerkschaftsverband in Shenz-

hen das Anliegen und unterstützt die Arbeiter_innen bei den Wahlen. Es ist unklar, ob es sich bei dem im Mai 2012 neu gewählten Gewerkschaftsvorsitzenden um eine_n Produktionsarbeiter_in handelt, wie in einigen Meldungen zu lesen ist. Festzustehen scheint jedoch, dass das neu gewählte betriebliche Gewerkschaftskomitee rund zur Hälfte aus Streikteilnehmer_innen besteht.

Die Arbeiter_innen bei Ohms Electronics sind durch die Erfolge selbstsicherer geworden. Nur neun Monate nach der Wahl kommt es Anfang 2013 zu neuen Protesten, ausgelöst durch die Weigerung des Unternehmens, unbefristete Verträge anzubieten, wozu es rechtlich verpflichtet ist.[3] Die Arbeiter_innen fühlen sich von ihrem neuen Gewerkschaftsvorsitzenden in dieser Frage in Stich gelassen. Mit einem Aushang am Fabriktor fordern sie seine Absetzung und Neuwahlen.

Die Restrukturierung der Elektronikbranche entwickelt sich immer weiter. Die 2011 angekündigte Übernahme der Mobiltelefonsparte von *Motorola* durch *Google* ist der erste große Schritt von bisher auf Software spezialisierten Anbietern in die Hardwareproduktion.[4] Den bislang letzten Höhepunkt markiert die diesjährige Übernahme der Handysparte von *Nokia* durch *Microsoft*. Gleichzeitig bleiben jedoch bestimmte Strukturmerkmale bestehen. So beginnt Google Ende 2012 damit, die Produktionsstandorte von *Motorola Mobility* an *Flextronics* zu verkaufen. Diese Auslagerungen machen den in Singapur beheimateten Kontraktfertiger zum weltweit größten Zulieferer von Fertigungsdienstleistungen von Motorola.

In Tianjin, wo sich der chinesische Produktionsstandort von Motorola Mobility befindet, löst diese Restrukturierung in Googles Zuliefererkette einen Streik aus. Im April 2013 blockieren rund 7000 Arbeiter_innen das Werkstor und fordern höhere Abfindungen. Da Flextronics ankündigt, nach der Übernahme neue Arbeitsverträge anbieten zu wollen, was als verklausulierte Formulierung für schlechtere Verträge verstanden werden kann, wollen sich die Arbeiter_innen so den Übergang oder Austritt erleichtern.

Obwohl Arbeitskämpfe in China zahlreich, kurz und oft militant sind, bleiben sie gleichzeitig in den entwickelten Industrienationen unbemerkt. Auch die zahlreichen Selbstmorde von Arbeiter_innen bei Foxconn haben an dieser Situation nur sehr wenig geändert. Die globale Elektronikindustrie mit ihren Produktionsstandorten in China und den weltweit verteilten Märkten ist eine Arena, in der das diskursive Wegsehen angegangen werden muss. Die in der Industrie herrschende hohe Flexibilität, drastisch verkürzte Produktlebenszyklen und die immense Fragmentierung der Zuliefererketten führen jedoch zu einer komplexen Problemlage. Der extreme Margendruck wird an die schwächsten Glieder in der Kette weitergegeben, an die Arbeiter_innen. Gleichzeitig erlaubt die Komplexität der Produktionsketten den Herstellern Taktiken der Verschleierung.

Die Erfolge der chinesischen Arbeiter_innen können nur als erste Schritte auf einem langen Weg betrachtet werden. Sie haben ein riesiges Feld vor sich. Nicht nur kämpfen sie für bessere Arbeitsbedingungen. Sie müssen gleichzeitig eine fundamentale Veränderung der bestehenden Gewerkschaftsstrukturen durchsetzen, in einem sich weiterhin als kommunistisch titulierendem Land.

Anmerkungen

1 *Den Streikenden gelang es, Lohnerhöhungen von 32 % durchzusetzen.*
2 *In China sind unabhängige Gewerkschaften nicht zugelassen.*
3 *Das Arbeitsvertragsgesetz von 2008 legt u. a. fest, dass nach zwei befristeten Arbeitsverträgen die Arbeiter_in nur auf Grundlage eines unbefristeten Arbeitsvertrages weiter beschäftigt werden kann.*
4 *Zwar hat Microsoft mit der Xbox den Einstieg in die Hardwareproduktion genommen, jedoch war dies in einen mit den Stückzahlen von Mobiltelefonen unvergleichlich kleineren Markt. Es geschah auch unter den Vorzeichen einer starken vertikalen Spezialisierung, bei der die Fertigung von Kontraktfertigern übernommen wurde (u. a. durch Flextronics).*

Referenzen

Chan, Jenny, Ngai Pun und Mark Selden (2013), The politics of global production: Apple, Foxconn and China's new working class, in: New Technology Work and Employment, 28:2, 100-115

Elfstrom, Manfred und Sorosh Kuruvilla (2013), The Changing Nature of Labor Unrest in China, Paper presented at the International Labor and Employment Relations Conference, 2.-5. Juli 2012, Philadelphia

Elfstrom, Manfred (2013), China Strikes – Mapping labor unrest across China, http://chinastrikes.crowdmap.com/

Friedman, Eli (2012), China in Revolt, http://jacobinmag.com/2012/08/china-in-revolt

Loon Yu, Au und Bai Ruixue (2012), New Signs of Hope: Resistance in China Today, http://www.worldlabour.org/eng/print/515

Lüthje, Boy 2013: Corporatism with Chinese Characteristics? Regimes of Production in German Transnationals in China, in: Anita Chan (Hg.): Chinese Labor in Comparative Perspective. Ithaca, NY: ILR Press.

Scherrer, Christoph (2011), China's Labor Question, http://www.global-labour-university.org/fileadmin/books/CLQ_full_book.pdf

Peter Pawlicki

Peter Pawlicki hat viele Jahre am Institut für Sozialforschung in Frankfurt zur Globalisierung in der Elektronikindustrie geforscht. Im Rahmen seiner Promotion untersuchte er Kontrolle und Organisation der Arbeit von Chipdesignern in Osteuropa. Zurzeit arbeitet er als Projektsekretär beim Vorstand der IG Metall. (Foto: Andreas Pleines)

Mario Dziamski

Produkt-Rankings bringen Licht in den Schatten

Elektronikmarken und Nachhaltigkeit aus der Sicht des Verbraucherportals *Rank a Brand*

Wie verhält es sich mit Nachhaltigkeit und Fairness bei Apple, Samsung & Co.? Was sind die wichtigen Themen? Diese und andere Fragen werden aus der Perspektive des Rank a Brand e. V. beleuchtet*, der es sich zur Aufgabe gemacht hat, Verbrauchern aufzuzeigen, wie nachhaltig ihre Lieblingsmarken sind.*

Foxconn ist seit ungefähr 2010/2011 der wohl bekannteste Zuliefererbetrieb der Welt. Ob unwürdige Arbeitsbedingungen oder gar Suizide, das taiwanesische Unternehmen Foxconn ist zum Synonym globaler Missstände für die Produktion westlicher Konsumgüter geworden. Im Jahr 2011 wurde Foxconn unter anderem für den Negative Award *Public Eye* nominiert. In Verbindung mit Foxconn wird vor allem ein Unternehmen gebracht: *Apple Inc*. Obwohl auch andere Elektronikhersteller bei Foxconn produzieren lassen – z. B. Nokia und Sony – wird vor allem Apple als unverantwortliches Unternehmen hervorgehoben.

Das Unternehmen, oder besser die Marke Apple erleidet damit dasselbe Schicksal wie andere große Marken: Ob *H&M* bei Modehäusern, *Coca-Cola* bei Softdrinks oder *McDonalds* bei Fast Food Restaurants – die populärsten Markenhersteller werden in Sachen Unternehmensverantwortung gleichzeitig am stärksten in die öffentliche Mangel genommen. Aufgrund ihrer Strahlkraft, ihrer enormen finanziellen Nachhaltigkeit sowie der weitreichenden Verknüpfung in den globalen Produktionsmärkten werden diese Unternehmen jedoch völlig zu Recht in die Mitte des Interesses gerückt. Die Hebelkraft im Sinne sozial und ökologisch nachhaltiger Produktionsbedingungen ist bei Apple, H&M, Coca-Cola oder McDonalds im Vergleich zu anderen Markenherstellern klar größer.

Dennoch, Unternehmensverantwortung bei Verbrauchermarken beschränkt sich nicht allein auf die populärsten, erfolgreichsten oder global verflochtensten Markenhersteller. Ebenso beschränkt sich Unternehmensverantwortung nicht allein auf Produktionsbedingungen in den Fabriken der Zulieferer. Unternehmerische Verantwortung ist weit mehr und muss wesentlich ganzheitlicher betrachtet werden.

Bei *Rank a Brand* haben wir Elektronikmarken auf ihre soziale Nachhaltigkeit in der Zuliefererkette sowie ökologische Nachhaltigkeit mit Bezug auf Klima- und Umweltschutzaktivitäten untersucht. Aus der Perspektive gut informierter sowie sehr interessierter Verbraucher haben wir rund 20 Bewertungsfragen für Elektronikhersteller entwickelt. Anhand dieser Bewertungsfragen möchten wir beispielsweise Kameramarken wie *Nikon* oder *Canon*, Spielkonsolenhersteller wie *Nintendo* oder *Sony*, Handyhersteller wie *Nokia* oder *Samsung* oder eben Computer- und/oder Smartphone-Hersteller wie Apple oder Microsoft miteinander vergleichen.

Transparenz notwendig für eine gute Beurteilung

Hinterlegt mit fundierten und transparent gemachten Bewertungskriterien zu jeder einzelnen Bewertungsfrage analysieren wir die Nachhaltigkeitsberichterstattung der Markenhersteller. Dabei ist es unser Ansatz, dass wir grundsätzlich keine Fragebögen an die Hersteller mit Bitte um Antwort schicken. Wir suchen nach Antworten auf unsere Fragen in den veröffentlichten Nachhaltigkeits- bzw. CSR-Berichten. Grundbedingung für ein möglicherweise gutes Ranking bei *Rank a Brand* ist somit eine veröffentlichte, transparente Berichterstattung zur Unternehmensverantwortung. Unternehmen, die das nicht tun, verwirken also von vornherein Chancen auf eine positive Bewertung. Dieser Ansatz hat Methode. Wir fordern Markenhersteller dazu auf, dass sie ihrem wichtigsten Stakeholder, dem Konsumenten, kontinuierlich und möglichst aktuell öffentlich Einblick zu den geplanten und getroffenen Maßnahmen sowie gesteckten und erreichten Zielen gewähren.

Zu unseren Rankings für Elektronikmarken haben wir daher beispielsweise die folgenden Fragen entwickelt:

- Hat der Markenhersteller in den vergangenen fünf Jahren die CO_2-Bilanz der eigenen Geschäftsbereiche bereits um mindestens 10 Prozent reduziert oder kompensiert?
- Hat der Markenhersteller PVC und bromierte Flammschutzmittel bereits aus allen Anwendungen entfernt?
- Bezieht der Markenhersteller zumindest fünf Prozent des Plastiks aus aufbereitetem Material und macht die Marke eindeutige Angaben, ob sie diesen Anteil bis 2025 auf mindestens 25 Prozent erhöhen will?
- Hat der Markenhersteller einen Verhaltenskodex *(Code of Conduct)*, in dem folgende Standards eingeschlossen sind: keine Zwangs- oder Sklavenarbeit, keine Kinderarbeit, keine Diskriminierung jeglicher Art sowie ein sicherer und hygienischer Arbeitsplatz?
- Hat der Markenhersteller eine Liste der Zulieferer veröffentlicht, die gemeinschaftlich mehr als 90 Prozent des Einkaufsvolumens beitragen?

Die Ergebnisse zu unseren Untersuchungen zeigen auf, dass es kein Unternehmen gibt, welches sich als klarer Vorreiter bezüglich Unternehmensverantwortung erweist. Der niederländische Elektronikkonzern *Philips* sowie der finnische Handyhersteller Nokia haben sich bisher entsprechend unserer Bewertungskriterien – Stand Mitte 2012 – noch als die nachhaltigsten Unternehmen hervorgetan. Philips kann vor allem gute Ergebnisse beim Klimaschutz vorweisen, Nokia dagegen beim Klima- und Umweltschutz. Jedoch auch diese beiden Unternehmen befinden sich insgesamt eher am Anfang, um ein wirklich nachhaltiger Hersteller von Elektronikprodukten zu werden. Eher ist es sogar so, dass der Status Quo auch bei Nokia und Philips bei einigen Themen mitunter sehr zweifelhaft ist.

Standards bei Sozialkriterien noch gering

Sowohl bei Nokia als auch Philips bleibt zum Beispiel unklar, wie fair die Produkte hergestellt werden. Allein die wesentlichste Grundlage für faire Arbeitsbedingungen in Zulieferbetrieben – der *Code of Conduct* – weist wie bei Apple, Samsung oder Dell deutliche Schwächen auf. Wichtige menschenrechtliche Bedingungen für eine Auftragserteilung an einen Zulieferer, zum Beispiel Arbeitszeit, Lohn oder gewerkschaftliches Vereinigungsrecht, wurden bisher nur sehr ungenügend oder gar nicht im *Code of Conduct* formuliert. Das sensibelste Thema, Kinderarbeit, haben jedoch alle genannten Unternehmen in ihrem *Code of Conduct* klar als nicht gestattet herausgestellt. Daran wird deutlich, dass Markenhersteller – über die Elektronikhersteller hinaus – auf öffentlichen Druck reagieren. Das Verbot von Kinderarbeit im *Code of Conduct* bedeutet allerdings nicht, dass dies in Zulieferbetrieben tatsächlich unterbunden wird.

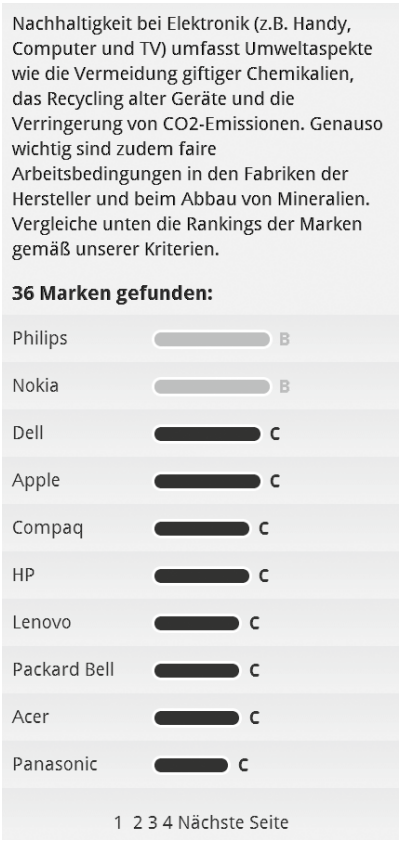
Es bedarf weiterer Maßnahmen der Hersteller, um problematische Umstände in Zuliefererbetrieben zu lösen. Neben regelmäßigen, möglichst unabhängigen Audits in den Fabriken ist die Zusammenarbeit mit anderen Stakeholdern wichtig. Denn kein noch so großer Markenhersteller hat gute Chancen auf Verbesserungen in der Zulieferkette – auch mit Bezug auf das Thema Konfliktmineralien – im Alleingang.

Wichtig ist daher unter anderem das aktive Mitwirken in Initiativen, bei denen die Industrie und Nichtregierungsorganisationen beteiligt sind. Der Beitritt von Apple zur *Fair Labor Association*, einer Organisation zur Kontrolle von Arbeitsstandards, ist in dem Zusammenhang ein guter Schritt in die richtige Richtung. Es geschah wahrscheinlich aufgrund des besonderen öffentlichen Drucks. Realistische Hoffnungen auf baldige, grundlegende Änderungen der Zustände in den Fabriken sollte man sich allerdings nicht machen. Es wird sehr wahrscheinlich noch viele Jahre dauern, bis die konfusen sowie unfairen Geflechte innerhalb der Produktionsketten von Elektronikmarken in Ordnung gebracht sind.

Was zudem die Hoffnung mindert, ist der Umstand, dass sich einzelne Hersteller ihre Verantwortung nicht ernsthaft eingestehen. Ein Beispiel dafür lieferte Samsung im Jahr 2011. Samsung wurde wegen schwerer Vorwürfe zu Arbeitsbedingungen und daraus folgenden Erkrankungen in Produktionsstätten für den *Public Eyes Negative Award* nominiert, wies jedoch einen Großteil der Verantwortung von sich.

Es bleibt festzuhalten: Apple ist bei Weitem nicht das einzige Unternehmen, welches einen langen Weg in Sachen Unternehmensverantwortung zu gehen hat. Foxconn ist nicht die einzige Fabrik, in der es Menschen für unseren von Technologie geprägten Lebensstil mitunter sehr schlecht ergeht. Die Branche für elektronische Konsumprodukte ist zu einer gigantischen, globalen Industrie herangewachsen. Die negativen Auswirkungen auf Mensch und Natur sind weit reichend und beschränken sich nicht auf die Zulieferkette. Die Auswirkungen auf das Klima, der Einsatz bedenklicher Chemikalien, Konfliktmineralien oder riesige Müllmengen stellen ebenso ernsthafte Probleme dar.

Die Markenhersteller müssen auch die Probleme anpacken. Der durch unser Ranking dargelegte Status Quo zeigt, dass global

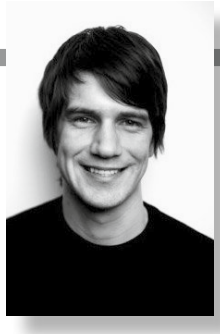


http://rankabrand.de/elektronik
abgerufen am 18.11.2013

agierende Elektronikkonzerne bei vielen Themen der sozialen und ökologischen Nachhaltigkeit am Anfang stehen. Zu dieser Aussage kommen auch die Bewertungen anderer Rankings. Sowohl der *Greenpeace Guide to Greener Electronics*, *Goodguide*, *Climate Counts* oder *Tomorrow´s Value Ranking* zeichnen ein sehr ähnliches Bild.

CC BY

Mario Dziamski



Ende 2010 habe ich – **Mario Dziamski** – zum ersten Mal von *Rank a Brand* aus den Niederlanden gehört. Anfang 2011 habe ich Rank a Brand in Deutschland gegründet. Warum? Ich war der Meinung, dass es Rank a Brand eigentlich in jedem Land geben sollte. Ich bin begeistert von den Möglichkeiten, die in Rank a Brand stecken und möchte sie im Sinne einer nachhaltigen Zukunftsgestaltung umsetzen. Ich leite den Aufbau des *Rank a Brand e. V.* und studiere Volkswirtschaftslehre an der Universität Potsdam.

Anna Lefik

Fairer Handel –

ein wichtiger Baustein

Als Fairer Handel (englisch Fair Trade*) wird ein kontrollierter Handel bezeichnet, bei dem die Produzenten für die gehandelten Produkte einen von Fair-Trade-Organisationen festgelegten Mindestpreis erhalten, der konstant ist und über dem Weltmarktpreis liegt. In der Produktion sollen außerdem internationale sowie von den Organisationen vorgeschriebene Umwelt- und Sozialstandards eingehalten werden. Fair gehandelte Produkte umfassen vor allem landwirtschaftliche Erzeugnisse sowie Produkte des traditionellen Kunsthandwerks. Zunehmend findet man zertifizierte Produkte aber auch bei Industrieprodukten wie Bekleidung. In der IT steckt der Faire Handel dagegen noch in den Kinderschuhen.*

Faire Produktvielfalt: Elektronik fehlt noch komplett (Quelle: Alle Rechte: TransFair e. V., http://www.transfair.org)

Das Fairtrade-Siegel der deutschen Siegelorganisation *TransFair e. V.* erfreut sich eines hohen Bekanntheitsgrades. Ökonomie, Ökologie und Soziales sind die drei Säulen der Fairtrade-Standards. Die Standards werden von *Fairtrade Labelling Organizations International* (FLO), der Dachorganisation der Fairtrade-Siegelinitiativen, entwickelt und bilden die Spielregeln des Fairen Handels. Fairtrade-Produzenten und Händler müssen die Standards einhalten – nur so lange dürfen sie ihre Produkte mit dem Fairtrade-Siegel auszeichnen.

Keine Almosen

Viele Menschen assoziieren mit dem Fairen Handel eine Art Entwicklungshilfe, aber der Faire Handel soll den Produzenten – wie jeder andere Handel auch – Wohlfahrt durch ihre eigene Leistung und die Teilnahme am Welthandel bringen. Deutschland ist eine Exportnation und darauf beruht unser Wohlstand. Die Entwicklungsländer exportieren auch, vor allem Rohstoffe wie Kaffee, Tee, Reis, Kakao und Zucker, aber die Wohlfahrt bleibt aus. Das liegt an geringen und schwankenden Preisen des Weltmarktes sowie am ausbeuterischen lokalen Zwischenhandel. Insbesondere Kleinbauern können ihre Waren nicht direkt an die Importeure verkaufen. Die produzierten Mengen sind zu gering und es fehlt die Infrastruktur zum Vertrieb ihrer Produkte. Sie sind auf Zwischenhändler angewiesen.

Der Faire Handel etabliert einen internationalen Handel unter gerechten Konditionen. Das wird erreicht durch einen über dem Weltmarkt liegenden Preis, der die Kosten einer nachhaltigen Produktion deckt. Weitere Aspekte sind die Möglichkeit zur Vorfinanzierung, langfristige Handelsbeziehungen sowie eine Fairtrade-Prämie, die den Produzentenorganisationen die Möglichkeit gibt, in gemeinsame Projekte aus Bereichen wie Bildung, Gesundheit oder Infrastruktur zu investieren.

Historisch entstand Fairer Handel aus einer Reihe glaubensbasierter und säkularer alternativer Handelsorganisationen sowie durch Engagement der Zivilbevölkerung in den Industriestaaten.

Standards

Verschiedene unabhängige Studien haben sich in den letzten Jahren mit der Frage nach der Wirkung des Fairen Handels auf die beteiligten Produzentenorganisationen befasst. Die positiven Auswirkungen auf die ökonomische Stabilität der Kooperativen, aber auch auf deren organisatorische Stärkung, wurden von verschiedenen Seiten bestätigt. Demnach hat die Präsenz von Fairtrade-zertifizierten Kooperativen oder Plantagen in einem bestimmten Gebiet positive Auswirkungen nicht nur auf die Produzentenorganisation, sondern auch auf die ländliche Entwicklung der jeweiligen Region.

Die Bedingungen, unter denen der Faire Handel zwischen den Organisationen und Unternehmen stattfindet, können variieren, unterliegen aber gemeinsamen Prinzipien. Grundsätzlich können die Prinzipien folgenden drei Dimensionen zugeordnet werden:

- Ökologie: Erhaltung von Natur und Ökosystemen für nachfolgende Generationen.
- Ökonomie: Verantwortungsvoller Umgang mit ökonomischen Ressourcen mit dem Ziel der Wohlstandsvermehrung.
- Soziales: Entwicklung einer Gesellschaft, an der alle Menschen in gleichem Maße partizipieren.

Die Dreidimensionalität des Fairen Handels entspricht dem Konzept von nachhaltiger Entwicklung, wie sie in der Präambel zum EU-Vertrag enthalten ist. Dieses Konzept geht auf die

United Nations Conference on Environment and Development (UNCED) zurück, im Rahmen derer sich die Völkergemeinschaft bereits 1992 zum Leitbild nachhaltiger Entwicklung bekannt hat.

Das Konzept der nachhaltigen Entwicklung kann auf alle Wirtschaftszweige übertragen werden, beispielsweise auch auf die Bekleidungs- oder IT-Industrie. Im Gegensatz zum IT-Sektor gibt es in der Bekleidungsindustrie bereits positive Beispiele. Der bekannteste Standard für nachhaltige Textilien ist der *Global Organic Textile Standard* (GOTS). Die GOTS-Zertifizierung hat zum Ziel, ökologische und soziale Standards für Textilien von der Ausgangsfaser bis zum Endprodukt zu definieren.

Entwickelt wurde der Standard vom *Internationalen Verband der Naturtextilwirtschaft*, IVN, (Deutschland) zusammen mit der *Soil Association*, SA, (England), der *Organic Trade Association*, OTA, (USA) und der *Japan Organic Cotton Association* (JOCA) (Japan).

Übertragbar oder nicht?

Die IT-Branche hat mit der Bekleidungsindustrie mehrere Gemeinsamkeiten. Zur Wertschöpfungskette sowohl von IT-Produkten als auch Kleidungsstücken gehören grob skizziert folgende Schritte: Rohstoffgewinnung, Produktion in Fabriken, Transport, Verkauf durch Markenfirmen/Distributoren/Discounter und Nutzung. Bei IT-Produkten spielen außerdem die Verschrottung und Rohstoffrückgewinnung eine wichtige Rolle. All diese Phasen im Lebenszyklus der Produkte können nach dem dreidimensionalen Konzept nachhaltiger Entwicklung gestaltet werden.

Folgende arbeitsrechtlichen Kriterien, die dem GOTS-Siegel zu Grunde liegen, sollten auch in einen fairen IT-Standard einfließen:

- Verbot von Zwangs- und Kinderarbeit,
- Versammlungsfreiheit und das Recht auf Kollektivverhandlungen,
- Gesundheitsschutz am Arbeitsplatz,
- Arbeitszeiten gemäß gültigen nationalen Gesetzen und Industriestandards,
- angemessene Löhne für reguläre Arbeitszeiten,
- Vergütung von Überstunden,
- Verbot jeglicher Diskriminierung,
- Einhaltung umweltschutzrechtlicher Auflagen.

Alle im Produktions- und Distributionsverfahren befindlichen Betriebe müssen einer jährlichen, unangekündigten Inspektion zustimmen. Die Einhaltung der Standards wird von einer neutralen Kontrollstelle geprüft, Verstöße werden verfolgt und geahndet.

Eine weitere Gemeinsamkeit von IT- und Bekleidungsbranche ist die Beherrschung durch multinationale Konzerne. Es ist nicht leicht, sie dazu zu bewegen, dass sie sich selbst faire Produktionsbedingungen auferlegen. Dennoch ist es in der Bekleidungsbranche bereits gelungen. Beispielsweise hat Tchibo 2005 unter öffentlichem Druck die Einkaufspraxis geändert. Dieser öffentliche Druck wurde durch die *Kampagne für Saubere Kleidung (Clean Clothes Campaign)* erzeugt. Clean Clothes Campaign wurde in den Niederlanden 1989 als Reaktion auf Berichte über skandalöse Arbeitsbedingungen in Zulieferbetrieben von C&A gegründet. Heute gibt es in 15 europäischen Ländern derartige Kampagnen, unter anderem in Deutschland.

Die Kampagne für Saubere Kleidung informiert Konsumentinnen und Konsumenten kontinuierlich über die Produktionsverhältnisse in der Bekleidungsindustrie und bringt Arbeitsrechtsverletzungen bei Textilunternehmen ans Licht. Mit Eilaktionen mobilisiert die Kampagne tausende Menschen weltweit. Sie fordert die Unternehmen auf, internationale Arbeitsstandards einzuhalten und gegen Arbeitsrechtsverletzungen in Zulieferbetrieben vorzugehen. Die Unternehmen geraten mit negativen Schlagzeilen in die Medien und werden aus Furcht vor einem drohenden Imageschaden aktiv.

Um die IT-Branche ebenso in Bewegung zu versetzen, wird noch viel zivilgesellschaftliches Engagement notwendig sein. Die ersten Schritte sind aber beispielsweise mit dem Netzwerk *GoodElectronics* bereits gemacht.

Der Faire Handel ist ein nachhaltiges Entwicklungskonzept. Er fordert gesellschaftliche Werte ein, die von höchster politischer Ebene bereits seit vielen Jahren propagiert werden.

Referenzen

http://www.fairtrade-deutschland.de/fileadmin/user_upload/ueber_fairtrade/fairtrade_wirkt/Impact_Study_2012_Zusammenfassung_der_Ergebnisse.pdf

Hauff, Michael von; Claus, Katja: Fair Trade. Ein Konzept nachhaltigen Handels. Konstanz: UVK Verlagsgesellschaft, 2012.

http://www.fairtrade-deutschland.de/

http://www.cleanclothes.org/

http://www.saubere-kleidung.de/

http://www.global-standard.org/de/

http://www.inkota.de

Anna Lefik

Anna Lefik engagiert sich seit rund fünfzehn Jahren für den Fairen Handel, u. a. mit ihrer unabhängigen Informationsseite *www.fairerhandel-aktuell.de*. Neben ihrer Beschäftigung als Online-Redakteurin schreibt sie ihre Dissertation im Fachbereich Ethnologie.

Stefanie Müller, Eberhard Zehendner

Für *FairIT* sensibilisieren –

Anknüpfungspunkte in Schule und Hochschule

Fair Play bezeichnet nicht nur das Einhalten der Spielregeln,
Fair Play umschreibt vielmehr eine Haltung des Sportlers:
der Respekt vor dem sportlichen Gegner und die
Wahrung seiner physischen und psychischen Unversehrtheit.
Fair verhält sich derjenige Sportler, der vom anderen her denkt.
Deklaration des Internationalen Fair Play-Komitees (CIFP) Oktober 1990

Über Fair Play reden alle – von FairIT *hören wir selten. Warum eigentlich? Ist IT weniger wichtig als Sport? Interessiert das Thema niemand? Oder ist IT immanent unfair? Dreimal können wir ohne große Rückbesinnung mit Nein antworten. Und dennoch: Im Schulunterricht oder in Hochschulcurricula kommt meist nicht einmal der Begriff FairIT vor. Dabei wäre es doch so leicht, gerade dort große, einschlägig arbeitende Zielgruppen zu erreichen.*

Der Themenkomplex *FairIT* ist reichhaltig, kann er doch mindestens in die folgenden drei Richtungen entwickelt werden, die sich teilweise überschneiden: Zunächst können die Wertschöpfungsketten bei der Herstellung und Vermarktung von IT-Produkten untersucht werden. Hierbei lässt sich leicht nachweisen, dass IT vorwiegend unfair produziert wird. Die enormen Gewinne kommen kaum denen zugute, die mit ihrer Arbeitskraft und oft auf Kosten ihrer Gesundheit prominente IT-Produkte herstellen. Dem lassen sich aber auch Projekte gegenüberstellen, mit denen faire IT-Produktion und -Vermarktung angestrebt werden.

Es lässt sich untersuchen, ob der Einsatz von IT-Produkten den Digital Divide tendenziell verringert oder ihn im Gegenteil begünstigt. Ein Schwerpunkt sollte dabei das Herausarbeiten von Gestaltungsalternativen sein. Ein dritter, ins Positive orientierter Ansatz wäre, sich fairen Prozessen in wichtigen gesellschaftlichen Domänen zu widmen, die durch den gezielten Einsatz geeigneter IT unterstützt werden. Zum Beispiel im *Ambient Assisted Living*, um nur ein Stichwort zu nennen, jedoch mit Augenmerk auf mögliches Überschießen der Bemühungen, was in übertechnisierten Umgebungen enden könnte.

Aufmerksamkeit und Problembewusstsein wecken – *FairIT* als Ziel schulischer Bildung

Laut aktueller KIM-Studie 2012 besitzt jedes zweite Kind zwischen sechs und dreizehn Jahren in Deutschland ein eigenes Handy oder Smartphone [KIM 2012, S. 8], etwa vier Fünftel der bis 19-Jährigen einen Computer/Laptop [JIM 2012, S. 7]. Bereits diese beiden Studienergebnisse lassen vermuten, dass Kinder und Jugendliche beim Kauf dieser Geräte maßgeblich entscheiden und so unbewusst Mitverantwortung tragen für Bedingungen, Normen und deren Konsequenzen in der IT-Entwicklung, Produktion und dem Vertrieb. Es scheint unwahrscheinlich, dass diese Faktoren im heimischen Wohnzimmer ein Thema sind. Das Interesse, Gestaltung und Konsum fairer Produkte zu fördern, um einen Zugewinn an fairerem Zusammenleben zu initiieren, ist aber eine gesamtgesellschaftliche Aufgabe, deshalb muss die Sensibilisierung für *Faire IT* im öffentlichen Raum Schule stattfinden. Sie sollte im schulischen Kontext so früh wie möglich beginnen, da die Zielgruppe für technische Geräte immer jünger wird. In der Entwicklungspsychologie (siehe z. B. [Kasten, 2007 bzw. 2009]) besteht ein breiter Konsens, dass Moralerziehung und Werteentwicklung bereits im frühen Kindes- und Jugendalter möglich sind. Diese Fähigkeiten sind Grundlage dafür, dass es auch in der Primarstufe bzw. Sekundarstufe 1 gelingen kann, die Schülerinnen und Schüler auf einen sensibleren Umgang mit Informationstechnik vorzubereiten.

Es liegt nahe, *FairIT* in das Schulfach Informatik[1] einzubetten, weshalb an dieser Stelle ein kurzer Blick in die länderübergreifenden Rahmenrichtlinien sinnvoll ist.

Die Bildungsstandards der *Gesellschaft für Informatik e V. (GI)* greifen *Informatik und Gesellschaft* im eigenständigen Inhaltsbereich *Informatik, Mensch und Gesellschaft* auf [GI 2008, S. 41], der sich in drei Einzelpunkte gliedert: Im zweiten Schwerpunkt werden die *Entscheidungsfreiheit im Umgang mit Informatiksystemen* sowie das persönliche *Handeln in Übereinstimmung mit gesellschaftlichen Normen* in den Vordergrund gestellt. Diese zentrale Festlegung wird explizit für Jahrgangsstufe 8 bis 10 noch einmal präzisiert: *„Schülerinnen und Schüler […] untersuchen an Beispielen die Probleme der Produktion, Nutzung und Entsorgung elektronischer Geräte"* [GI 2008, S. 43]. Die Empfehlungen der GI schreiben *FairIT* also als regulären Unterrichtsgegenstand vor.

Die *Einheitlichen Prüfungsanforderungen in der Abiturprüfung (EPA)* für das Fach Informatik[3] erwähnen *FairIT* nicht direkt, in der allgemeinen Formulierung der fachlichen Inhalte *„gesellschaftliche, ethische und rechtliche Aspekte (z. B. Auswirkungen des Computereinsatzes in der Arbeitswelt und im Freizeitbereich, gesetzliche Rahmenbedingungen)"* [KMK 2004, S. 6], schließen sie aber auch nicht aus.

Die einzelnen Bildungspläne der Länder weichen zwar von den zentralen Empfehlungen ab und sehen *FairIT* selten direkt vor, trotzdem können *FairIT*-Sequenzen im schulischen Kontext erfolgreich sein. Da für die Entwicklung einer ganzheitlichen Bildung zunehmend mehr vernetzte Unterrichtsstrukturen[4] gefordert werden und tiefer greifende Betrachtungen zu *FairIT* ohnehin nur multiperspektivisch erfolgen können, ist eine fachübergreifende Behandlung bei diesem Unterrichtsgegenstand

Erkennen	Bewerten	Handeln
Informationsbeschaffung und -verarbeitung	Perspektivenwechsel und Empathie	Solidarität und Mitverantwortung
Erkennen von Vielfalt	Kritische Reflexion und Stellungnahme	Verständigung und Konfliktlösung
Analyse des globalen Wandels	Beurteilung von Entwicklungsmaßnahmen	Handlungsfähigkeit im globalen Wandel
Unterscheidung gesellschaftlicher Handlungsebenen		Partizipation und Mitgestaltung

Tabelle: Zielkompetenzen für die Bildungsarbeit im Themenbereich FairIT [BMZ 2007, S. 82]

unumgänglich. Sie gelingt aufgrund der Komplexität und Flexibiltät von *FairIT* vorzugsweise in Projektform. Es bietet sich eine Zusammenarbeit der Fächer Informatik, Medienkunde, Ethik/Religion, Wirtschaft/Recht, Sozialkunde und Geografie im Rahmen von Projekttagen oder -wochen an. Auch für eine AG scheint das Thema sehr geeignet, idealerweise in Besetzung von zwei Fachlehrern oder eines Informatiklehrers mit gesellschaftswissenschaftlichem Kombinationsfach.

Da die Inhalte von *FairIT* vielschichtig miteinander verflochten sind, ermöglicht das Thema eine flexible Betrachtung. Eine Planungsgrundlage zum Aufbau einzelner Module und zur Ausbildung wünschenswerter Kernkompetenzen liefert der *Orientierungsrahmen für den Lernbereich Globale Entwicklung* der Kultusministerkonferenz (KMK) und des Bundesministeriums für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ). Der Orientierungsrahmen nennt Zielkompetenzen für den Themenbereich *Waren aus aller Welt: Produktion, Handel und Konsum*, wie in der Tabelle oben dargestellt.

Das Internet bietet reichlich Material für die Umsetzung von *FairIT* in der Schule, häufig beschränken sich die Angebote jedoch auf das Handy. Wünschenswert wären weitere Materialien, die auch die Produktion von PCs kritisch beleuchten.

Multiplikatoren und spätere Praktiker sensibilisieren – *FairIT* an der Hochschule diskutieren

In Informatik-Studiengängen für das Lehramt an Gymnasien bestehen günstige Rahmenbedingungen für die Themen aus *Informatik und Gesellschaft*, auch für das Thema *FairIT*. Lehramtsstudierende belegen stets zwei oder sogar drei schulische Fächer, die gleichrangig und mit annähernd vergleichbarem Aufwand studiert werden. Somit verfügen diese Studierenden neben fundierten Informatik-Kenntnissen auch über fachliche Kompetenzen aus mindestens einem anderen Fach und sind daher für interdisziplinäre Fragestellungen häufig aufgeschlossen sowie zu deren Bearbeitung hinreichend qualifiziert. Die Examensarbeit, mit der das Lehramtsstudium abgeschlossen wird und die in Umfang und Ernsthaftigkeit einer Diplom- oder Masterarbeit in nichts nachsteht, kann interdisziplinär aus einem Schnittfeld der studierten Fächer stammen. Auch eine Projektarbeit, häufig von den Studienordnungen vorgeschrieben, kommt hierfür in Frage, insbesondere um erste Erfahrungen mit einem Thema zu sammeln, das starke Bezüge zu mehreren Gebieten aufweist. Wir erleben, dass solche interdisziplinären Themen sowohl bei Lehramtsstudierenden als auch bei ihren Betreuern auf lebhaftes Interesse stoßen – vermutlich, weil sie spannender und häufiger auch anwendungsorientierter sind als klassische fachinterne Themen.

In Bezug auf alle anderen Informatik-Studiengänge hat sich die Situation durch die Bologna-Reform ebenfalls so weit verbessert, dass interdisziplinäre IT-Themen heutzutage kein Tabu mehr sind. Sie müssen nicht wie früher hinter unverdächtigen Veranstaltungstiteln versteckt werden. Insbesondere die *Euro-Inf Rahmenstandards und Akkreditierungskriterien für Informatikstudiengänge* erwarten von Bachelor-Absolventen explizit *„die Berücksichtigung der in der Berufspraxis der Informatik vorhandenen wirtschaftlichen, sozialen, ethischen und rechtlichen Bedingungen“* [EQANIE 2011, S. 4]. Damit ist der Weg frei, sich mit *FairIT* auch im Rahmen vollständig anerkannter und akzeptierter Lehrveranstaltungen zu beschäftigen. Wenn Lehrende dazu bereit waren, konnten sie sich seit 2005 auf ähnlich gelagerte Forderungen aus dem *Qualifikationsrahmen für Deutsche Hochschulabschlüsse* [KMK 2005] berufen, auch für Masterstudiengänge. Die 2005 verabschiedeten *Empfehlungen der Gesellschaft für Informatik e. V. (GI) für Bachelor- und Masterprogramme im Studienfach Informatik an Hochschulen* [GI 2005, S. 35f] sahen ebenfalls für grundlagenorientierte wie anwendungsorientierte Bachelor-Studiengänge explizit *Seminare zur Stärkung der Selbstkompetenz, z. B. aus dem Bereich Informatik und Gesellschaft* vor.

Ein Beispiel für die gezielte Umsetzung dieser gar nicht so neuen Möglichkeiten ist das Modul *Informatik und Gesellschaft*, das in verschiedenen Bachelor- oder Masterstudiengängen der Informatik an der Friedrich-Schiller-Universität Jena als Seminar im Bereich *Allgemeine Schlüsselqualifikationen* seit mehreren Jahren angeboten wird. Für das Sommersemester 2014 ist die spezielle Ausrichtung *GreenIT*, *FairIT* dieses Seminars geplant (beide Themen haben ja starke wechselseitige Bezüge). Erkenntnisse daraus sollen in einen Kurs der *Thüringer JuniorAkademie 2014* einfließen.

Perspektiven und Ausblick

Wie aktuell das Thema *Faires Handeln* in der Schule ist, beweist die Ausschreibung für den Schulwettbewerb des Bundespräsidenten zur Entwicklungspolitik 2013/2014 *Global und lokal denken und handeln* (http://www.eineweltfueralle.de/). Eine rege Teilnahme von Schülerinnen und Schülern an Wettbewerben, Aktivitäten und Projekten dieser Art in der Schule wäre aus drei Perspektiven wünschenswert: zum einen ist so eine persön-

liche Sensibilisierung für *FairIT* möglich, andererseits könnte der Grundgedanke von fairer Technik in die Schule als Institution getragen werden. Außerdem wären die zukünftigen Studierenden in der Lage, ihr Vorwissen zu *FairIT* an der Hochschule zu intensivieren und dortige Initiativen zu stärken, um sie gemeinsam mit ihren Dozenten forschend weiter zu entwickeln.

Anmerkungen

1 *Natürlich können und sollten FairIT-Unterrichtssequenzen auch in anderen Schulfächern durchgeführt werden – beispielsweise im Fach Medienkunde, Sozialkunde oder Ethik.*

2 *Die Grundsätze und Standards für die Informatik in der Schule wurden vom Arbeitskreis Bildungsstandards des Fachausschusses Informatische Bildung in Schulen und der Fachgruppe Didaktik der Informatik im Jahr 2008 verabschiedet. Seitdem stellen die verfassten Mindeststandards das Leitwerk für zeitgemäßen und kompetenzorientierten Unterricht in der Sekundarstufe I dar und bieten zusätzlich einen Aufgaben-Pool in Form einer Onlinedatenbank (http://www.informatikstandards.de).*

3 *Die Einheitlichen Prüfungsanforderungen in der Abiturprüfung (EPA) sind eine bundesweite Vereinbarung mit Festlegungen für die Gestaltung einer einheitlichen Abiturprüfung und der gymnasialen Oberstufe in den einzelnen Bundesländern. Sie wurden von der Kultusministerkonferenz der Länder im Jahr 2004 neu gefasst und bis zur Abiturprüfung 2007 umgesetzt. Die gemeinsamen Festlegungen beschreiben die grundlegenden Anforderungen an den Unterricht im mathematisch-naturwissenschaftlich-technischen Aufgabenfeld und somit an das Fach Informatik.*

4 *Diese Entwicklung spiegelt sich beispielsweise in der Einführung und Etablierung des Thüringer Schulfaches Mensch-Natur-Technik (MNT) wider.*

Referenzen

[BMZ 2007] Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung: Orientierungsrahmen für den Lernbereich Globale Entwicklung im Rahmen einer Bildung für nachhaltige Entwicklung. Ergebnis des gemeinsamen Projekts der Kultusministerkonferenz (KMK) und des Bundesministeriums für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ), Juni 2007. http://www.globaleslernen.de/sites/globaleslernen.de/files/files/link-elements/orientierungsrahmen_20f_c3_bcr_20globales_20lernen_1.pdf

[EQANIE 2011] European Quality Assurance Network for Informatics Education: Euro-Inf Rahmenstandards und Akkreditierungskriterien für Informatikstudiengänge. Deutsche Fassung vom 29.6.2011. http://www.eqanie.eu/media/Quality%20Label/Euro-Inf%20Framework%20Standards%20and%20Accreditation%20Criteria_German_V2011-06-29.pdf

[GI 2005] Gesellschaft für Informatik: Empfehlungen der Gesellschaft für Informatik e. V. (GI) für Bachelor- und Masterprogramme im Studienfach Informatik an Hochschulen. Bonn, 2005. http://www.gi.de/fileadmin/redaktion/empfehlungen/GI-Empfehlung_BaMa2005.pdf

[GI 2008] Gesellschaft für Informatik: Grundsätze und Standards für die Informatik in der Schule. Bildungsstandards Informatik für die Sekundarstufe I. Bonn, 2008. Beilage zu LOG IN 28 (2008) Heft 150/151. http://www.gi.de/fileadmin/redaktion/empfehlungen/Bildungsstandards_2008.pdf

[KMK 2004] Ständige Konferenz der Kultusminister der Länder in der Bundesrepublik Deutschland: Einheitliche Prüfungsanforderungen in der Abiturprüfung Informatik. Beschluss vom 1.12.1989 i.d.F. vom 5.2.2004. http://www.kmk.org/fileadmin/veroeffentlichungen_beschluesse/1989/1989_12_01-EPA-Informatik.pdf

[KMK 2005] Ständige Konferenz der Kultusminister der Länder in der Bundesrepublik Deutschland: Qualifikationsrahmen für Deutsche Hochschulabschlüsse. Beschluss vom 22.4.2005. http://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-03-Studium/02-03-02-Qualifikationsrahmen/2005_Qualifikationsrahmen_HSAbschluesse.pdf

[KIM 2012] Medienpädagogischer Forschungsverbund Südwest (mpfs), KIM-Studie 2012, 26.9.2013. http://www.mpfs.de/fileadmin/KIM-pdf12/KIM_2012.pdf

[JIM 2012] Medienpädagogischer Forschungsverbund Südwest (mpfs), JIM-Studie 2012, 26.9.2013. http://www.mpfs.de/fileadmin/JIM-pdf12/JIM2012_Endversion.pdf

[Kasten 2007] Entwicklungspsychologische Grundlagen: 0-3 Jahre, Berlin, Düsseldorf 2007.

[Kasten 2007] Entwicklungspsychologische Grundlagen: 4-6 Jahre, Berlin, Düsseldorf 2009.

CC BY

Stefanie Müller, Eberhard Zehendner

Stefanie Müller studierte an der Friedrich-Schiller-Universität Jena Informatik, Geschichte und Medienkunde und ist als Lehramtsanwärterin am Staatlichen Gymnasium „Dr. Konrad Duden“ in Schleiz/Thüringen tätig. Während ihres Informatikstudiums begann sie, sich kritisch mit Wechselwirkungen zwischen Informatik und Gesellschaft auseinanderzusetzen. Im Förderprogramm Demokratisch Handeln in Jena betreute sie besonders gern Jugendliche innerhalb der deutschlandweit stattfindenden Lernstatt Demokratie und entdeckte ihre Vorliebe für die projektbezogene Arbeit mit Schülerinnen und Schülern. Sie ist seit 2011 Mitglied im FIfF.

Eberhard Zehendner ist Professor für Technische Informatik an der Friedrich-Schiller-Universität Jena. Er führt seit langem Seminare aus dem Bereich Informatik und Gesellschaft durch, die auch gerne von Gasthörern besucht werden, und betreut entsprechende Studien- und Abschlussarbeiten. Zu seinen Anliegen gehören ferner die Sicherheit von IT-Systemen und die Sensibilisierung von Benutzern für das Systemverhalten der Rechnerarithmetik. Im Fachbereich Bildung, Wissenschaft und Forschung der Gewerkschaft ver.di arbeitet er zu hochschulpolitischen und tariflichen Themen mit. Dem FIfF gehört er seit 1985 an.

Klaus Willke

Gesetzliche Regulierungen in Sachen Elektroschrott

Wo stehen wir in Europa und Afrika?

Zum Thema Elektronik-Schrott (E-Schrott) gab es in den letzten Monaten ab und zu einen Bericht in den Druckmedien, meistens in Verbindung mit unzulässigen Praktiken bei der Entsorgung dieses Abfallstroms in westafrikanischen Ländern. Kinderarbeit, fehlender Arbeitsschutz oder ökologische Desaster waren die Vorwürfe. Die globale Dimension dieser Entsorgung wird selten weiter als bis Westafrika betrachtet und die Schwierigkeiten bei den Exportkontrollen nur am Rande erwähnt. Die Unterscheidung zwischen Nicht-Abfall und Gebrauchtgeräten gegenüber Abfall ist eine ständige Herausforderung, zumal die zuständigen Behörden dieses gegen einen potenziellen Exporteur zu belegen haben.

So wie die Produktion von Elektronikgeräten global organisiert ist, so hat auch die Entsorgung globale Dimensionen, deren gesetzliche Rahmenbedingungen auf den verschiedenen Ebenen hier auf Europa und Afrika bezogen vorgestellt werden sollen. Zur Definition: E-Schrott sind Elektro- und Elektronikgeräte sowie deren Bauteile, die nicht mehr verwendet werden, da sie entweder ihre vorgesehene Aufgabe nicht mehr erfüllen oder durch bessere Geräte ersetzt worden sind. Im deutschen Gesetz werden sie als Altgeräte geführt.

Dass exportierter E-Schrott soziale und ökologische Probleme in Ländern des globalen Südens verursacht, war schon kurz nach der Jahrtausendwende bekannt. Das *Basel Action Network (BAN)* veröffentlichte schon 2002 eine Studie wie auch einen Film zur Situation in Guiyu im Süden der Volksrepublik China[1]. Dass sich in Westafrika etwas Ähnliches anbahnen würde, ahnten nur ein paar interessierte Insider. Im Oktober 2005 veröffentliche BAN schließlich eine Studie zur E-Schrott Situation in Lagos/Nigeria.[2]

Fast ein Jahr später, vor sieben Jahren, als Medien weltweit über einen Giftmüllskandal in der Elfenbeinküste berichteten, wurde die E-Schrott-Problematik teilweise erwähnt, verwoben oder unerklärt nebeneinandergestellt.[3]

Was war geschehen? Mehr als ein Dutzend Menschen starben in Abidjan, nachdem sie in Kontakt mit importierten Abfall oder Produktionsresten kamen, die Tags zuvor von dem Frachter *Probo Koala* gelöscht worden waren. Die giftigen Produktionsreste stammten von einer Art schwimmenden Raffinerie, zu der das Schiff genutzt worden war. Beim *Probo-Koala*-Desaster wurden durch eine billige und illegale Beseitigung von mehr als 500t Giftmüll auf Kosten des Lebens unbeteiligter Menschen in der Elfenbeinküste[4] ein Extraprofit für die international tätige Rohstoffhandelsfirma *Trafigura* aus Europa erwirtschaftet.

Eine weitere Dimension war ein möglicher Konflikt zwischen zwei völkerrechtlichen Vereinbarungen. War neben dem *Basler Übereinkommen über die Kontrolle der grenzüberschreitenden Verbringung gefährlicher Abfälle und ihrer Entsorgung* (BÜ[5]) möglicherweise auch das internationale *Übereinkommen zur Verhütung der Meeresverschmutzung durch Schiffe* (MARPOL[6]) verletzt worden? Das letztere regelt – wie der Titel schon sagt – die Verhütung der Meeresverschmutzung durch Schiffe, das erste regelt die Kontrolle der grenzüberschreitenden Transporte von gefährlichen Abfällen, wozu auch E-Schrott zählt, wenn er gefährliche Substanzen enthält, was meistens der Fall

Elektroschrottberg in Guiyu, China
Quelle: CC-BY Rainer Rehak

ist. Danach ist der Export von E-Schrott in Nicht-OECD- Staaten untersagt, aber auch jeder andere Transport von gefährlichem Abfall dorthin ist verboten.

Reaktionen in Afrika

Auf der folgenden Vertragskonferenz des Basler Übereinkommens Ende November 2006 in Nairobi war nicht nur der *Probo-Koala*-Skandal[7] ein Thema, auch E-Schrott als spezieller globaler Abfallstrom wurde zum führenden Programm des *Baseler Übereinkommens*. 2008 begann – neben anderen Projekten und Arbeitsgruppen, die zum Teil schon früher starteten – das *E-waste Africa Project*. In ihm hat das Sekretariat der Basler Konvention (SBC) verschiedene Institutionen mit ihren Erfahrungen und Spezialwissen zusammengebracht.

Neben verschiedenen Länderstudien gibt es nun für Ghana und Nigeria jeweils eine sozial-ökonomische Studie zu den Auswirkungen des E-Schrotts in diesen beiden westafrikanischen Staaten. Größenschätzungen vom importierten wie auch selbst erzeugten E-Schrott liegen nun vor. Ebenso gibt es eine Beschreibung der formalen und informalen Marktstrukturen dieses Sektors. Diese Berichte, wie auch Dokumente aus den anderen Aktivitäten zu diesem Projekt sind auf der speziellen Webseite[8] des *BÜ* hinterlegt. Einen Überblick gibt die dort erhältliche Broschüre *Where are WEEE9 in Africa?*

Die grenzüberschreitende Abfallverbringung ist durch die aktuelle EU-Verordnung (EG) 1013/2006 reguliert. Sie hatte zwei

Vorläufer: Richtlinie (EWG) 84/631 und Verordnung (EWG) 259/93. Mit der ersteren reagierte die damalige Europäische Wirtschaftsgemeinschaft auf das Verschwinden von hochgiftigen Abfallfässern aus dem *Seveso*-Desaster in Frankreich, nachdem sie aus Italien dorthin transportiert worden waren. Die zweite, Anfang der neunziger Jahre beschlossene Verordnung setzte das bestehende Basler Übereinkommen sowie den OECD-Beschluss über die Verbringung von Abfällen zur Verwertung in EU-Recht um. Als Verordnung gilt sie unmittelbar. In Deutschland ist sie durch das Abfallverbringungsgesetz national umgesetzt worden. Darin wird die Verpflichtung von Kontrollen und der Umsetzung der Regelungen auf die jeweils zuständigen Behörden übertragen, die – bis auf Zolldienststellen und das Bundesamt für Güterverkehr – Länderbehörden sind. Gemäß der Verordnung und damit auch dem Abfallverbringungsgesetz ist der Export von gefährlichen Abfällen in Nicht-OECD-Staaten auch hier verboten.

Wie sieht es in Europa aus?

Um die Umweltbelastungen der wachsenden E-Schrott-Menge zu minimieren veröffentlichte die EU-Kommission 1998 einen ersten Entwurf für Elektro- und Elektronik-Altgeräte. Im Januar 2003 trat dann die WEEE-Richtlinie 2002/96/EG in Kraft. Zusammen mit der Richtlinie zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten[10] wurden die Mitgliedsstaaten darin verpflichtet, diese bis August 2004 in ihre nationalen Gesetze umzusetzen. In Deutschland trat im August 2005 das Elektro- und Elektronikgerätegesetz in Kraft. Damit werden das Inverkehrbringen, die Rücknahme sowie die umweltgerechte Entsorgung von diesen Geräten geregelt.

Beide Richtlinien wurden 2011 neu geschrieben und traten 2012 in Kraft. Für unser Thema sind die neuen *Mindestanforderungen an die Verbringung* von Interesse, weil dort eine Beweislastumkehr eingeführt wurde. Danach muss demnächst der Exporteur auf Nachfrage der Kontrollbehörden die Funktionsfähigkeit seiner zur Ausfuhr bestimmten gebrauchten Geräte glaubhaft nachweisen. Diese ist unter anderem durch eine Dokumentation der Funktionsprüfung nachzuweisen. Ob es schon eine rechtsverbindliche Abgrenzung von Gebrauchtgeräten und Abfall werden wird, wird sich in der Praxis zeigen. Inwieweit die Minimalkriterien dieses Nachweises europaweit in 2014 in den jeweils nationalen Gesetzgebungen vereinheitlicht und praxisnah geregelt sein werden, ist ebenfalls eine offene Frage. Die einheitliche Durchsetzung ist dann noch eine völlig andere Sache.

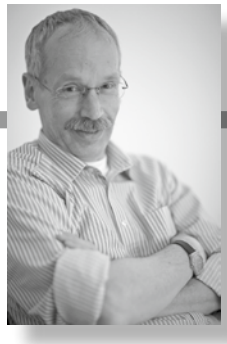
Wie man erkennen kann, sind wir in Europa schon recht weit, was den gesetzlichen Rahmen betrifft. In der Umsetzung ist eine Tendenz zu erkennen, dass von Seiten der EU-Kommission versucht wird, durch verstärkte Regularien die Durchsetzung europaweit zu vereinheitlichen und den zuständigen Behörden auch neue Instrumente zur Verfügung zu stellen, wie z. B. eine Beweislastumkehr und Inspektionspläne.

In Afrika ist man dabei, sich auf seine eigene Verantwortung zu besinnen, und entwickelt die politischen und rechtlichen Rahmenbedingungen weiter. Bei der Durchsetzung vor Ort hängt es noch stärker als in Europa davon ab, inwieweit das wenig vorhandene geschulte Personal auf den verschiedenen Ebenen kooperiert und sich vernetzt, um trotz der ungenügenden gesetzlichen Rahmenbedingungen doch etwas zu erreichen.

Daher ist es sinnvoll, die Entwicklungen zu beobachten und sich dazu auszutauschen, auch in konkreten Verdachtsfällen, damit weitere Wege der zweiten Wertschöpfungskette (Wertschöpfungskette nach der ersten Nutzung) besser aufgespürt werden können und in Fällen von illegaler Verbringung auch zeitnah grenz- und kontinentüberschreitend gehandelt werden kann. Nicht nur wegen der gemeinsamen, zum Teil unrühmlichen (Kolonial-)Geschichte, sondern auch bei den gegenwärtigen asymmetrischen Handelsbeziehungen scheint es sinnvoll zu sein, eine faire Partnerschaft anzustreben. Sich darüber zu verständigen, sie entsprechend zu pflegen sowie regelmäßig zu überprüfen, sollte eine gute Basis dafür sein, die negativen Auswirkungen dieser globalen Abfallentsorgung etwas einzudämmen.

Anmerkungen

1 *Exporting Harm: http://www.ban.org/library-page/order-films/exporting-harm-the-high-tech-trashing-of-asia/*
2 *The Digital Dump: http://ban.org/BANreports/10-24-05/index.htm*
3 *http://www.spiegel.de/spiegel/print/d-48902727.html*
4 *http://en.wikipedia.org/wiki/2006_Ivory_Coast_toxic_waste_dump (Stand: 23. Aug. 2013)*
5 *http://de.wikipedia.org/wiki/Basler_%C3%9Cbereinkommen*
6 *http://de.wikipedia.org/wiki/Internationales_%C3%9Cbereinkommen_zur_Verh%C3%BCtung_der_Meeresverschmutzung_durch_Schiffe*
7 *http://www.basel.int/TheConvention/ConferenceoftheParties/ReportsandDecisions/tabid/3303/Default.aspx (Stand: 27. Aug. 2013)*
8 *http://www.basel.int/Implementation/TechnicalAssistance/EWaste/EwasteAfricaProject/tabid/2546/Default.aspx*
9 *Im Englischen: Waste from Electrical and Electronic Equipment (WEEE) aktuell: 2012/19/EU*
10 *Restriction of Hazardous Substances (RoHS), damals 2002/95/EG; aktuell: 2011/65/EU*



Klaus Willke

Klaus Willke lebt in Hamburg und ist seit Ende 2011 in der passiven Phase der Altersteilzeit. Davor hat er knapp 19 Jahre bei der dortigen Umweltbehörde im Bereich der Abfallwirtschaft gearbeitet, die letzten sieben Jahre im Sachgebiet der grenzüberschreitenden Abfallverbringung. Bevor er nach Hamburg kam, lebte er zusammen fast acht Jahre lang in Zimbabwe und Ghana.

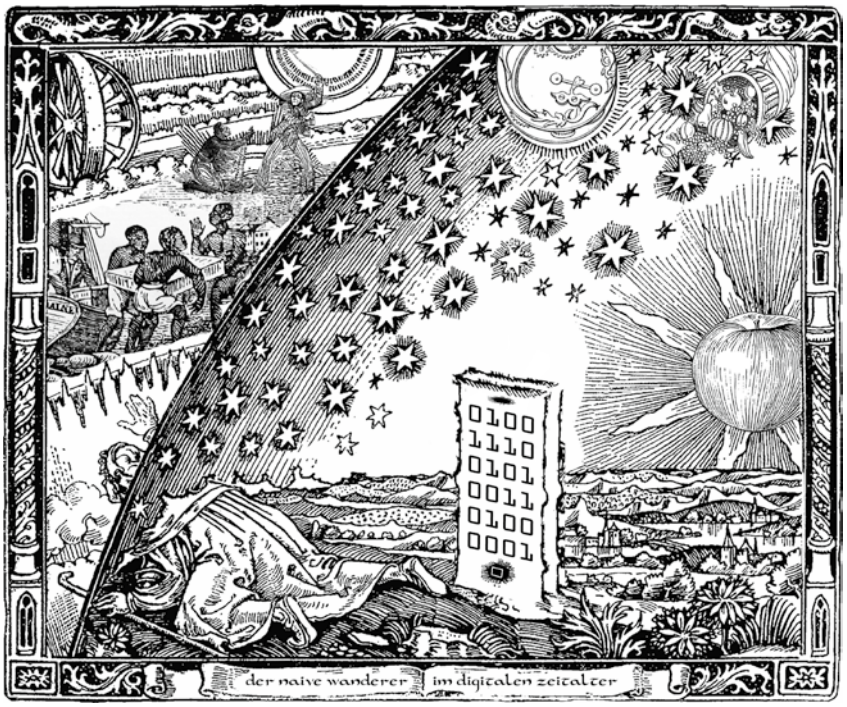
Stefan Ullrich

Und nun?

Der Wanderer am Weltenrand, so berichtet Camille Flammarion 1888, war ein naiver Mensch des Mittelalters, der eine Stelle entdeckte, wo Himmel und Erde sich zwar berührten, aber nicht gut verschweißt waren. So war er in der Lage, einen Blick hinter den Horizont zu werfen.[1] Der bekannte Holzstich zu der Geschichte dient bis heute als Illustration der kopernikanischen Wende und anderer Zäsuren der Wissenschaftsgeschichte. Das Motiv ist uns durch moderne dystopische Literatur ebenfalls bekannt: Die Protagonistin stolpert durch Zufall hinter die Bühne der Welt und wird auf die dort verborgenen Mechanismen aufmerksam, die nicht unbedingt zum Vorteil aller Menschen ihre Geschicke bestimmen.

Aufmerksamkeit ist eine knappe und begehrte Ressource, die zudem sehr unfair verteilt ist. Der moderne Mensch verschwendet keinen Gedanken daran, dass er sauberes Trinkwasser aus dem Wasserhahn bekommt oder jederzeit Strom hinter den zahlreichen Steckdosen vermuten darf. Im Digitalen treten physikalische Objekte sogar zur Gänze in den Hintergrund: Alle lesen den Online-Artikel, aber niemand sieht den Bildschirm.

Rücken wir für einen Augenblick die unsichtbaren Träger digitaler Medien und deren Entstehung in den Vordergrund – und nun? Reicht der Blick in die Werkhallen, die so offensichtlich die unfairen Arbeitsbedingungen zeigen, um eine Handlungsänderung zu bewirken? Wieso schaffen wir es, erst einen Artikel über ausgenutzte Arbeiterinnen von Elektronikfirmen zu lesen, nur, um danach per Twitter erfreut mitzuteilen, dass man sich soeben ein neues Smartphone gekauft habe?

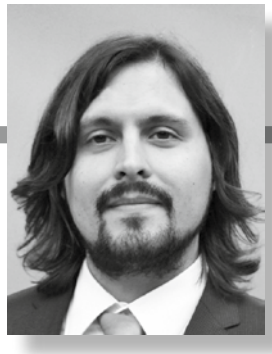


La recherche du Paradis digital
http://www.turing-galaxis.de/fiff/Flammarion2.0.jpg
Bild-Rechte: Collage von sak. cc-by

Beim Versuch, diese Frage zu beantworten, stößt man schnell auf ein Ohnmachtsgefühl, auf die Meinung, es sei eben so, und man könne sowieso nichts ändern. Der Computerpionier und Gesellschaftskritiker *Joseph Weizenbaum* hat sich über diese Haltung furchtbar aufgeregt. Er rief uns ins Gedächtnis, dass es Menschen sind, die die technische Welt gestalten.[2] Die Informatikerinnen haben in dieser von der Digitaltechnik geprägten Welt eine besondere Verantwortung! Wer, wenn nicht sie, sind dazu aufgefordert, den Diskurs in die Öffentlichkeit zu tragen?

Die Forderung nach fairen Computern, also Geräten, die unter sozial gerechten Bedingungen hergestellt wurden, hören wir jeden Sonntag von Politikerinnen und Herstellerinnen, die dann montags auf die komplizierte Welt- und Marktsituation hinweisen. Dann hat die interessierte, aber (am Computer!) arbeitende Bürgerin keine Zeit mehr, sich zu empören oder, schlimmer noch: sie hält die Empörung für sinnlos.

Zugegeben, die Größenordnungen können einschüchtern. Der *xkcd*-Zeichner Randall Munroe rechnet anhand des Energieverbrauchs aus, dass etwa der PR-Gigant *Google* momentan zwischen 1,8 und 2,4 Millionen Server betreibt, die zusammen über 300 Megawatt verbrauchen.[3] Das Thema Energieverschwendung ist unter dem Schlagwort *Green IT* sehr präsent, was beispielsweise die Selbstverpflichtung von Google zeigt, „saubere Energie“ einzukaufen.[4] Das Thema *Fair IT* wird hingegen nicht so prominent behandelt.



Stefan Ullrich

Stefan Ullrich ist seit 2011 Sprecher der Fachgruppe *Informatik und Ethik* der *Gesellschaft für Informatik* und einer der Autorinnen der Kolumne *Gewissensbits* der Fachzeitschrift *Informatik Spektrum*. *http://gewissensbits.gi.de/*

Und nun? Informatikerinnen denken bei kleinen und großen Problemen zumeist an technische Lösungen; in diesem Fall kann es keine solche geben. Es ist eine bestimmte Haltung zur Welt gefragt, das Problem können wir nur moralisch (und in der Folge dann politisch) angehen. Technik lässt sich für wunderbare Dinge einsetzen, wie das Beispiel der computergestützten Schulbildung in Uruguay zeigt.[5] Der Verzicht auf den Einsatz von Technik würde auch humanitäre Projekte bremsen; es geht also um einen bewussten Umgang mit der Technik.

Ein Ansatz ist das Hinterfragen der scheinbar gottgegebenen, pardon: jobsgegebenen Obsoleszenz. Der gesunde Menschenverstand lacht über die eingeredete Notwendigkeit, alle sechs Monate ein neues Smartphone kaufen zu müssen – der innere Schweinehund hingegen giert auf das goldene Gadget. Es ist klein, elegant, portabel, man führt es stets mit sich herum; und vermisst es, wenn es an der Bushaltestelle nicht da ist oder die Chefin im Vortragsraum zehn Minuten auf sich warten lässt. Diese Kompaktheit ist ein Grund, warum beispielsweise Tantal-Kondensatoren anstelle von Elektrolytkondensatoren verwendet werden. Die Bedingungen in den zur Tantal-Produktion notwendigen Coltan-Minen sind der Leserin bekannt.[6]

Das Thema *Fair IT* gehört aufs Tapet. In zahlreichen Behörden und anderen öffentlichen Einrichtungen (wie Universitäten) lassen sich ohne großen Aufwand die Anforderungen an die zu beschaffende technische Ausstattung entsprechend ergänzen. Im Freundeskreis kann über das Thema gesprochen werden, es ist mit vertretbarem Aufwand möglich, eine entsprechende ePetition beim Bundestag oder andere politische Aktionen zu organisieren.

Informatikerinnen in Universitäten können entsprechende Seminare oder Vorlesungen anbieten, Programmiererinnen können ihre Software mit einer entsprechenden Klausel versehen, dass sie nur auf *Fairen Computern* eingesetzt werden darf, Technikerinnen können Anleitungen zum Bau eines eigenen fairen Gadgets veröffentlichen – es gibt unzählige Möglichkeiten, wenn wir nur den Mut haben, unsere Aufmerksamkeit bei diesem Thema zu lassen und die Schweißnaht weiter aufzureißen.

Anmerkungen

1 http://gallica.bnf.fr/ark:/12148/bpt6k408619m.image.f167
2 Beispielsweise im Dokumentarfilm von Jens Schanze: Plug & Pray, Deutschland, 2009, 1:17:15.
3 Randall Munroe, What if? – Google's Datacenters on Punch Cards, 17.9.2013, URL: http://what-if.xkcd.com/63/
4 Google Inc., Using green power – A closer look, URL: http://www.google.com/green/energy/use/#purchasing
5 Plan Ceibal ist ein ministeriell gefördertes Projekt, das allen Grundschulkindern im Land einen eigenen Computer kostenlos zur Verfügung stellt. URL: http://www.ceibal.edu.uy/Paginas/Quienes-Somos.aspx
6 Siehe auch den Beitrag von Sebastian Jekutsch in diesem Heft.

CC BY

Dietrich Meyer-Ebrecht

„Töten per Fernbedienung"

Das Buch zur Kampagne gegen Drohnen

„Ewig summt der Tod", titelt die Frankfurter Rundschau in einem Dossier über den US-amerikanischen Drohneneinsatz in Waziristan – ein Szenario wie aus einer Science-Fiction-Dystopie. Weit weg, unvorstellbar, aber real. Und die logische Konsequenz einer Rüstungsentwicklung, die sich auf die 1996 vom US-Generalstab herausgegebene *Joint Vision 2010* gründet – ein Strategiepapier, das der Informationstechnik eine Schlüsselstellung zuweist. Die *Joint Vision 2010* begründete die neue Doktrin der Rüstungsplanung und Strategiekonzepte in den USA wie auch später in der NATO und in Deutschland. Ein wesentliches Element ist die ‚vernetzte Operationsführung': Informationsaustausch, Kontrolle und Steuerung zu jeder Zeit und an allen Orten, von Militärs und Politikern als *‚revolution in military affairs'* apostrophiert. Von Beginn an waren Drohnen zur Aufklärung und zum Kampfeinsatz ein entscheidender Baustein der Doktrin. Nun sind Drohnen mehr als spezielle Fluggeräte. Sie verfügen über hochkomplexe Informationstechnik für Flugkontrolle, Navigation, Beobachtung und Zielfindung, und sie stützten sich in ihrem Einsatz auf die global verfügbare Kommunikationsinfrastruktur des *cyber space*. Weltweiter Drohneneinsatz und Beherrschung des *cyber space* – eine synergetische Ergänzung! Unter dem Republikaner George W. Bush begonnen, wurde gerade unter dem Demokraten und Friedensnobelpreisträger Barack Obama der Ausbau dieser beiden Rüstungssegmente enorm forciert: *cyber warefare, drones, and special forces – Obama's way to war* ...

Peter Strutynski (Hg.)(2013):
Töten per Fernbedienung – Kampfdrohnen im weltweiten Schattenkrieg,
Wien, Promedia
ISBN 978-3-85371-366-2;
14,90 €

Bemerkenswert lange hat es gedauert, bis die Öffentlichkeit von der Brisanz dieser Entwicklung Kenntnis nahm. Bereits seit 2001 fliegen US-amerikanische und britische Drohnen in Afghanistan Gefechtseinsätze. Seit 2004 erscheinen regelmäßig Medienberichte über völkerrechtswidrige tödliche Drohneneinsätze, vor allem in Pakistan. Schon im Kosovo-Krieg 1998/99 wurden Aufklärungsdrohnen auch von der Bundeswehr eingesetzt. Vor gut einem Jahr endlich hat sich auch bei uns der Protest formiert, als Graswurzelbewegung, inzwischen gut organisiert mit einer sehr aktiven Beteiligung zahlreicher Friedensorganisationen und

-initiativen. Nun findet die Bewegung mit dem Erscheinen des Sammelbandes *Töten per Fernbedienung – Kampfdrohnen im weltweiten Schattenkrieg*, herausgegeben durch den Politikwissenschaftler und Friedensforscher *Peter Strutynski* aus Kassel, eine wertvolle Unterstützung. Denn drei Dinge braucht ein Erfolg versprechender Protest: Engagement, Organisation und seriöse Sachkenntnis. Der gut 200 Seiten starke Band liefert in zwölf Aufsätzen namhafter AutorInnen eine Fülle von Daten, Fakten und Hintergründen – ein sachlich und verständlich geschriebenes Kompendium, das erschauern lässt.

Zahlreich sind die sehr ernsten Argumente gegen Drohnenausrüstung und -einsatz, die der Herausgeber in seiner Einführung zusammenfasst. Das bedrohlichste, die Senkung der Hemmschwelle zu kriegerischen Auseinandersetzungen. Zur Regel geworden sind die *target killings*, Operationen unterhalb der öffentlichen Aufmerksamkeitsschwelle und abseits der völkerrechtlichen Normen, der ‚heimliche Krieg'. Während Politiker in Europa wie in den USA regelmäßig die Formel „ethisch untadelig, legal und notwendig" bemühen, zeigt die Praxis des Einsatzes – durchgeführt unter höchster Geheimhaltung, ohne Mandat, auf den Territorien souveräner Staaten, abseits erklärter Kriege – ein mittlerweile selbstverständlich gewordenes Unterlaufen des Völkerrechts, so *Norman Paech* in seinem Beitrag. Angesichts des Potenzials dieser Waffe würden internationale Verträge kaum Wirkung haben, nur eine Ächtung wird ihre Gefahren begrenzen können. Und es eilt: „*Das internationale Recht basiert auf der Vorstellung, dass eine Aktion, die heute verboten ist, dennoch zulässig ist, wenn sie nur von genügend Ländern praktiziert wird*", zitiert *Elsa Rassbach* einen ranghohen israelischen Militär. Selbst sehr aktiv in der deutschen Anti-Drohnen-Kampagne, gibt sie mit ihrem Beitrag einen umfassenden Situationsbericht über Protestbewegungen, Protestaktionen und die politische Reaktion in Europa, auch über die vergeblichen Bemühungen um Aufhebung der Geheimhaltung.

Die strikte Geheimhaltung, argumentiert *Chris Cole* in einem Beitrag, der sich speziell der Rolle Großbritanniens widmet, macht eine Überprüfung der immer wieder behaupteten Schonung der Zivilbevölkerung unmöglich. Konterkariert wird eine seriöse Evaluation bereits durch die Definition der Zielgenauigkeit: Die *circular error probability (CEP)* erfasst die 50 % der zielnächsten Einschlagpunkte. Die Nebensächlichkeit von 50 % Fehltreffern macht deutlich, dass nicht die Vermeidung ziviler Opfer das Primat ist, sondern die Tötung der zum Ziel auserkorenen Personen, der „Hochwertziele". Mit der gerne behaupteten ‚Sauberkeit' des Einsatzes, der Minimierung von Kollateralschäden, räumt auch *Knut Mellenthin* in seinem faktenreichen Bericht über den Einsatz bewaffneter Drohnen von Afghanistan bis Somalia auf. Darin prangert er an, dass, wenn schon die Praxis der *targeted killings* sich jeder rechtsstaatlichen Norm entzöge, erst recht die Möglichkeiten und der Wille zur eindeutigen Zielbestimmung – Kombattant oder Zivilperson? – in Frage zu stellen seien. Die perfide Praxis des *double tap*, ein kurzzeitig nachfolgender Angriff, dem die Helfer zum Opfer fallen, ist hierauf nur noch das ‚Sahnehäubchen'.

Kaum öffentlich diskutiert rüstet auch die Bundeswehr auf. Kampfdrohnen sind zentraler Bestandteil der „Neuausrichtung der Bundeswehr", schreibt *Lühr Henken* in seiner Analyse der Beschaffungspolitik der Bundeswehr. Mit Stolz stellt die Bundeswehr die Leistungsfähigkeit ihrer Waffensysteme heraus, insbesondere jener aus deutscher Rüstungsentwicklung und -produktion. Die qualitative Umrüstung soll die weltweite Angriffsfähigkeit (!) steigern. Zu sichern seien Handelswege und Ressourcenzugang. Kampfdrohnen erscheinen in diesem Licht als ideales Mittel, um in Auslandseinsätze einzusteigen. Gegen die Ausrüstung mit Drohnen zu protestieren, so schließt Henken, ist zwingend für den Protest gegen Auslandseinsätze. Den Einblick in die bundesdeutsche Verquickung politischer Ziele und wirtschaftlicher Interessen ergänzt *Frank Sölkner* mit seinem Situationsbericht aus Österreich. Die Beschaffung von Drohnen wird mit einem undifferenzierten Mix aus ihrer militärischen, polizeilichen und zivilen Nützlichkeit begründet. Eine agile Industrie unterläuft Exportrestriktionen. So exportiert die Firma Schiebel ihren *Camcopter* als Aufklärungsdrohne, derweil sie vom britisch-französischen Rüstungskonzern Thales erfolgreich mit Leichtraketen ausgerüstet getestet wird. Und wer wusste, dass die Motoren des *Predators* aus dem oberösterreichischen Gunskirchen kommen?

Wie auf der einen Seite die Angriffsfähigkeit mit Wirtschaftsinteressen begründet wird, so ist die Industrie auf der anderen Seite treibende Kraft für die politische Durchsetzung von Rüstungsbeschaffungen. Das gilt in besonderem Maße für ein so komplexes und kostspieliges Waffensystem wie die Drohne. Das macht *Tom Barry* in seinem Beitrag zur politischen Ökonomie von Drohnen an den Geldflüssen deutlich, mit denen die US-amerikanische Rüstungsindustrie Politiker ‚kauft' und die Proliferation des Drohnenprogramms in den USA damit einer wirksamen parlamentarischen Kontrolle entzieht. Genauso, wie auch Forschungs- und Wirtschaftsförderung in diesem Bereich kaum gesellschaftlicher Kontrolle unterliegt. Hier ist es der vielfältige zivile und behördliche Nutzen der Drohnen, der vorgegeben wird. Tatsächlich sind Drohnen im Grenzschutz- und Polizeieinsatz, für zivile Überwachungs- und Aufklärungsaufgaben bereits etabliert. Über die zahlreichen gegenwärtigen Einsatzbereiche in Deutschland berichten *Matthias Monroy* und *Andrej Hunko*, und auch, wie die Europäische Union Drohnentechnologie unter dem Label Sicherheit fördert.

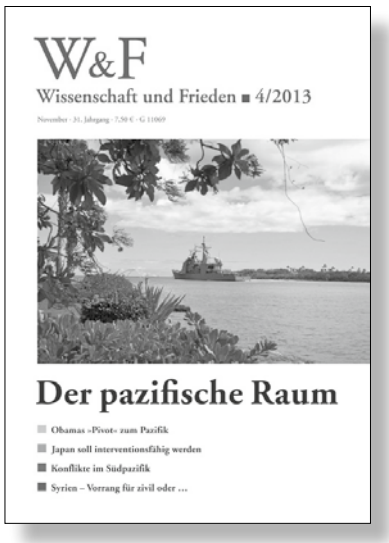
Wie ist es zu erklären, dass diese höchst problematische Entwicklung mit einer derartigen Zielstrebigkeit vorangetrieben wird? Fliegende Roboter sind ein Faszinosum. Die Öffentlichkeit ist geblendet von den neuen technischen Errungenschaften, und die Militärs sind begeistert über die Optionen ferngesteuerter oder gar ‚automatisierter' Kriege. *Nick Turse* gibt das Szenario eines Gefechts zwischen autonomen unbemannten Luft- und Seefahrzeugen wieder, die vernetzt in Teams operieren, vorprogrammiert lediglich auf die Anforderungen und Eingrenzung ihrer Mission. Mit diesem kürzlich veröffentlichten Szenario treibt das US-Verteidigungsministerium, nahtlos anknüpfend an die oben zitierten *Joint Vision*, die weitere Aufrüstung des Drohnen-Arsenals propagandistisch voran. Und diese findet statt, ungeachtet aller – wenig publizierten! – Schwachstellen und Rückschläge. Die Faszination schlägt allerdings jäh zu einer Horrorvorstellung um, wenn unbemannte Kampffahrzeuge zu autonomen Tötungsmaschinen werden. Todbringende Roboter. Und als solche soll man sie auch benennen, so *Hans-Arthur Mariske* in seinem Essay, anstatt mit neutralen Begriffen wie *unmanned aerial vehicle* auf die technische Domäne abzulenken. Sie bleiben Roboter. Der Terminus, geprägt vor einem knappen Jahr-

hundert, steht für die Fiktion des künstlichen Menschen, und in dieser Fiktion schwingt auch die dystopische Vision einer Machtergreifung der Roboter mit. Naiv wäre es, so Mariske, diese Option völlig von der Hand zu weisen. Der „Terminator", der vor drei Jahrzehnten noch ein Science-Fiction-Konstrukt war, wird mit der Entwicklung bewaffneter Roboter-Fahrzeuge unaufhaltsam Realität.

50 Staaten entwickeln oder beschaffen bereits Roboter-Plattformen als Waffenträger, so recherchierte *Noel Sharkey*, seit vielen Jahren ein profilierter Warner vor einer fortschreitenden Automatisierung des Krieges. Zwischen Mensch-gesteuert und vollautonom operierend spannt sich ein Kontinuum. Abzusehen ist, dass sich die Rolle des Menschen in der Entscheidungsschleife fortschreitend verringern wird. Vernebelt wird diese Entwicklung durch begriffliche Konfusion, die Verantwortlichkeit wird im Dunkeln gelassen. Sharkey ruft auf, aus der Drohnenproblematik zu lernen: Dass bereits die Fernsteuerung einer Tötung die Moral ausschaltet. Dass der schon dort erreichte Grad an Autonomie den Weg zu den ‚geheimen Kriegen' gebahnt hat. Dass die neuen ‚Freiheiten' dieser Waffengattung den Kriegsschauplatz ausweiten. Und dass die Illusion ihrer Treffsicherheit nicht aufrecht zu erhalten ist. Ein Einhalt dieser Entwicklung ist dringend geboten. Wie müsste eine Rüstungskontrolle für Drohnen, oder weiter gefasst für ‚unbemannte bewaffnete Fahrzeuge', gestaltet sein, fragt *Jürgen Altmann*. Ein generelles Verbot hält er derzeit für nicht durchsetzbar. Zwar sind bereits bestehende Verträge wie START auch auf unbemannte Systeme anwendbar, jedoch lassen sie viele Schlupflöcher, insbesondere, wenn sie bestimmte Waffentypen nicht verbieten, sondern nur begrenzen. In einem umfangreichen Katalog stellt Altmann Optionen zusammen, wie bestehende Verträge und Abkommen modifiziert und ergänzt werden müssten, auch wie Verifikationsmechanismen entsprechend zu erweitern seien. Angesichts der fortschreitenden Entwicklung autonomer System jedoch plädieren Altmann wie Sharkey für die grundsätzliche Pflicht, den Menschen in der Entscheidungsschleife zu belassen, und aus ethischen Gründen eine Tötungsentscheidung nie einer Maschine zu überlassen. Über alle Erwägungen zu begrenzten und begrenzenden Verboten stellen sie deshalb eine generelle Ächtung autonomer bewaffneter Fahrzeuge, wie sie das *International Committee for Robot Arms Control, ICRAC*, gegründet von Altmann, Sharkey et al., bereits 2010 forderte.

Die ICRAC-Forderung ist auch ein Appell an die Wissenschaft. Denn Robotik ist ein attraktives Forschungsfeld, insbesondere die Methodik und Technologie für autonome Fahrzeuge. Forschungsgelder fließen reichlich an Universitäten, und Wettbewerbe werden ausgeschrieben. Die Materie bringt es mit sich, dass eine militärische Verwertbarkeit der Ergebnisse – *dual use* – oder sogar eine genuin militärische Zielsetzung leicht zu verdecken sind und auch bequem ignoriert werden können. In seinem Beitrag über diese Verflechtungen appelliert *Ralf E. Streibl* an die Verantwortung der Lehre und Forschung mit einem Leitzitat von Altmann, „dass Krieg und Frieden zwar im Kern politische Fragen seien, dass jedoch neue Waffentechnologien […] massiven Einfluss auf gesellschaftliche Prozesse und Entwicklungen haben und den Frieden gefährden". Drohnen gehören bestimmt dazu. Und die Informationstechnik in noch viel umfassenderen Maße.

Wissenschaft & Frieden 4-2013 – Der pazifische Raum



Pazifik verbinden viele von uns vermutlich mit blauem Meer, langen Sandstränden, mildem Klima und üppiger Vegetation. Dabei sind die politischen Entwicklungen in dieser Region hoch spannend. Mit dem „Pivot to Asia-Pacific" der Obama-Regierung formulieren die USA deutlich ihre hegemonialen Interessen vor Ort. Sie stoßen dabei allerdings auf Konkurrenz und widerstreitende Interessen einer Reihe anderer Länder. Einige Aspekte davon beleuchten die Artikel im Schwerpunkt der November-Ausgabe von *Wissenschaft & Frieden*:

Joseph Gerson: Obamas Pivot – die Neuausrichtung der USA auf Asien und den Pazifik, *Christine Ahn*: Kollateralschaden des Koreakrieges – 60 Jahre ohne Friedensvertrag, *Eiichi Kido*: Japan soll interventionsfähig werden, *Herbert Wulf*: Indien / China – Konflikt, Kooperation und Konkurrenz, *Roland Seib*: Umbrüche und Konflikte im Südpazifik, *Daniel Lambach*: Australien zwischen Asien und Europa, *Tanja Rother*: Crown-Maori Beziehungen in Neuseeland.

Weitere AutorInnen befassen sich mit dem Krieg in Syrien, der Protestbewegung in Uganda und den Menschenrechten beim Softwareexport.

Wissenschaft & Frieden, Nr. 4-2013 **Der pazifische Raum**,
€ 7,50 plus Porto.

W&F erscheint vierteljährlich, dreimal im Jahr liegt W&F ein 12 bis 20seitiges Dossier bei. Jahresabo 30 €, ermäßigt 20 €, Ausland 35 €, ermäßigt 25 €. 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. Fördermitglieder von Wissenschaft und Frieden (mindestens 60 € jährlich) erhalten auf Wunsch die gedruckte und die digitale Ausgabe. Bezug: W&F, Beringstr. 14, 53115 Bonn, Email: *buero-bonn@wissenschaft-und-frieden.de, www.wissenschaft-und-frieden.de*

FIfF e.V.

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

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

FIfF-Büro

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

Die aktuellen Bürozeiten entnehmen Sie bitte unseren Webseiten.

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

FIfF im Netz

Das ganze FIfF:
www.fiff.de

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

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

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

FIfF-Beirat

Michael Ahlmann (Bremen); **Peter Bittner** (Bad Homburg); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Wolfgang Coy** (Berlin); Prof. Dr. **Wolfgang Däubler** (Bremen); Prof. Dr. **Leonie Dreschler-Fischer** (Hamburg); Prof. Dr. **Christiane Floyd** (Hamburg); Prof. Dr. **Klaus Fuchs-Kittowski** (Berlin); Prof. Dr. **Michael Grütz** (Konstanz); Prof. Dr. **Thomas Herrmann** (Dortmund); Prof. Dr. **Wolfgang Hesse** (Marburg); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (Konstanz); **Ulrich Klotz** (Frankfurt); Prof. Dr. **Klaus Köhler** (München); Prof. Dr. **Herbert Kubicek** (Bremen); Dr. **Constanze Kurz** (Berlin); Prof. Dr**. Klaus-Peter Löhr** (Berlin); **Werner Mühlmann** (Oppung); Prof. Dr. **Frieder Nake** (Bremen); Prof. Dr. **Rolf Oberliesen** (Bremen); Prof. Dr. **Arno Rolf** (Hamburg); Prof. Dr. **Alexander Rossnagel** (Kassel); Prof. Dr. **Gerhard Sagerer** (Bielefeld); Prof. Dr. **Gabriele Schade** (Erfurt); Prof. Dr. **Dirk Siefkes** (Berlin); **Ralf E. Streibl** (Bremen); Prof. Dr. **Marie-Theres Tinnefeld** (München); Dr. **Gerhard Wohland** (Waldorfhäslach)

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Prof. Dr. **Dietrich Meyer-Ebrecht** (stellv. Vorsitzender) – Aachen
Sylvia Johnigk – München
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Rainer Rehak – Berlin
Jens Rinne – Mannheim
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Ingrid Schlagheck – Bremen
Prof. Dr. **Werner Winzerling** – Fulda
Prof. Dr. **Eberhard Zehendner** – Jena

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen
Sara Stadler – Bremen

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 100 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	Sebastian Jekutsch
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	Oh Wunder Kommunikationsdesign
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*)

30C3 – Chaos Communication Congress 2013
27. bis 30. Dezember in Hamburg

Arbeitskreis RUIN – Rüstung und Informatik
9. Februar 2014 in Berlin

FIfF-Klausurtagung 2014
21. bis 23. März 2014 in Bad Hersfeld

FIfF-Vorstandsitzung
8. Februar 2014 in Berlin, ab 10:00 Uhr

FIfF-Kommunikation
1/2014 »Jahrestagung 2013: Cyberpeace«
Sylvia Johnigk, Kai Nothdurft, Stefan Hügel
Redaktionsschluss 1.2.2014

2/2014 »Datenausspähung und Videoüberwachung«
Stefan Hügel, Peter Bittner
Redaktionsschluss 1.5.2014

3/2014 »Gender«
Britta Schinzel, Sara Stadler
Redaktionsschluss 1.8.2014

W&F – Wissenschaft & Frieden
2/13 – Kriegslügen
3/13 – Jugend und Konflikt
4/13 – Der pazifische Raum
1/14 – Innergesellschaftliche Konflikte
2/14 – Neuer Kolonialismus
3/14 – Krieg und Frieden und die Künste

DANA – Datenschutz-Nachrichten
1/13 – Löschen
2/13 – Datenschutz mit Hindernissen
3/13 – Kommunaler Datenschutz

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.

Sebastian Jekutsch

Dead Mountain Edition

„Dead Tree Edition" wird bedrucktes Papier ironisch genannt, dessen Inhalt auch elektronisch verfügbar ist: Wikipedia-Bücher, Faltblätter mit Konferenz-Timetables oder gedruckte PDFs. Man ignoriert dabei, dass für die Online-Infrastruktur und all die Computer zum Lesen der eBooks nicht nur Bäume, sondern gleich ganze Berge (auf denen auch mal Bäume gestanden haben) abgetragen werden müssen, um an die Mineralien für die Metalle in den Geräten und Kabeln zu kommen.

Ok Tedi Mine (Gold- und Kupfer) in Papua-Neuguinea
Foto: Ok Tedi Mine CMCA Review

Bauxitmine (Aluminium) auf Jamaika
Foto: Paul Morris

Bingham Canyon Mine (Kupfer) in Utah, USA
Foto: Spmusick

Roşia Poieni (Kupfer) in Rumänien
Foto: Cristian Bortes

Grube in Bangka (Zinn) in Indonesien
Foto: Päivi Pöyhönen, FinnWatch/makeITfair

Homestake Mine (Gold) in South Dakota, USA
Foto: Rachel Harris