H 7625

FIfF-Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

30. Jahrgang 2013 Einzelpreis: 7 EUR

1/2013 – März 2013

Digitalisierte Gesellschaft – Wege und Irrwege

ISSN 0938-3476

• 29C3 Not my Department! • Datenschutz • FIfF-Studienpreis •

FIfF-Kommunikation

Titelbild: iStockphoto

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Inhalt

Ausgabe 1/2013

inhaltt

Editorial

Drei Ereignisse und Entwicklungen stehen im Mittelpunkt dieser Ausgabe: Die FIfF-Jahrestagung 2012, der 29. Chaos Communication Congress und die Debatten zum Datenschutzrecht – national zum Beschäftigtendatenschutz und auf europäischer Ebene zur EU-Datenschutz-Grundverordnung.

Die FIfF-Jahrestagung fand mit dem Titel *Digitalisierte Gesellschaft – Wege und Irrwege* im November 2012 in Fulda statt. Ihr Thema war der in allen Bereichen der Gesellschaft zunehmende Rechnereinsatz: das Internet ist nicht nur für Industrie, Handel und Behörden, sondern auch für den Privatbereich zu einem zentralen Teil der Infrastruktur geworden. Der Einfluss der Digitalisierung auf unser tägliches Leben wächst überall – von der Kindheit über Ausbildung und Berufsleben bis hin zur Freizeit. Neben den Hauptvorträgen und Arbeitsgruppen, die wir in diesem Heft dokumentieren, gab es auch die Verleihung des FIfF-Studienpreises – dessen Preisträger stellen Ihre Arbeiten vor.

Zwischen Guckkasten und Rummelplatz ist der Titel des ersten Beitrags aus dem Schwerpunkt von *Manfred Nagl*. Er untersucht darin *Konstanten und Wandel in der Welt der Kindermedien* und gibt einen geschichtlichen Abriss vom Mittelalter bis heute. Er stellt darin auch dar, welche Bedrohungen für die Entwicklung von Kindern im Lauf der Zeit gesehen wurden – von der Lese- bis hin zur Internetsucht – und welche nicht – so waren Kinder früher Gewaltdarstellungen ausgesetzt, die heute selbst für Erwachsene unvorstellbar sind.

Von *Neuen LebensWeltKrisen* im Social Web berichtet *Anja Lorenz: „Die derzeitigen Möglichkeiten, die vor allem das Social Web mit sich bringt, eröffnen es nahezu jedem, sich an der Verbreitung von Informationen – passiv wie aktiv – zu beteiligen. Diese Partizipationsmöglichkeiten bringen fraglos positive Effekte, aber auch negative Phänomene zum Vorschein"*, erläutert sie einleitend.

Über *Kampfdrohnen als Mittel der High-Tech-Kriegsführung* schreibt *Jutta Weber* in ihrem Beitrag und fragt, ob der Einsatz dieser Systeme zu *Automatisierter Verantwortungslosigkeit* führt. Als Quintessenz fordert sie ein Moratorium aller Kampfdrohnen und einen Bann autonomer Waffensysteme.

Im letzten Beitrag aus der Reihe der Hauptvorträge in diesem Heft fragt *Rainer Kuhlen*: *Was hat „Eigentum" und „Wissenschaftsfreiheit" mit dem Urheberrecht zu tun* und stellt fest: *Mit Reförmchen ist es nicht länger getan. „Eigentum und Wissenschaftsfreiheit sind zweifellos unaufgebbare Grundrechte. Zweifelhaft aber, ob sie über das Urheberrecht verteidigt werden müssen."*

In den Arbeitsgruppen wurden die Themen der Tagung diskutiert und vertieft. In diesem Heft finden sich Berichte zu *Fairen Computern*, *Weltbildern in der Informatik*, *Ethik und Verantwortung* und *Cyberwar und Cyberpeace*. Vier Preisträger konnten wir im Rahmen der Tagung mit dem FIfF-Studienpreis 2012 auszeichnen. *Rainer Rehak*, *Göde Both*, *Stefanie Müller* und *Angel Tchorbadjiiski* stellen ihre preisgekrönten Arbeiten vor.

Der aktuelle Teil dieses Hefts enthält einen „kleinen" Schwerpunkt zum 29. Chaos Communication Congress – dem *29C3*. Der 29C3 stand dieses Jahr unter dem Motto *Not my department!* und wandte sich damit gegen den Versuch, Verantwortung für das eigene (informatische) Handeln auf andere abzuwälzen. Er fand nach langer Zeit wieder in Hamburg statt; das FIfF war neben einem Informationsstand mit drei Vorträgen beteiligt: Einen Bericht vom gesamten 29C3 hat *Kai Nothdurft* zusammengestellt, in dem er auch vom Vortrag zu *Cyberpeace* von *Sylvia Johnigk* berichtet. *Britta Schinzel* beantwortet in ihrem Beitrag die Frage *Was ist, was kann, was soll Gender Studies Informatik?* und *Sebastian Jekutsch* setzt sich mit der Frage *Sind faire Computer möglich?* auseinander.

Breiten Raum nimmt der Datenschutz im aktuellen Teil ein. In Brüssel tobt gerade die Lobby-Schlacht um die geplante *EU-Datenschutz-Grundverordnung*. Das FIfF hat dazu eine Stellungnahme erarbeitet, deren Kurzfassung wir hier dokumentieren. Eine Reihe von Bürgerrechtsvereinigungen und rund 500 Einzelpersonen wenden sich mit der *Brussels Declaration* gegen die zu befüchtende Aushöhlung der Verordnung und damit gegen den Angriff starker wirtschaftlicher Interessen auf unsere Persönlichkeitsrechte: *„We are outraged!"*. Auch diesen Aufruf dokumentieren wir im Heft.

Gleichzeitig gab es eine Initiative der Bundesregierung, einen zwei Jahre alten Gesetzentwurf zum *Beschäftigtendatenschutz* auf die Schnelle durch das Parlament zu peitschen. Eine Kampagne von Datenschützern, die fast 70.000 Unterstützer fand, war vorläufig erfolgreich: die Beratungen wurden kurzfristig verschoben. Was genau passiert ist, und worum es beim Beschäftigtendatenschutz – der auch künftig nicht durch europäisches Recht abgedeckt wird – geht, hat *Werner Hülsmann* zusammengestellt.

Monika Ermert berichtet von der *World Conference on International Telecommunication (WCIT)* im Dezember in Dubai und damit über die Zukunft der weltweiten Telekommunikation. Mit *Positionsinformationen*, und was sie für unsere Privatsphäre bedeuten, setzt sich *Björn Schembera* in seinem Beitrag auseinander.

Last but not least darf ich eine neue Rubrik in der FIfF-Kommunikation ankündigen: Ab jetzt wird *Sebastian Jekutsch* regelmäßig über Neuigkeiten im Bereich sozialverträglicher IT-Produktion berichten – *Betrifft: Faire Computer*.

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

Gesetze und Wurst

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

"There are two things in the world you never want to let people see how you make ´em: laws and sausages", stellt *Leo McGarry,* der fiktive Stabschef im Weißen Haus, in einer Folge der ersten Staffel der amerikanischen Fernsehserie *West Wing* fest. Momentan müsste ich die Aufzählung wohl noch um Lasagne ergänzen, aber darum soll es hier nicht gehen. Vor kurzem konnten wir im Deutschen Bundestag die Verabschiedung des Meldegesetzes verfolgen, das, wäre es nicht im Bundesrat gestoppt worden, womöglich als „57-Sekunden-Gesetz" in die legislative Geschichte eingegangen wäre, nachdem es offenbar in der letzten Sitzung des Innenausschusses noch entscheidend verändert worden war. Es gibt immer wieder Diskussionen über Gesetze, die wortwörtlich aus den Vorlagen von Lobby-Vereinigungen übernommen werden – heftige Diskussionen dazu gab es beispielsweise während Finanzkrise und Bankenrettung. Und auch jetzt scheint in Brüssel wieder eine Lobby-Schlacht zu toben – um die EU-Datenschutz-Grundverordnung, nachdem die Änderungsvorschläge des Berichterstatters im Europäischen Parlament, Jan Philipp Albrecht, gerade diskutiert werden. So etwas habe er „noch nie erlebt", erklärte er dazu gegenüber der *Süddeutschen Zeitung*. Dass einzelne Unternehmen um ihr Geschäftsmodell fürchten, das gerade auf der Verletzung der Persönlichkeitsrechte ihrer Nutzer aufbaut, ist ja auch nachvollziehbar.

Vielleicht schafft eine neue Initiative hier Abhilfe: *LobbyPlag*, ein Portal, das gesetzgeberische „Plagiate" bei der Entwicklung der EU-Datenschutz-Grundverordnung aufdecken soll, d.h. Fälle, in denen Gesetzentwürfe direkt aus Papieren der Lobbyisten übernommen werden. Es ist zu wünschen, dass das Bewusstsein für solche Fälle gestärkt und dadurch langfristig die Macht finanzstarker Lobby-Vereinigungen zurückgedrängt wird.

Um nicht missverstanden zu werden: Lobbying ist nicht generell abzulehnen. Auch für Datenschutz und Bürgerrechte treten Lobby-Vereinigungen ein: zum Beispiel EDRi – European Digital Rights – wo das FIfF seit Jahren Mitglied ist. Auch wir selbst sind im Brüsseler Transparenzregister für Lobby-Vereinigungen eingetragen. Doch wenn Organisationen, die weitgehend auf ehrenamtlicher Basis arbeiten, gegen Vereinigungen antreten, die von großen Konzernen finanziert werden, ergibt sich ein Ungleichgewicht, das schädlich ist: schädlich für die Demokratie, schädlich für die europäische Einigung. Größtmögliche Transparenz in diese Abläufe zu bringen, ist der erste Schritt in die richtige Richtung. Leider sind die Fortschritte der europäischen Institutionen selbst noch ausbaufähig – die Teilnahme am genannten Transparenzregister ist zum Beispiel nicht obligatorisch.

Es wäre die vordringliche Aufgabe der Medien, mehr Transparenz in die Politik zu bringen. Ein Genuss ist es beispielsweise, die Interviews eines Günter Gaus aus den sechziger Jahren mit Spitzenpolitikern – unter anderem Konrad Adenauer, Franz Josef Strauß, Willy Brandt, Rudi Dutschke – wieder zu sehen. Diese inhaltliche Tiefe der Gespräche ist heute im Fernsehen kaum mehr vorstellbar – außer vielleicht in Randzeiten, in denen kaum jemand zusieht. Fundierte Berichterstattung wird leider häufig durch die hastige Behandlung von Trivialitäten ersetzt, meist zugespitzt auf Personalien. Leider gilt um so mehr der Satz, den Neil Postman bereits 1992 in seinem Buch *Wir amüsieren uns zu Tode* geschrieben hat: *„Problematisch am Fernsehen ist nicht, dass es uns unterhaltsame Themen präsentiert, problematisch ist, dass es jedes Thema als Unterhaltung präsentiert."* Über Wahlen wird heute eher im Stil von Sportereignissen berichtet. Geht es aber dabei wirklich in erster Linie darum, dass ihr Ausgang *spannend* ist?

Letzter Höhepunkt ist wohl die Diskussion, ob der Entertainer Stefan Raab das *TV-Duell* zwischen Bundeskanzlerin Merkel und Herausforderer Steinbrück moderieren soll. Ein besseres Indiz, dass fundierte politische Debatten – und damit letztlich die Wählerinnen und Wähler – von den Verantwortlichen kaum noch ernst genommen werden, kann es fast nicht geben.

Der Datenschutz ist derzeit ein bedeutendes Thema in der Arbeit des FIfF: Sowohl die bereits genannte EU-Datenschutz-Grundverordnung, zu der wir eine umfangreiche Stellungnahme verfasst und den zuständigen Abgeordneten des Europäischen Parlaments zugeleitet haben, als auch der Beschäftigten-Datenschutz – ein wichtiger Bereich des Datenschutzes, der durch die Verordnung bewusst nicht abgedeckt wird. Zu letzterem gibt es eine Vorlage von 2010, die vor einigen Wochen anscheinend handstreichartig durchgesetzt werden sollte. Schmackhaft machen wollte man der Öffentlichkeit den Entwurf mit dem Verbot verdeckter Überwachung am Arbeitsplatz – der fehlende Hinweis auf die erhebliche Erweiterung offener Überwachung war sicherlich der allgemeinen Hektik des Gesetzgebungsverfahrens geschuldet. Der sofort einsetzende massive Protest von Datenschützern konnte (vorerst?) Schlimmeres verhindern.

Nach der sehr interessanten und gut besuchten Jahrestagung des FIfF im November in Fulda können wir in diesem Jahr auch unsere Teilnahme am 29C3 – dem Chaos Communication Congress – in Hamburg als großen Erfolg verbuchen. Neben einem Informationsstand, der auf breites Interesse stieß, war das FIfF mit drei Vorträgen – zu Cyberpeace, Gender und Fair IT – beteiligt, die auch in den überregionalen Medien Beachtung fanden. Herzlichen Dank an alle, die daran mitgewirkt haben!

Mit FIfFigen Grüßen

Stefan Hügel

Das FIfF verleiht 2013 wieder den

FIfF-Studienpreis

für herausragende Abschlussarbeiten aus dem Bereich Informatik und Gesellschaft.

Wir wollen damit Studierende sowie Wissenschaftlerinnen und Wissenschaftler in der Qualifikationsphase zur fundierten und differenzierten Auseinandersetzung mit den gesellschaftlichen Auswirkungen der Informatik ermutigen.

Das FIfF möchte mit der Einrichtung dieses Studienpreises herausragende Leistungen des wissenschaftlichen Nachwuchses in diesem Bereich würdigen und die Aufmerksamkeit der Öffentlichkeit auf das Thema der Arbeit sowie die besonderen Leistungen der Autorinnen und Autoren lenken.

Wir laden dazu ein, geeignete Arbeiten bis 31. Mai 2013 einzureichen.

Das Preisgeld beträgt:

1. Preis: 333 €
2. Preis: 222 €
3. Preis: 111 €

Es können Qualifikationsarbeiten (Bachelor-, Master-, Diplomarbeiten oder Dissertationen) eingereicht werden, die in den letzten zwei Jahren vor Nominierungsschluss abgeschlossen wurden. Die Ausschreibung bezieht sich zwar schwerpunktartig auf Abschlussarbeiten in Informatik, jedoch wird auch zur Einreichung thematisch einschlägiger Arbeiten anderer Fachgebiete ausdrücklich eingeladen.

FIfF-Geschäftsstelle
– Studienpreis 2013
Goetheplatz 4, 28203 Bremen
oder per E-Mail an *studienpreis@fiff.de*.
Weitere Details unter *http://www.fiff.de/studienpreis.*

Der Preis wird in einer Feierstunde im Rahmen der FIfF-Jahrestagung am 26. Oktober 2013 in Siegen verliehen.

bitte vormerken – bitte vormerken – bitte vormerken – bitte vormerken – bitte vormerken

FIfF-Jahrestagung 2013

Cyberpeace

25. bis 27. Oktober 2013 in Siegen

Ort: Universität Siegen, Artur-Woll-Haus, Am Eichenhang 50, 57076 Siegen

Weitere Informationen in Vorbereitung

bitte vormerken – bitte vormerken – bitte vormerken – bitte vormerken – bitte vormerken

Stellungnahme des FIfF

zur Besetzung des Lehrstuhls *Informatik und Gesellschaft und Didaktik der Informatik* an der Humboldt-Universität zu Berlin

Die Berliner Senatorin für Bildung, Jugend, Wissenschaft und Forschung – Frau Senatorin Sandra Scheeres – wird in Kürze über die Berufungsliste zur Besetzung des Lehrstuhls „Informatik und Gesellschaft und Didaktik der Informatik" zu entscheiden haben. Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF) hat Hinweise erhalten, dass die durch das altersbedingte Ausscheiden von Prof. Dr. Wolfgang Coy freigewordene Professur für Informatik und Gesellschaft fachfremd beziehungsweise nur mit marginalem Fachbezug wiederbesetzt werden soll. Sollten diese Hinweise den Tatsachen entsprechen, so ist das FIfF über die drohende Fehlbesetzung besorgt und möchte die Senatorin, den Präsidenten der Humboldt-Universität, den Dekan der Mathematisch-Naturwissenschaftlichen Fakultät II und die interessierte Öffentlichkeit vor dem damit verbundenen weiteren Abbau des Faches Informatik und Gesellschaft warnen – besonders in einer Zeit, in der die Informatik unsere Gesellschaft immer stärker durchdringt.

Mit diesem Beitrag sollen die Fachinhalte des Gebietes *Informatik und Gesellschaft* noch einmal kurz verdeutlicht werden. Denn momentan besteht die große Gefahr, dass dieses Gebiet lediglich als Auseinandersetzung mit einer losen Sammlung von Themen wie Mensch-Maschine-Interaktion, Interface-Design und Datenschutz missverstanden wird. Doch darum geht es im Kern dieser Disziplin nicht.

Über die Ursprünge einer Disziplin: Verantwortung, Kritik und Aufklärung

Die Informatik war nie eine neutrale Natur- und Technikwissenschaft. Im Gegenteil: Militär und die Wirtschaft haben die Entstehung und Entwicklung dieser Disziplin entscheidend geprägt, im guten wie im schlechten Sinne. Die De-Chiffrierung der Enigma und die Hollerith-Maschinen von IBM mit ihrer Bedeutung für den Holocaust sind nur zwei von vielen gegensätzlichen Fallbeispielen dieser Geschichte. Davon Zeugnis zu geben, haben in den 1940er und 50er Jahren nur die wenigsten Mitwirkenden (z. B. Heinz von Foerster, Norbert Wiener, Heinz Zemanek) als ihre Aufgabe angesehen. In der Zeit nach den Weltkriegen und den ersten Atombombenabwürfen, die ebenfalls ohne Rechentechnik undenkbar gewesen wären, drängte sich die Frage nach der Verantwortung des Wissenschaftlers unumgänglich auf.

Die Informatik wuchs in den 1960/70er Jahren in einem geistigen Klima der Rationalisierung heran. Die irreführende Metapher vom Computer als Gehirn oder als künstliche Intelligenz hat dort ihren Ursprung. Das Leben selbst war in der Vorstellung mancher Technokraten ein berechenbares System; schlimmer noch: Mensch und Tier galten als informationsverarbeitende Systeme! Diese „Ohnmacht der Vernunft" und die Rücksichtslosigkeit gegenüber dem Leben schließlich waren es, welche die Wissenschafts- und Gesellschaftskritik zu einem festen Bestandteil der später entstehenden Teildisziplin *Informatik und Gesellschaft* machen sollte.

Ihre Institutionalisierung fand in vielen deutschen Städten in den 1980/90er Jahren statt und war der Ausdruck eines Erkenntnisinteresses, das nach den Wechselwirkungen von Technik und Gesellschaft fragte, und die Rolle der Informatik in der aufkommenden Informationsgesellschaft zu untersuchen begann. Das Nachdenken über die Technik, ihren Gehalt, ihre Herkunft, ihren Sinn und ihren gesellschaftlichen Kontext wurde zu einem Wesenszug der frühen Gemeinschaft von Wissenschaftlern der *Informatik und Gesellschaft,* von denen die meisten selbst Ingenieure, Mathematiker oder Naturwissenschaftler waren.

Und während die gesellschaftlichen Umwälzungsprozesse durch die Informationstechnik in den folgenden Jahrzehnten zunahmen, wurde ihre politische, rechtliche und kulturelle Bedeutung für die Öffentlichkeit immer sichtbarer: Welche Chancen haben wir, diese permanenten Umwälzungen nicht sich selbst oder gar wenigen mächtigen Menschen oder Organisationen zu überlassen? Wie lassen sich technische Abhängigkeiten in Selbstbestimmung und bewusstes Gestalten überführen? Und welche technischen Freiheitsgrade sind für die Gesellschaft förderlich und schützenswert? All diese Fragen haben damit zu tun, die Technik einordnen und beurteilen zu können – und zwar so, dass jeder betroffene Mensch dazu in der Lage ist. Diese Form der Mündigkeit zu ermöglichen ist die genuine Aufgabe der besagten Disziplin.

Die Lebendigkeit des Begriffs *Informatik und Gesellschaft* schöpft aus eben diesem geschichtlichen und geistigen Hintergrund. Er beinhaltet die Verbindung von Technik- und Geisteswissenschaften und hat sich in einem Kanon von Themengebieten niedergeschlagen: die Rolle der Informatik in der Informationsgesellschaft (und damit verbunden gesellschaftstheoretische Grundlagen aus den Bereichen Politik, Recht und Wirtschaft), Recht und Informatik (z. B. technischer und nichttechnischer Datenschutz), Geschichte der Informatik, Informatik als Wissenschaft, Ethik in Technik und Informatik, Digitale Medien, Digitale Langzeitarchivierung, Wissensordnung in der digitalen Welt und die Klärung informatischer Begriffe.

Paradoxerweise erlebt das Fachgebiet *Informatik und Gesellschaft* in den letzten Jahren einen Rückschlag nach dem anderen, obwohl ihre Fragestellungen nun endgültig von der Politik und der Gesellschaft, z. B. in der Netzpolitik, aufgegriffen worden sind. Ihre Lehrstühle werden von den Universitäten umgewidmet, fallengelassen oder sinnentleert.

Über Bildung

Die Bezeichnung des Lehr- und Forschungsgebietes *Informatik in Bildung und Gesellschaft* hebt noch einen weiteren Bereich hervor: Bildung. Bildung, im Humboldtschen Sinne als ganzheitliche Formung der autonomen und mündigen Persönlichkeit be-

griffen, bedeutet für die Informatik zweierlei: Sie kann erstens als Fachgebiet nicht losgekoppelt von den Geistes- und Sozialwissenschaften, den Künsten, den Sprachen, der Literatur und Geschichte gelehrt und gelernt werden. Die Schnittstellen zu all diesen Bereichen und auch die Hybridität der Informatik innerhalb der Mathematik, Natur- und Ingenieurwissenschaften werden nur allzu gern vergessen – mit langfristig fatalen Folgen. Zweitens wird vom Fachbereich *Informatik in Bildung und Gesellschaft* vor diesem Hintergrund ganz konkret die *Didaktik der Informatik* gelehrt. Das bedeutet auch, dass dort Lehrerinnen und Lehrer für allgemein- und berufsbildende Schulen ausgebildet werden.

Eine informatische Bildung und Didaktik integriert kritische Urteilsfähigkeit, Verantwortungs- und Geschichtsbewusstsein, Gerechtigkeitsempfinden, Kommunikationsfähigkeit und Kreativität als zentrale Bestandteile in die Vermittlung informatischer Konzepte und Methoden. Das moderne Paradigma kompetenz- und problemlösungsorientierter Didaktik, das auch in den aktuellen Berliner Rahmenlehrplänen (RLP) der Informatik verankert ist, ist anschlussfähig an diese breite Herangehensweise. Als zentrale Fachkompetenzen für Informatik in der Sekundarstufe II werden genannt: „Wechselwirkungen zwischen Informatiksystemen, Mensch und Gesellschaft beurteilen", „Informatiksysteme verstehen", „Kommunizieren und Kooperieren", „Problemlösen", „Informatisches Modellieren" und „Mit Informationen umgehen".

Die komplexen Herausforderungen des Bildungssystems lassen sich nicht durch Techniken wie intelligente Tutorensysteme (ITS) bewältigen, sondern bedürfen individueller menschlicher Zuwendung. Dem Computer die menschliche Fähigkeit des „Verstehens" einzuprogrammieren, bleibt nach mehr als vier Jahrzehnten der Forschung nicht nur eine abwegige Wunschvorstellung. Ein solch grobes Missverständnis von Informatikdidaktik muss bei der Besetzung des Lehrstuhls *Informatik und Gesellschaft und Didaktik der Informatik* vermieden werden.

Es wird sicher nicht einfach sein, den Platz von Prof. Dr. Wolfgang Coy, der ein Pionier und eine bedeutende Leitfigur von *Informatik und Gesellschaft* ist, gleichwertig auszufüllen, aber das FIfF sieht für die Nachfolge dennoch etliche geeignete Kandidatinnen und Kandidaten im In- und Ausland.

Das FIfF appelliert an die beteiligten und betroffenen Personen, sich dieses Berufungsverfahrens anzunehmen und eine Fehlbesetzung zu vermeiden. Die Zukunft des Fachgebiets *Informatik und Gesellschaft* an der Humboldt-Universität ist nicht nur für die Informatik insgesamt richtungsweisend, sondern tangiert auch das Ansehen der Universität.

Bremen, 22. Dezember 2012

Stellungnahme des FIfF

zur Datenschutz-Grundverordnung vom 25. Januar 2012 mit Änderungsvorschlägen des Berichterstatters vom 17. Dezember 2012

Der Entwurf für eine EU-Datenschutzgrundverordnung von der EU-Kommission stammt vom Januar letzten Jahres; eine erste Stellungnahme wurde bereits auf der FIfF-Mitgliederversammlung beschlossen (siehe FIfF-Kommunikation 4/2012). Darauf aufbauend hat eine fünfköpfige Arbeitsgruppe die Stellungnahme erweitert und auch die Änderungsvorschläge des Berichterstatters im EU-Parlament, Jan Philipp Albrecht, analysiert. Die Langfassung des vorliegenden Text wurde am 12. Februar 2013 vom FIfF-Vorstand beschlossen und an Mitglieder der Ausschüsse und des EU-Parlaments verschickt, die bis Ende Februar Änderungsvorschläge am Entwurf einreichen konnten. Neben dem FIfF haben einige andere Bürgerrechtsorganisationen Änderungsvorschläge gemacht (siehe dazu protectmydata.eu und privacycampaign.eu). Allerdings ist der Druck der wirtschaftsnahen Lobby-Organisationen sehr stark. Sie wollen wesentliche Punkte der Verordnung entschärfen und die Bürgerrechte schwächen.

Das FIfF befürwortet den vorgelegten Entwurf der EU-Kommission zur Modernisierung des Datenschutzes – eine solche Initiative war überfällig! Wir befürworten ebenfalls eine Reihe von Änderungsvorschlägen des Berichterstatters, insbesondere die Grundrechte-Schutzklausel: *„Die Mitgliedstaaten sind nach der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) verpflichtet, dafür Sorge zu tragen, dass solche Datenströme angemessen reguliert werden."*

Durch die Einführung europaweit einheitlicher Standards wird – trotz noch bestehendem Änderungsbedarf – endlich ein EU-weites Datenschutzniveau etabliert. Wir treten für eine weitere Verbesserung ein und fordern, dass die Verordnung nicht wegen wirtschaftlicher Interessen eingeschränkt wird.

1 Für eine weitere Präzisierung der Einwilligung

Das FIfF begrüßt ausdrücklich die Präzisierung der Einwilligung, insbesondere die explizite und eindeutige Einwilligung und das Recht auf Widerruf und Widerspruch.

Das FIfF fordert: Wie auch im Änderungsvorschlag des Berichterstatters vorgesehen, *dürfen Voreinstellungen, die die betroffene Person verändern muss, um der Verarbeitung zu widersprechen (opt-out), keine freie Zustimmung ausdrücken.* Da sich die technischen Bedingungen ständig ändern, fordern wir *eine Begrenzung der Gültigkeit einer Einwilligung auf maximal vier Jahre*. Beim Auslaufen ist die verarbeitende Stelle verpflichtet, die Daten unverzüglich zu löschen. *Die wirksame Einwilligung Minderjähriger erfordert die Zustimmung der gesetzlichen Vertreter des einsichtsfähigen Minderjährigen. Die Einwilligung muss immer gegenüber der verantwortlichen Stelle abgegeben werden.* Die Verordnung muss hier präzise Festlegungen treffen.

2 Für die Bevorzugung der Betroffenen gegenüber den Datenverarbeitern

Das FIfF begrüßt ausdrücklich die Ergänzungen zur Unterrichtungspflicht der betroffenen Person durch den für die Verarbeitung Verantwortlichen, wobei die Gründe für den Vorrang seiner Interessen offenzulegen sind.

Das FIfF fordert: *Die Fälle, in denen „berechtigtes Interesse" angenommen wird, sind auf drei einzuschränken:* Die *Ausübung von Grundrechten*, insbesondere des Rechts auf freie Meinungsäußerung und der Freiheit der Medien und der Künste, die *Durchsetzung von berechtigten Rechtsansprüchen* – insbesondere der Strafverfolgung – oder bei *gewerblichen Beziehungen zwischen Unternehmen,* wenn die Daten mit Kenntnis des Betroffenen für diesen Zweck erhoben wurden. *Nutzung zur Direktwerbung ist an die ausdrückliche Zustimmung der Betroffenen zu binden.* Der Änderungsvorschlag bietet noch zu viele Möglichkeiten für eine Datenverarbeitung ohne Zustimmung.

3 Für verbesserte Dokumentationspflichten

Das FIfF begrüßt ausdrücklich die Vorschläge des Berichterstatters zur Straffung der Dokumentationspflichten, die Zusammenführung mit den Informationsrechten der Betroffenen und die Pflicht zur Dokumentation technischer und organisatorischer Maßnahmen und Verfahren.

4 Für die Beschränkung von Profiling und Ausweitung der Informationspflicht

Die Definition von Profiling und die engere Fassung des Erlaubnisvorbehalts werden zu mehr Rechtssicherheit führen. Die erweiterten Auskunftspflichten stärken die informationelle Selbstbestimmung der Betroffenen.

Das FIfF fordert: *Logik und Algorithmus von Profiling-Maßnahmen sind offen zu legen. Besondere Kategorien* personenbezogener *Daten* dürfen nicht zur Auswertung verwendet werden, es sei denn, sie fallen unter die explizit genannten Ausnahmen. Durch Profiling entstandene Bewertungen sind nie vollständig und auch eine menschliche Beurteilung kann Vorurteile oder Fehlinterpretationen enthalten. Deshalb *müssen Betroffene eine zweite Meinung zur Bewertung einholen können*. Die Kosten hat der Verantwortliche für die Datenverarbeitung zu tragen.

Das FIfF fordert außerdem: *Ein generelles Verbot von Profiling-Maßnahmen, die zu Diskriminierung führen.* Das gilt auch für das *Zusammenwirken einzelner Profiling-Maßnahmen.*

5 Für die Orientierung an Schutzzielen und datenschutzfreundliche Voreinstellungen

Das FIfF begrüßt die Verpflichtung zu datenschutzfreundlicher Technikgestaltung bei Verarbeitung und Erhebung personenbezogener Daten. Die Betroffenen müssen ihre Verbreitung kontrollieren können.

Das FIfF fordert: *Die erweiterten Schutzziele sind in die Verordnung aufzunehmen:* Diese sind Transparenz, Zweckbindung und Intervenierbarkeit (neben den vom Berichterstatter bereits bekräftigten Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit). *Auch sie sind in technischen und organisatorischen Prozessen umzusetzen.*

Das FIfF fordert außerdem: *Hersteller sind zu Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen zu verpflichten*, etwa durch verpflichtende Zertifizierung. Diese ist durch eine EU-Institution zu kontrollieren und für alle Prozesse sicherzustellen (Systementwicklungsprozesse, Datenschutzprozesse und fachliche Geschäftsprozesse). Zertifizierungen sollten besonders dann verpflichtend sein, wenn besondere Kategorien personenbezogener Daten oder solche von Kindern verarbeitet werden oder wenn Profile erstellt werden.

6 Für angemessene Garantien beim Grenzübertritt mit mobilen Geräten

Das FIfF begrüßt ausdrücklich Ortsbindung (Orientierung am Unternehmensort der meisten Dienste-Nutzer), Zweckbindung, Transparenz und die Bindung an die europäische Gesetzgebung. Wir lehnen mit dem Berichterstatter die Anerkennung von Verarbeitungssektoren in Drittstaaten ab. Drittländer oder Gebiete ohne angemessenen Datenschutz müssen von der Übermittlung personenbezogener Daten ausgeschlossen werden können. Wir begrüßen die Forderung finanzieller Entschädigungsleistungen bei nicht genehmigter Verarbeitung von Daten in Drittstaaten. Das FIfF begrüßt die Rechenschafts- und Nachweispflicht.

Das FIfF fordert: *Mobile Dienste-Anbieter müssen einen Sitz in dem Land haben, in dem mehrheitlich die Vertragsnehmer ansässig sind.* Verlagert sich diese Mehrzahl der Vertragsnehmer während der Dauer von zwei Jahren in einen anderen Mitgliedstaat, ist der Sitz dorthin zu verlegen. *Die Speicherorte der personenbezogenen Daten sind transparent zu machen.* Wir fordern ein Widerspruchsrecht, wenn die personenbezogene Daten an Dienste-Anbieter außerhalb der EU übermittelt werden, die nicht der Verordnung unterliegen. Ein Recht auf Einsichtnahme in übermittelte personenbezogene Daten und ein Einspruchsrecht bei Zu- und Abschaltung von Wirknetzen international kooperierender Dienste-Anbieter ist vorzusehen. *Mobile Geräte müssen zum Schutz personenbezogener Daten auf Antrag unbrauchbar gemacht werden.*

7 Für eine grundsätzliche Verpflichtung zu anonymisieren oder zu pseudonymisieren

Das FIfF unterstützt, den Begriff der anonymen Daten zu spezifizieren, und den Geltungsbereich der Verordnung auf pseudonyme Daten und IP-Adressen auszuweiten.

Das FIfF fordert: *Die grundsätzliche Verpflichtung zur Anonymisierung oder Pseudonymisierung personenbezogener Daten* ist in angemessenem Rahmen vorzuschreiben. Wenn die Identität nicht relevant ist, muss anonymisiert werden, wenn sie relevant ist, pseudonymisiert. *Der Schutz pseudonymisierter Daten ist dem von personenbezogenen Daten gleichzustellen.* Anbieter dürfen die Funktionen bei anonymer Nutzung nicht

einschränken und nicht vorgeben, anonyme oder pseudonyme Nutzung sei nicht möglich.

8 Zur Ausnahme von Polizei und Justiz von der Verordnung

Das FIfF teilt die Kritik des Berichterstatters, dass die Zusammenarbeit bei der Strafverfolgung im Vorschlag der Kommission nicht geregelt wird.

Das FIfF fordert: *Angemessene Festlegungen für Fälle wie den Zugriff von Strafverfolgungsbehörden auf geschäftliche Daten sind in die Verordnung aufzunehmen* und dadurch einheitlich in Europa zu regeln.

9 Für eine verpflichtende Folgenabschätzung

Das FIfF begrüßt ausdrücklich die Forderung nach einer verpflichtenden Folgenabschätzung. Diese Verpflichtung sollte für alle Profiling-Maßnahmen gelten.

Das FIfF fordert: Je nach Art der Datenverarbeitung ist eine angemessene Abschätzung auch der längerfristigen Folgen (über die Dauer der Datenverarbeitung hinaus) für die Rechte und Freiheiten der Betroffenen verpflichtend vorzusehen. Die Folgenabschätzung sollte möglichst vollständig veröffentlicht und den Betroffenen vor der Einwilligung zur Verfügung gestellt werden, soweit sie nicht Auskunft über vertrauliche interne Vorgänge enthält.

10 Für eine Begrenzung der delegierten Rechtsakte

Das FIfF begrüßt ausdrücklich die Ersetzung des Berichterstatters von delegierten Rechtsakten der EU-Kommission durch Regelungen des Europäischen Datenschutzausschusses. Die ursprünglich vorgesehenen Befugnisse der Kommission würden zu einer großen Zahl an Detailregelungen führen, die der parlamentarischen Kontrolle entzogen sind. Diese Rechtsunsicherheit gefährdet die effektive Durchsetzung von Bürgerrechten und birgt wirtschaftliche Risiken. Sinnvoll sind delegierte Rechtsakte, wenn technischer Fortschritt häufige Anpassungen der Regelungen erfordert.

Das FIfF fordert: Um die parlamentarische Kontrolle sicherzustellen, *sind delegierte Rechtsakte und Entscheidungen des Europäischen Datenschutzausschusses innerhalb von sechs Monaten vom Parlament zu bestätigen.* Ein Aufweichen von Regelungen, Demokratiedefizit und Rechtsunsicherheit muss verhindert werden, dazu *ist ein enger Rahmen für die verbleibenden Befugnisse vorzugeben. Alle durch Rechtsakte vorgenommenen Konkretisierungen müssen den anerkannten, verbindlichen Schutzzielen folgen.* Alle Prozesse sind bei Entwicklung und Nutzung der IT-Systeme an diesen Schutzzielen auszurichten.

11 Für eine stärkere Unabhängigkeit der Aufsichtsbehörden und Datenschutzbeauftragten

Das FIfF begrüßt ausdrücklich die Sicherstellung der Unabhängigkeit der Aufsichtsbehörden, den Vorschlag, dass die bei der Angemessenheit die Bevölkerungszahl und der Umfang der zu verarbeitenden personenbezogenen Daten zu berücksichtigen ist, und die Klarstellung der Rechenschaftspflicht gegenüber den nationalen Parlamenten. Weitere Vorgaben sind zur Sicherstellung der Unabhängigkeit zu ergänzen.

Das FIfF fordert: *Die Befugnis zu Ernennung der Mitglieder der Aufsichtsbehörden sollte ausschließlich beim Parlament als den gewählten Vertreterinnen und Vertretern der Bevölkerung liegen. Genauere Vorgaben für die Finanzkontrolle* müssen die Unabhängigkeit sicherstellen; *die Aufsichtsbehörden müssen finanziell so ausgestattet werden, dass sie ihren Aufgaben effektiv nachkommen können.* Die Unabhängigkeit der betrieblichen Datenschutzbeauftragten sollte durch einen *mindestens einjährigen Kündigungsschutz* gestärkt werden.

12 Für die Verpflichtung eines Datenschutzbeauftragten auch in kleineren Unternehmen

Das FIfF begrüßt ausdrücklich, den Einsatz eines Datenschutzbeauftragten von der Anzahl der Betroffenen abhängig zu machen und die Profilerstellung sowie die Verarbeitung besonderer Kategorien von Daten explizit in den Katalog der Tätigkeiten aufzunehmen, die einen Datenschutzbeauftragten erfordern.

Das FIfF fordert: *Die Bestellung eines Datenschutzbeauftragten muss verpflichtend sein, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 10 Personen beschäftigt sind.* Die im Entwurf der Kommission vorgesehene Zahl von 250 Beschäftigten ist zu hoch, auch wenn die Situation von kleinen und mittleren Unternehmen berücksichtigt werden muss.

13 Gegen die Erhebung politischer Einstellungen durch Parteien

Nach Erwägungsgrund 44 dürfen politische Parteien im öffentlichen Interesse Daten über die politische Einstellung von Personen sammeln.

Das FIfF fordert: *Die Ausnahme ist zu streichen.* Ein Missbrauch dieser Daten kann niemals mit hinreichender Sicherheit ausgeschlossen werden. Die drohenden Eingriffe in die Persönlichkeitsrechte der Betroffenen sind nicht hinnehmbar.

14 Für die Regelung des Beschäftigten-Datenschutzes durch die Mitgliedstaaten

Das FIfF begrüßt ausdrücklich die Möglichkeit, spezielle Gesetze zu detaillierten Regelungen des Beschäftigungssektors zu erlassen oder beizubehalten.

Das FIfF fordert: *Die Einschränkung der EU-Kommission, dass dies nur in den Grenzen dieser Verordnung erfolgen darf, muss entfallen.* Wir unterstützen die Auffassung des Berichterstatters, dass der Beschäftigungssektor ein hochkomplexer Bereich ist, der auf einzelstaatlicher Ebene detailliert geregelt ist, und dort am besten geregelt werden kann.

Die Stellungnahme ist abzurufen unter: *http://fiff.de/stellungnahme-des-fiff-zur-datenschutz-grundverordnung*

Kai Nothdurft

Not my Department!

Bericht vom 29. Chaos Communication Congress (29C3) in Hamburg am 27.-30. Dezember 2012

Der Congress fand wie jedes Jahr zwischen den Feiertagen vom 27. bis 30. Dezember statt, diesmal seit vielen Jahren das erste Mal wieder in Hamburg. Das Berliner Congress Centrum (bcc) war bei den letzten Congressen stets aus allen Nähten geplatzt. Der Vorverkauf für die Karten war für manche schon zu einem Clickcontest geworden, und wer nicht schnell genug war, kam nicht mehr rein. Auch im Gebäude war es immer sehr beengt und bei vielen Vorträgen musste man schon Glück haben, um in die Veranstaltungsräume zu kommen.

Das Congress Centrum Hamburg (CCH) als neue Heimat erwies sich als gute Wahl, denn es gab reichlich Platz, obwohl mit 6.900 Tickets ein neuer Besucherrekord erzielt wurde.

Der 29C3 stand unter dem Motto: *Not my department!* (frei übersetzt: *Das ist doch nicht meine Baustelle.)* Der Titel geht auf eine Persiflage von Tom Lehrer über Werner von Braun zurück, der seine Verantwortung für seine beruflichen Tätigkeiten als Raketenbauer negierte.[1] Diese unter Ingenieuren und auch in der IT leider noch immer weit verbreitete Haltung sollte kritisch behandelt werden. Der Congress griff damit eines der zentralen Themen des FIfF auf, das die berufliche Verantwortung von Informatikern schon in seinem Namen als Anliegen kenntlich macht.

Das FIfF war dieses Jahr passend zum Motto auch besonders stark auf dem Congress präsent. Der FIfF-Stand war die ganze Zeit besetzt, meist mit mehreren Freiwilligen, und wurde gut besucht. An dieser Stelle möchten wir den Standbetreuern herzlich danken. Dieses Jahr kamen die Kisten mit den Materialien alle wohlbehalten und rechtzeitig an. Neben den FIfF-Kos und Broschüren fanden auch die neuen T-Shirts mit dem Cyberpeace-Logo dankbare Abnehmer. Es gab sie in weiß und in schwarz, der Lieblings*farbe* der Hacker. Restbestände können noch über die Geschäftsstelle erworben werden.

Das FIfF-Team am Stand

Neben dem Stand schaffte es das FIfF aber auch mit gleich drei Vorträgen in das Hauptprogramm, die alle gut besucht und in zahlreichen Medien (Links siehe Endnoten 2 bis 5) erwähnt wurden:

Sylvia Johnigk stellte im Vortrag *Cyberpeace statt Cyberwar* die friedenspolitische Cyberpeace-Kampagne des FIfF vor.[6] In ihren Vortrag flossen auch die Ergebnisse des gleichnamigen AKs von der FIfF-Jahrestagung 2012 in Fulda ein (siehe den Bericht auf den Seiten 55ff). Die angeregte Diskussion im Anschluss zeigte einmal mehr, dass das FIfF hier ein wichtiges Thema vorantreibt.

Sylvia Johnik – Cyberpeace statt Cyberwar

In einem mitternächtlichen Workshop wurden von einigen FIfFerlingen und weiteren Interessierten Strategien und Aktivitäten diskutiert, die die Cyberpeace-Kampagne weiter voranbringen.

Prof. Britta Schinzel hielt im riesigen Hauptsaal 1 den Vortrag: *Was ist, was kann, was soll Gender Studies Informatik?*[7] Sie ging auf drei Kategorien der Genderforschung ein und gab damit einen Eindruck von der Bandbreite der Themen, die jeweils mit konkreten Beispielen exemplarisch vorgestellt wurden. Sie erwähnte Untersuchungen darüber, wie unterschiedlich stark bestimmte Gruppen (Frauen-/Männer-Verhältnis, Altersverteilung, verschiedene Ethnien) in der Informatik als Fach in unterschiedlichen Ländern vertreten sind. Als Beispiel nannte sie den extremen Rückgang des Frauenanteils unter dem Informatik-Studierenden in Ostdeutschland nach der Wende. Auch die beim Studienpreis des FIfF ausgezeichnete Arbeit von Göde Both über Siri fand dabei Erwähnung.

Sebastian Jekutsch stellte die Frage: *Sind faire Computer möglich?*[8] Die schockierenden Bilder von Produktions- und Arbeitsbedingungen bei der Rohstoffgewinnung und Fertigung, zum Teil aus dem vom FIfF unterstützten Film *Behind the Screen* entnommen, erzeugten eine deutliche Wirkung beim Publikum. Mit der *Fair-IT-Maus* von *Nager-IT* stellte er das erste zumindest teilweise fair produzierte IT-Produkt vor, das im Anschluss auch

auf dem FIfF-Stand großes Interesse erregte. Im Projektstatus ist auch ein *Fair Phone*, das Gerüchten zufolge demnächst auf den Markt kommen soll. Anschließend ergab sich eine angeregte Diskussion, die zeigte, dass das Thema bei vielen Congressbesuchern auf großes Interesse stieß. Der Vortrag fand im Saal 2 in unmittelbarer Nähe des FIfF-Stands statt, der im Anschluss von zahlreichen Besuchern frequentiert wurde, die weiter diskutierten und Fragen stellten.

Neben den FIfF-Vorträgen wurde das Motto aber auch in zahlreichen weiteren gesellschaftspolitischen Vorträgen aufgegriffen. In der Keynote[9] appellierte Jacob Applebaum an das gesellschaftliche Engagement der Hacker, sich gegen Überwachungstechnologien zur Wehr zu setzen. Zwei ehemalige Mitarbeiter der NSA und ihre Anwältin berichteten von den Erfahrungen als Whistleblower.[10] Es wurden Beweise manipuliert und versucht, ihnen Landesverrat unterzuschieben.

Erschreckend waren auch die Berichte aus dem Thüringer Untersuchungsausschuss zur Rolle der V-Leute des Verfassungsschutzes im Rahmen der NSU-Affäre.[11]

Der CCC selbst berichtete über die Nachwirkungen seiner Enthüllungen zum Bayerntrojaner. Außerdem arbeitet der Club gerade an einer Verfassungsklage gegen die Antiterrordatei.[12]

Neben zahlreichen Hacking-Vorträgen zu Schwachstellen und wie man sie ausnutzt, oder wie man durch Reverse-Engineering IT kreativ nutzbar macht, kam auch der sonstige Spaß nicht zu kurz. Die *Fnord News Show*[13] war mal wieder das bestbesuchte Event und füllte sogar den riesigen Saal 1, der über 4000 Personen fasst.

Auf dem Congress wurden von einigen Teilnehmenden *Creeper-Cards*[14] (grün, gelb, rot) eingesetzt, die als Verwarnungs- oder Strafkarten bei sexuellen Übergriffen dienen sollten. Die Idee dahinter ist, Betroffenen damit eine effektive Möglichkeit zur Gegenwehr zu bieten.

Für das *Hacker-Jeopar*dy[15] wurde den Moderatoren eine Karte überreicht, was viele für eine völlig überzogene Reaktion hielten. Die anschließende *Anhörung* bei den Missbrauchsbeauftragten hatte nach Aussage einer Augenzeugin den Charakter eines unfairen Tribunals. Auch in weiteren Fällen wurden die Karten eher fragwürdig eingesetzt, etwa als ein Mann eine gelbe Verwarnung erhielt, weil er einer Frau die Tür aufgehalten hatte. Im Nachgang wurde der Einsatz der Karten kontrovers diskutiert. Bisher ist der Congress auch nicht als besonders problematisch aufgefallen, es herrscht im Gegenteil eine eher entspannte und tolerante Atomsphäre, die diesmal durch die größeren Räumlichkeiten noch unterstützt wurde. Man konnte sich diesmal sogar zum Plausch in eine gemütliche Ecke zurückziehen.

Britta Schinzel – Was ist, was kann, was soll Gender Studies Informatik?

Sebastian Jekutsch – Sind faire Computer möglich?

Der Congress war wieder einmal ein anregendes, interessantes und geselliges Ereignis, das wir weiterempfehlen können.

Anmerkungen

1 *https://www.youtube.com/watch?v=w5JmDNpjKYc*
2 *http://blog.zdf.de/hyperland/2012/12/ccc-cyberpeace-statt-cyberwar/*
3 *http://www.taz.de/CCC-Kongress-in-Hamburg/!108099/*
4 *http://www.zeit.de/digital/internet/2012-12/29c3-chaos-computer-club/*
5 *http://www.spiegel.de/netzwelt/netzpolitik/hardware-ethik-unfaire-tastaturen-und-blutige-smartphones-a-875173.html*
6 *http://mirror.fem-net.de/CCC/29C3/mp4-h264-HQ/29c3-5221-de-en-cyberwar_statt_cyberwar_h264.mp4; vgl. den Bericht auf den Seiten 55-57 in diesem Heft*
7 *http://mirror.fem-net.de/CCC/29C3/mp4-h264-HQ/29c3-5396-de-en-gender_studies_informatik_h264.mp4; siehe auch den Bericht auf den Seiten 12-14 in diesem Heft*
8 *http://mirror.fem-net.de/CCC/29C3/mp4-h264-HQ/29c3-5121-de-en-sind_faire_computer_moeglich_h264.mp4; siehe auch den Bericht auf Seite 15 in diesem Heft*
9 *http://mirror.fem-net.de/CCC/29C3/mp4-h264-HQ/29c3-5385-en-not_my_department_h264.mp4*
10 *http://mirror.fem-net.de/CCC/29C3/mp4-h264-HQ/29c3-5338-en-enemies_of_the_state_h264.mp4*
11 *http://mirror.fem-net.de/CCC/29C3/mp4-h264-HQ/29c3-5287-de-en-hinter_den_kulissen_nsu_h264.mp4*
12 *http://mirror.fem-net.de/CCC/29C3/mp4-h264-HQ/29c3-5382-de-en-antiterrordatei_h264.mp4*
13 *http://mirror.fem-net.de/CCC/29C3/mp4-h264-HQ/29c3-5198-en-de-fnord_jahresrueckblick2012_h264.mp4*
14 *http://events.ccc.de/congress/2012/wiki/Creepercards*
15 *http://mirror.fem-net.de/CCC/29C3/mp4-h264-HQ/29c3-5309-de-en-hacker_jeopardy_h264.mp4*

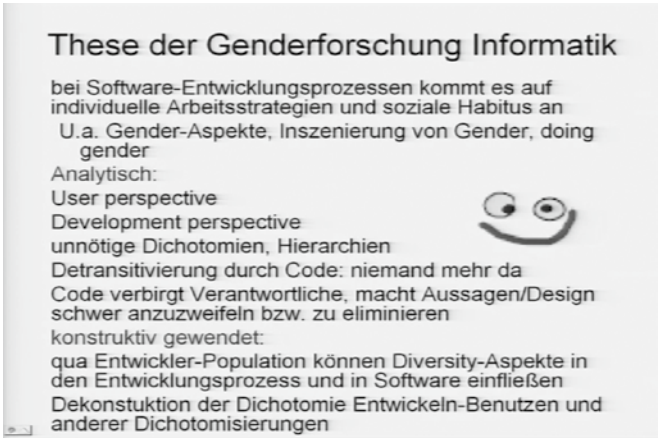
Britta Schinzel

Was ist, was kann, was soll Gender Studies Informatik?

Behandelt wird die Frage, was Informatik und Geschlecht miteinander zu tun haben, und womit sich Genderforschung Informatik beschäftigt. Einerseits wird Informatik als objektives mathematisch-technisches Fach angesehen, in dem soziale oder Geschlechter-Unterschiede nichts zu suchen haben. Blickt man andererseits in Informatik-Lehrveranstaltungen, dann überwiegt ein Geschlecht unübersehbar. Die Genderforschung beabsichtigt unter anderem – und ist in der Lage –, diesen Widerspruch zu erklären.

Das deutsche Wort *Geschlecht* bezeichnet die Begriffe *sex* (biologisches Geschlecht) und *gender* (soziales Geschlecht), die wegen der Wechselwirkungen zwischen Biologie und Sozialem untrennbar vereint sind. Bestes Beispiel für solche wechselweisen Einflüsse ist die Plastizität des Gehirns, welches sich durch „Embodiment" von Erfahrungen variabel materialisiert und dessen Formung umgekehrt die Wahrnehmungen beeinflusst. Gender wird jedoch oft vereinfachend als isolierte Kategorie betrachtet, die sich in sozialen Interaktionen, in gesellschaftlichen Prozessen, in der eigenen Körperwahrnehmung und sogar auch in technischen Artefakten realisiert. Der Begriff *Gendering* bezeichnet eben jene soziokulturellen Prozesse, die Gender konstruieren, und die sich u. a. in Technik verfestigen.

In der Genderforschung werden Konzepte von Männlichkeit oder Weiblichkeit nicht vorausgesetzt, sondern z. B. danach gefragt, ob InformatikerInnen Annahmen haben über Geschlecht, und wenn ja, welche, und ob bzw. wie sie sich als Männer oder Frauen inszenieren (*„doing gender"*), weiter ob bzw. wie die Vorstellungen und Ausprägungen von Geschlecht im Verlauf der Geschichte veränderlich oder auch aktiv veränderbar (*„degendering"*) sind. Eine These der Genderfoschung Informatik ist es weiter, dass es bei Entwicklungsprozessen auf individuelle Arbeitsstrategien und sozialen Habitus ankommt, d.h. dass auch persönliche oder soziale Gender-Einstellungen in die Software-Entwicklung Eingang finden und sich dann in den Produkten verfestigen können (*„Ko-Konstruktion von Technik und Geschlecht"*). Solches geschieht beispielsweise, wenn unnötige Dichotomien (d. h. Grenzziehungen und Unterscheidungen) oder Hierarchien in Entwurf, Modellen oder Ontologien oder Übergeneralisierungen aufgrund von *„ego-approach"* etabliert werden oder indem Auslassungen und blinde Flecken zu inadäquaten Problemlösungen führen, wie bei unsichtbaren Arbeitsanteilen etwa im Sekretariatsbereich oft geschehen. Hinzu kommt, dass der endgültige Code meist unzugänglich und oft genug materiell verfestigt ist (*„Ko-Materialisierung von Technik und Geschlecht"*), somit Verantwortliche verbirgt, was es schwer macht, implizit im Code verborgene Aussagen oder das Design anzuzweifeln bzw. zu eliminieren.



Genderforschung Informatik analysiert und kritisiert schädliches Gendering in Informatik und Softwareentwicklung, um es in einer konstruktiven Wendung durch neutrales Design oder unschädliches Gendering (wissend, dass notwendigerweise alle soziotechnischen Prozesse *„gegendert"* sind) zu ersetzen. So können bereits qua diversifizierter personeller Beteiligung Diversity-Aspekte in den Entwicklungsprozess und in Software einfließen. Und bewusster Umgang mit Phänomenen des Gendering kann zu adäquateren Software-Problemlösungen führen.

Was ist Gender Studies Informatik?

Allgemein werden die Gender-Forschungen zur Technik unterteilt in die Kategorien:

1. Frauen, Männer, Altersgruppen, Ethnien, soziale Schichten, etc., die in dem Fach/Beruf vertreten sind. Wie befinden sie sich dort? Hierzu gehören beispielsweise vergleichende Studien zwischen Ländern und Kulturen, die erklären, warum die Frauenbeteiligung in der Informatik in allen nah- und fernöstlichen Ländern so viel höher ist als hierzulande. Und solche, die zeigen, dass die Einladung von breiteren Kompetenzen und curricularen Änderungen, die bereits zu Studien-

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.

beginn mehr Motivation aus den Anwendungen zu gewinnen erlaubt, zu einer diversifizierten Studierendenpopulation führen kann. Ein anderes Beispiel für diese Kategorie stellt unsere gerade beendete DFG-Studie zu Weltbildern der Informatik in Deutschland dar.

2. Wie wird Geschlecht in dem entsprechenden Fach behandelt, mit welchen Folgen? Die u. a. von der Informatik bereitgestellte Bildgebung und Bildbearbeitung sind Medien, mittels derer auch Geschlecht repräsentiert wird. Sie erleichtern die öffentliche und die medizinische Präsentation von Stereotypen und verfestigen so unnötigerweise überkommene Geschlechtervorstellungen.

3. Wie wirken sich historische oder/und aktuelle Einseitigkeiten der Beteiligung in Zielen, Methoden, Modellen und Ergebnissen des jeweiligen Faches aus? Als erstes Beispiel wurden Studien zur Spieleentwicklung vorgestellt. Interessant ist zudem eine Studie über die *Virtual Personal Assistant* (VPA) *Siri*, die tiefergehende Theorien zur Analyse und Reflexion der verwendeten Hintergrundannahmen und der Gestaltung(smöglichkeiten) verwendet.

Ad 1. A. Zum ersten Punkt wurden zunächst einige wenige Zahlen vorgestellt, die zeigen, dass die geringe Frauenbeteiligung in der Informatik in deutschsprachigen Ländern kein Naturgesetz ist. Es fällt auf, dass in den nordwestlichen Industrieländern viel weniger Frauen in technischen Bereichen zu finden sind als in den später industrialisierten Ländern des Ostens und Fernostens, aber auch in Südamerika.[1] Weiter scheint der Kommunismus im Vergleich zum Kapitalismus Frauen zur gleichberechtigten Teilnahme an technischen Berufen eingeladen zu haben. Aber auch in kapitalistischen Ländern ist es möglich, eine paritätische Geschlechterbeteiligung zu erreichen, wie es das Beispiel der Informatik an der Carnegie-Mellon-Universität, Pittsburgh, USA zeigt. Obgleich Anfang der 1990-er Jahre die Frauenbeteiligung bei 8 % lag, konnte sie innerhalb von weniger als 10 Jahren auf heute stabile 46 % gesteigert werden. Auch hält die CMU-Computer-Science seit 20 Jahren im amerikanischen Ranking in Informatik die Nr. 1. Die Änderung wurde erreicht durch Ergänzung der Eingangsqualifikationen durch Zugangsprüfungen um Kommunikations-, Organisations- und Sprachfähigkeiten, weiter durch Änderungen des Curriculums, indem von Beginn des Studiums an eine Kontextualisierung in Anwendungen erfolgte und schließlich durch eine wissenschaftliche Begleitung des Änderungsprozesses, um auf auftauchende Probleme reagieren zu können.[2]

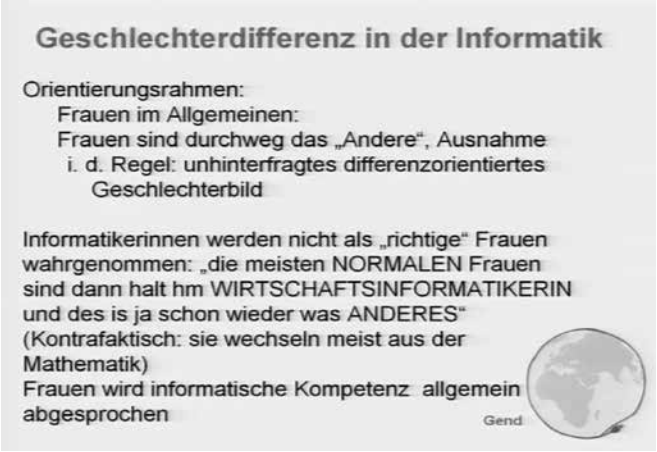
Ad 1. B. Im DFG-Projekt *Weltbilder der Informatik* befragten wir Informatik-Studierende zu Beginn des Studiums und ab dem 5. Semester nach ihren Einstellungen und jenen Weltbildern, die für die Informatik relevant sind, also Technik-, Wirklichkeits- und Menschen-Bildern, Bildern der Nutzenden und auf die Informatik selbst. Wir gehen davon aus, dass solche in Informatik-Handlungen einfließen und damit Einfluss auf die produzierte Software haben. Denn im Verlauf des gesamten Software-Entwicklungsprozesses werden unzählige – große und kleine – Entscheidungen getroffen, die keineswegs alle explizit auf Qualitätsstandards oder professionellen Normen beruhen, sondern oft dem Gutdünken der Entwickelnden anheim gestellt sind. Somit bilden die Weltbilder der Entwickelnden einen wichtigen, bisher aber noch nicht berücksichtigten Qualitätsfaktor für Software. In einer Sekundärevaluation wurden nicht nur die Weltbilder, sondern u. a. auch Kategorien wie Diversity, Geschlecht und die Frage nach der Verantwortung von InformatikerInnen untersucht.[3] Alle Kategorien, Technik-, Informatik- und Menschenbilder, Geschlechter- und Ethikbilder hängen zusammen und bedingen sich gegenseitig. Geschlecht hier einmal dennoch isoliert betrachtet zeigt ein fast durchweg differenzorientiertes Geschlechterwissen. Frauen, direkt gefragt, fühlen sich „gut aufgenommen". Sie erfahren jedoch besondere Aufmerksamkeit, werden belächelt und wollen oder müssen sich beweisen. Unter Kompetenzen, die eine InformatikerIn haben muss, nennt eine Frau als erstes: Aushalten, dass man allein unter Männern ist, dann erst mathematische Fähigkeiten, etc. Für die Studierenden ist Informatik männlich und allgemein wird Frauen informatische Kompetenz abgesprochen. Frauen in der Informatik aber sind immer das „Andere", die Ausnahme, und sie werden nicht als „richtige" Frauen wahrgenommen.[4]

Ad 2. Zum Thema Geschlecht in Science and Technology trägt auch die Informatik mit ihren Bildverarbeitungsmethoden zur Erzeugung visueller Evidenz von Geschlechterdifferenzen im Gehirn bei. Zunächst ist es wichtig zu wissen, dass funktionelle medizintechnische Hirnbilder keine Abbilder des Körperinneren sind, sondern Konstruktionen über kontingent kombinierte physikalische mathematische, statistische und informatische Verfahren.

Als Beispiel wurden die häufig zitierten Lateralisierungsunterschiede bei der Sprachverarbeitung einer kritischen Analyse unterzogen. Untersuchungen zur Reimerkennung mit kleinen Befundzahlen, die beidseitige neuronale Aktivierung bei Frauen und linksseitige bei Männern zeigen (allerdings ohne Leistungsunterschiede), werden insbesondere für die Popularisierung wissenschaftlicher Ergebnisse universalisiert[5], obgleich es auch umgekehrte Ergebnisse gibt und sich bei großen Fallzahlen keine signifikanten Unterschiede zeigen.[6] So werden Geschlechterstereotype in die Neurowissenschaften eingeschrieben und popularisiert.[7]

Ad 3. Unter dieser letzten Kategorie werden jene Gender-Phänomene zusammengefasst, die tiefer in der Wissenschaft und in ihren Produkten eingelassen sind.

Das erste Beispiel behandelt Untersuchungen zur Spiele-Entwicklung. An der University of East London ließ Eva Turner ihre Studierenden beim Erlernen von Visual Basic Außerirdischen bildlich erklären, was Informatiker und Informatikerinnen tun.[8] Die bild-



liche Modellierung von Informatikern geschah nach Fotos gut aussehender amerikanischer Filmschauspieler, während Informatikerinnen abstrakt dargestellt wurden. In einer Wiener Spielentwicklungsfirma zeichneten Entwickelnde ihre Gedanken bei der (Weiter-) Entwicklung eines existierenden Abenteuerspiels für den Massenmarkt auf. Männliche Spielcharaktere wurden anatomisch korrekt modelliert anhand von Fotos realer Personen, die einzige weibliche Figur aber lehnte sich an eine bestehende Computer-generierte Figur an, die anatomisch unrealistisch war – obgleich die Beteiligten graphischen Realismus als Qualitätsanforderung angenommen hatten, d.h. das Verständnis von Realismus ist nicht neutral, sondern stellt kulturelle Phantasien von Differenz als natürlich dar. Auch die Selbstkonzepte der Entwickelnden vor der Untersuchung besagten, sie seien objektiv und neutral, während sich danach große Betroffenheit zeigte.[9]

Ein weiteres Beispiel ist die stark theoretisch geleitete Analyse von Göde Both der iPhone-Applikation *Siri*[10], eine personalisierbare Software-Agentin für multimodale Benutzungsschnittstellen, welche er mittels Rolle (in der Interaktion mit Benutzenden), Initiative (aktiv oder passiv) und Geschlecht charakterisiert. *Siri* tätigt über direkte Spracheingabe Anfragen, Suchen, Bestellungen oder Reservierungen, Flugstatus, etc. und die Applikation beansprucht, Arbeit zu ersparen über das Interaktionsparadigma der Delegation. Both exploriert die Anthropomorphisierungen, die Konfiguration der Nutzenden und die Einschreibungen der geschlechtsspezifischen Arbeitsteilung in *Siri*, sowohl als Mann (Jo) wie als Frau (Donna). Siri konfiguriert Nutzende als westliche Individuen und weist sich als deren (weise, weibliche) Assistentin aus. Die *agency*, die Nutzenden durch *Siri* eingeräumt wird, besteht darin, aus einem vorgegebenen Angebot eine Wahl zu treffen, auch wenn völlige Freiheit der Fragen oder Anweisungen suggeriert wird. Der Prozess der Spracherkennung wird als Nachdenken inszeniert. Die Dialoganalyse erweist die Inszenierung von *Siri* als Cyborg und in der Kommunikation als zurückhaltend, kooperativ, verständnisvoll, unagressiv und machtlos. Auf Beleidigungen oder Kritik reagiert *Siri* entschuldigend, auf Lob bescheiden und selbstherabsetzend. Sie erfüllt mit dem gemeinsamen Erarbeiten von Lösungen, aktiver Unterstützung des Sprechers, Bezugnahme auf Vorangegangenes, konstruktiver Kritikfähigkeit so überwiegend weibliche Stereotype. Umgekehrt die Konfiguration der Nutzenden: mit dem Fokus auf Konsum, Reisen und Unterhaltung imaginiert *Siri* Konsumenten, die hochmobil, wohlhabend und berufstätig sind, die unabhängig über zeitliche Ressourcen verfügen können, insgesamt also das Bild eines männlichen Nutzers, welcher sich auf Geschäftsreisen befindet. Der von Apple angesprochene „everybody" wird im wesentlichen von höheren Angestellten und Geschäftsleuten verkörpert, denen der neoliberale Unternehmer seiner selbst als Norm eingeschrieben ist.

Mit alledem erscheint die These der Genderforschung, dass es bei Software-Entwicklungsprozessen auf Weltbilder, Geschlecht und Habitus ankommt, bestätigt.

Was kann, was soll Gender Studies Informatik?

Aus den o.g. Beispielen ergibt sich zwangsläufig ihr Sinn: Gender Studies sind Augenöffner für Einseitigkeiten, die in Zielen, Methoden und Prozessen der Technologien, in Software, ihren Modellen und den Benutzungsmöglichkeiten eingelassen sind. Bei der Rezeption solcher Analysen kann sich der Blick weiten, und konstruktiv gewendet können so adäquatere Lösungen gefunden werden, was letztlich auch ökonomische Folgen nach sich ziehen kann.

Anmerkungen

1 *Näheres hierzu findet sich in meinen Texten zum Kulturvergleich unter www.mod.iig.uni-freiburg.de/cms/fileadmin/publikationen/online-publikationen/Frauenanteil.Informatik.International.pdf, ff.*

2 *Fisher, A., Margolis, J., Unlocking the Clubhouse: the Carnegie Mellon Experience, in: ACM SIGCSE Bulletin, vol. 34, no. 2, S. 79-83, Juni 2002.*

3 *Britta Schinzel, Monika Götsch, Yvonne Heine, Karin Kleinn, Michael M. Richter: Verlernen Informatik-Studierende Verantwortungnahme?, FIfF-Kommunikation 1/2012, S. 55-63, ISSN 0938-3476.*

4 *Gesamt-Veröffentlichung folgt im Informatik-Spektrum 2, 2013.*

5 *vgl. Pease, Allan & Pease, Barbara. Why Men Don't Listen & Women Can't Read Maps, London: Orion, 2001.*

6 *z. B. Frost, J., Binder, J.R.; Springer, J.A.; Hammeke, T.A.; Bellgowan, P.S.F.; Rao,S.M.; Cox, R.W.; Brain 122, 199-208, 1999; Binder et al. (2000). Reply to „Language processing in both sexes: evidence from brain studies." Brain 123 (Pt 2): 404; Kaiser, Anelis/Haller, Sven/ Schmitz, Sigrid/Nitsch, Cordula (2009): „On sex/gender related similarities and differences in fMRI language research"; in: Brain Res. Rev. 61, 49-59.*

7 *vgl. z. B. Schinzel, Britta: De-gendering neuro-images: Contingencies in the construction of visualisation technologies and their use for establishing sex-differences; Interdisciplinary Science Reviews, Vol. 36 No. 2, June 2011, 168–79, Pollitzer, E. et al. (eds.): Special Issue on Gender in Science. (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1895435##); Schinzel, Britta: Wissenskonstruktion durch Zeigen: zur Erzeugung visueller Evidenz und medizinischer Erkenntnis mittels bildgebender Verfahren. In: Robert Schmidt, Wiebke-Marie Stock, Jörg Volbers (Hrsg.): „ZEIGEN" Dimensionen einer Grundtätigkeit, Velbrück Wissenschaft, Weilerswist 2011, ISBN 978-3-942393-22-5, S. 153-178)*

8 *Eva Turner: Designing webpages about computer scientists for ETs; FIfF-Kommunikation 3/2001.*

9 *Allhutter, D.; Hanappi-Egger, E.; John, S. (2008) Mind Scripting: Zur Sichtbarmachung von impliziten Geschlechtereinschreibungen in technologischen Entwicklungsprozessen. In: Schwarze, B.; David, M.; Belker, B.C. (Hrsg.), Gender und Diversity in den Ingenieurswissenschaften und der Informatik; Bielefeld: UVW, S. 153-165.*

10 *http://edoc.hu-berlin.de/master/both-goede-2011-07-19/PDF/both.pdf*

Sebastian Jekutsch

Sind faire Computer möglich?

Das im Titel genannte Thema ist für einen Hackerkongress eher untypisch. Umso überraschender, dass der größere der beiden kleinen Säle eingeplant wurde. Und siehe da: Er war gut gefüllt.

Inhaltlich war der Vortrag eine gekürzte und aktualisierte Version des Fuldaer Workshop-Impulses, siehe den entsprechenden AG-Bericht und die Nachrichten in der neuen Kolumne *Betrifft: Faire Computer,* beides an anderer Stelle in diesem Heft. Statt also die Inhalte zu wiederholen möchte ich lieber über die Reaktion auf den Vortrag berichten.

Online wurde über den Vortrag von *golem.de* (*Zeit Online* hat diesen Beitrag übernommen), *Heise Online News*, *Spiegel Online* und *netzpolitik.org* berichtet. Der Tenor bei allen drei: Puh, die Hoffnungen auf eine fairer werdende IT-Produktion sind leider gering. Aber immerhin gibt es erste Initiativen. Es bleibt der Frust, dass man als Endkunde nicht viel machen kann. Der Vortrag wirkte damit wohl ein wenig ernüchternd, nachdem doch schon Ende letzten Jahres Gerüchte (ohne Grundlage) über ein bald erscheinendes Faires Smartphone die Runde machten.

Am Ende des Vortrags blieb reichlich Zeit für eine Diskussionsrunde. Es gab Empörung über unseren Konsum und Enttäuschung über die Wegwerfprodukte. Natürlich wünscht man sich ein Siegel, das einem sagt, was man kaufen kann. Und wenn schon eine teilfaire Maus fünfmal so teuer ist wie ein Billigprodukt vom Blödmarkt, wie teuer wird dann erst ein faires Handy?

Leider kann ich diese und einige anderen der berechtigten Fragen noch nicht beantworten. Und wie immer bei Vorträgen über ein so umfangreiches Thema musste vieles ungesagt bleiben, was für eine Meinungsbildung nötig gewesen wäre. Zum Beispiel, dass manche Firmen gar nicht wissen, wohin mit ihren Gewinnen, und sie dann ihren Aktionären schenken statt den Arbeitern am Fließband. Oder dass der Abbau der Erze in Afrika enorm günstig ist und vor allem die Zwischenhändler mit ihren Kontakten Geld damit verdienen – ja sogar spekulieren und dadurch die Rohstoffe teuer machen, weswegen immer billigere Abbaumöglichkeiten gesucht werden. Es sind mächtige Marktstrukturen verantwortlich, dass das Geld nicht bei denen ankommt, die während des Vortrags gezeigt wurden: Minenarbeiterinnen, Schüler in Produktionshallen, Hinterhofschrottverwerter.

Die genannten Online-Quellen bieten auch die Möglichkeit zur Kommentierung. Auch hier überwiegt die „Leider-Geil"-Haltung: Die neuesten Geräte möchte man schon gerne haben, natürlich zu einem günstigen Preis. Man entdeckt auch wertvolle Abwägungen und Ausblicke, bei Heise z. B. eine fruchtbare Diskussion, wie teuer fair eigentlich sein muss und bei netzpolitik.org, dass man als Hersteller durchaus etwas bewegen kann, wenn man sich bemüht. Meist endet die Diskussion aber darmit, dass man doch besser wieder in Deutschland produzieren sollte, dass die Geräte langlebiger und wiederverwendbarer sein sollten oder dass es halt so ist wie es ist und immer so sein wird. Und, natürlich, wie bekloppt der Name vom FIfF doch sei ☺.

Angesprochen und angeschrieben wurde ich im Anschluss und den Tagen nach dem Vortrag von vielfältigen Initiativen, einer Bildungseinrichtung zur Aufbereitung von Altgeräten, einem Portal zur Fairness-Bewegung, einem Medienkongress, einer kleinen linken Filmreihe. Unter diesen könnte eine Perle sein, und vielleicht ist eine solche Vernetzung der wichtigste Erfolg eines öffentlichen Vortrags.

Als Fazit nehme ich für mich mit: Auf einige Fragen, vor allem auf die, was man als Konsument tun kann, damit sich die Lage verbessert, muss ich noch pointierter antworten. Was waren die in der Vergangenheit erfolgreichen Strategien? Was funktioniert schon? Wie sage ich es meinem Händler und dem Markenhersteller? Meine Überzeugung ist, dass viele verschiedene parallele Herangehensweisen nötig sind und zu kleinen Erfolgen führen werden. Die Lösung ist aus meiner Sicht, dass wir als Kunden Alternativen, eine Auswahl, haben müssen, um dann das richtige wählen zu können.

Und: Der latente Widerspruch zu den Umweltaspekten, die ich in meinen Beiträgen immer ganz außen vor lasse, muss thematisiert werden: Ich bin aus sozialer, menschenrechtlicher Sicht nicht der Meinung, dass unserer enormer Konsum schlecht sei. Nichtkaufen ist nicht die Lösung. Fair sein, d.h. Menschen, die für mich arbeiten, ein angenehmes Leben zu ermöglichen, ist etwas anderes als nicht unfair sein, d.h. den Menschen nichts zu arbeiten zu geben. Die Arbeiterinnen in Südamerika, Afrika und China würden nicht glücklicher, wenn wir aufhörten, ihre Produkte zu kaufen, weil uns nicht gefällt, wie sie arbeiten.

Zum Schluss noch diese Bemerkung: Der Aufwand und die Aufregung im Vorfeld und Nachgang eines solchen Vortrags sind nicht gering für jemanden, der eine solch schwierige Materie nicht gerade regelmäßig vor unbekanntem Publikum referiert. Auch werde ich die gewonnene Öffentlichkeit schon aus Zeitgründen leider nicht optimal nutzen können. Die Arbeit für das FIfF ist letztlich doch nur ein Hobby.

Sebastian Jekutsch

Sebastian Jekutsch ist FIfF-Mitglied aus Hamburg. Kontakt: *sj@fiff.de.*

Werner Hülsmann

Gesetz zum Beschäftigtendatenschutz – eine „unendliche Geschichte“

Die Regierung will es, die Gewerkschaften fordern es, die Betriebe brauchen es: Ein Gesetz zum Beschäftigtendatenschutz. Aber der alte Spruch „Was lange währt, wird endlich gut“ gilt für den Beschäftigtendatenschutz leider (noch?) nicht. Obwohl das Thema schon über mehrere Legislaturperioden zumindest diskutiert wird, ist bis zum Redaktionsschluss von keiner Regierung ein Gesetzesentwurf zum Beschäftigtendatenschutz vorgelegt worden, der diesen Namen verdient hätte.

Ende Januar diesen Jahres konnte die Initiative *Beschaeftigendatenschutz.net*[1] mit Unterstützung von *campact*, *Deutscher Vereinigung für Datenschutz*, *digitalcourage* und selbstverständlich auch dem FIfF einen ersten Erfolg verbuchen:

> *„Das viel kritisierte Gesetz zum Beschäftigtendatenschutz ist vorerst vom Tisch. Der Protest eines breiten Bündnisses und von fast 70.000 Unterschriften war erfolgreich. Wie heute verlautete, werden weder der Innenausschuss noch der Bundestag das Gesetz in dieser Woche behandeln – wie ursprünglich geplant. Eine große Schlappe für den Gesetzgeber, ein wichtiger Erfolg für Datenschutz- und Bürgerrechtsorganisationen der Zivilgesellschaft.“*[2]

Was war passiert?

Ein Überraschungscoup der Regierung und der Regierungsfraktionen konnte im Januar 2013 verhindert werden. Zu dem bereits am 3. September 2010 von der Bundesregierung in den Bundesrat und am 15. Dezember 2010 nur leicht verändert in den Bundestag eingebrachten „Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes“ (vgl. [BT-Drs. 17/4230]) war es nach einer Anhörung im Innenausschuss 2011 ziemlich ruhig geworden. Im April 2012 drangen zwar Änderungsvorschläge an die Öffentlichkeit[3], aber da nichts weiter passierte, vermuteten immer mehr Expertinnen und Experten, dass es in dieser Legislaturperiode nicht mehr zu einem Gesetzesbeschluss des Bundestages kommen würde. Dann aber überschlugen sich die Ereignisse:

Am 10. Januar 2013 wurde von der Regierungskoalition ein Änderungsantrag [17(4)636] für die Sitzung des Innenausschusses am 16. Januar 2013 eingebracht. Im Gegensatz zu den Gesetzentwürfen selbst werden derartige Änderungsanträge für Ausschusssitzungen nicht veröffentlicht, sondern nur die Beschlussempfehlungen der Ausschüsse. Im Bundestag sollte der Gesetzentwurf bereits am 1. Februar abschließend in 2. und 3. Lesung behandelt werden. Allerdings wurde der Änderungsantrag einigen Mitgliedern der Initiative *Beschaeftigtendatenschutz.net* zugespielt, so dass bereits am 12. Januar 2012 eine Synopse aus Gesetzentwurf und Änderungsantrag veröffentlicht werden konnte[4]. Hierdurch war es möglich, dass sowohl amtliche Datenschutzbeauftragte als auch Gewerkschaften und andere am Beschäftigtendatenschutz interessierte Kreise deutliche Kritik sowohl am Entwurf und Änderungsantrag als auch an der geplanten Vorgehensweise äußern konnten. Das führte dazu, dass die Behandlung von der Tagesordnung der Innenausschusssitzung am 16. Januar 2013 abgesetzt wurde. Der Versuch der Regierungskoalition, (nahezu) unbemerkt von der Öffentlichkeit in kürzester Zeit einen unbeliebten Gesetzentwurf durchzupeitschen war somit erst mal vereitelt. Zwar wurde der Tagesordnungspunkt noch für die Tagesordnung der Innenausschusssitzung am 30. Januar 2013 eingeplant. Der öffentliche Protest war aber schon so groß, dass am 29. Januar der Beschäftigtendatenschutz sowohl von der Tagesordnung des Innenausschusses als auch von der Tagesordnung des Bundestages genommen wurde – zu diesem Zeitpunkt hatte der campact-Appell[5] schon knapp 70.000 Unterschriften erhalten.

Vorgeschichte

Um die aktuelle Diskussion um gesetzliche Regelungen zum Beschäftigtendatenschutz besser einordnen zu können, ist ein Blick auf die Geschichte des Beschäftigtendatenschutzes (früher überwiegend als Arbeitnehmerdatenschutz bezeichnet) hilfreich.

Das Volkzählungsurteil 1983 – Ein Meilenstein auf dem Weg zum Beschäftigtendatenschutzgesetz

Im sogenannten Volkzählungsurteil vom 15. Dezember 1983 hat das Bundesverfassungsgericht (BVerfG) das Grundrecht auf informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht und dem Schutz der Menschenwürde aus Art. 1 Abs. 1 und Art. 2 Abs. 2 Grundgesetz abgeleitet. Nach den Ausführungen des BVerfG gibt es „kein belangloses Datum mehr“. Beschränkungen dieses Grundrechts „bedürfen einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht“[6].

Der ehemalige Vorsitzende am Bundesarbeitsgericht Prof. Franz Josef Düwell (Honorarprofessor am Fachbereich Rechtswissenschaft der Universität Konstanz) sah und sieht hier den Gesetzgeber in der Pflicht: „Die Erfüllung dieser Voraussetzungen im Arbeitsleben erfordert eine bereichsspezifische Regelung.“[7]. Wie beim allgemeinen Datenschutzgesetz war auch hier wieder Hessen der Vorreiter.

> *„Mit der zweiten Novellierung seines Landesdatenschutzgesetzes am 11. November 1986 ging das Bundesland Hessen einen Schritt in diese Richtung. Es schuf dank seines engagierten Datenschutzbeauftragten Prof. Dr. Simitis die erste Norm eines gesetzlichen Beschäftigten-Datenschutzes. Der Bund war erst nach über 22 Jahren später soweit.“*[8]

Die Regelung im Hessischen Landesdatenschutzgesetz galt allerdings nur für die Beschäftigten des Landes Hessen, für die Beschäftigten in privatwirtschaftlichen Firmen und Institutionen galten weiterhin die sehr allgemeinen Regelungen des Bundes-

datenschutzgesetzes (BDSG) und das sich vor allem durch die Rechtsprechung des Bundesarbeitsgerichts (BAG) entwickelte Richterrecht[9]. Der damals zuständige Bundesarbeitsminister der schwarz-roten Koalition, Olaf Scholz, hat zwar noch am 4. September 2009 – kurz vor der Bundestagswahl – einen eigenständigen Diskussionsentwurf vorgestellt, dieser hatte aber nach der Wahl, die zur aktuellen schwarz-gelben Koalition führte, keine Chance mehr auf eine vertiefte Diskussion.

Beschäftigtendatenschutz im Bundesdatenschutzgesetz

Zum 1. September 2009 trat ein neuer Paragraph im BDSG in Kraft: § 32 Beschäftigtendatenschutz. Dessen Regelungen vermittelten den Eindruck, dass die Regierung auf Grund der vielen Skandale um Überwachungen von Arbeitnehmern und Arbeitnehmerinnen (genannt seien hier exemplarisch Deutsche Bahn AG, Deutsche Telekom AG und Lidl) sich einem Handlungsdruck ausgesetzt sah. Inhaltlich weichen die Regelungen des § 32 BDSG nicht von der etablierten Rechtsprechung der Arbeitsgerichte ab. Zwar ist es – gerade für betriebliche Datenschutzbeauftragte – hilfreich, wenn wesentliche Grundprinzipien zum Beschäftigtendatenschutz als Gesetzestext und nicht nur in unzähligen Gerichtsurteilen vorliegen, ein großer Wurf war und ist der Paragraph zum Beschäftigtendatenschutz aber nicht. So bleiben nach wie vor viele Fragen aus der täglichen Praxis im Betrieb gesetzlich ungeregelt. Einige Beispiele:

- Unter welchen Umständen ist im Betrieb – während der Betriebszeiten – eine Videoüberwachung zulässig?
- Unter welchen Umständen kann eine Einstellung oder Versetzung von der Zustimmung zu einer ärztlichen Untersuchung abhängig gemacht werden?
- Wie sind Maßnahmen zur Korruptionsbekämpfung oder zum Abgleich mit den EU-Terrorlisten zu gestalten?
- Welche personenbezogenen Daten dürfen im Rahmen eines Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden?
- Ist eine Recherche in sogenannten sozialen Netzwerken (XING, StudiVZ, MeinVZ, Facebook usw.) zulässig, und wenn ja, welche Informationspflichten hat der Arbeitgeber gegenüber BewerberInnen und Beschäftigten?

Ein Gesetz zur Regelung des Beschäftigtendatenschutzes war also weiterhin erforderlich. Das war auch der schwarz-gelben Regierungskoalition bewusst, die im Koalitionsvertrag festhielt:

> *„Privatheit ist der Kern persönlicher Freiheit. Wir setzen uns für eine Verbesserung des Arbeitnehmerdatenschutzes ein und wollen Mitarbeiterinnen und Mitarbeiter vor Bespitzelungen an ihrem Arbeitsplatz wirksam schützen. Es dürfen nur solche Daten verarbeitet werden, die für das Arbeitsverhältnis erforderlich sind. Datenverarbeitungen, die sich beispielsweise auf für das Arbeitsverhältnis nicht relevantes außerdienstliches Verhalten oder auf nicht dienstrelevante Gesundheitszustände beziehen, müssen zukünftig ausgeschlossen sein. Es sollen praxisgerechte Regelungen für Bewerber und Arbeitnehmer geschaffen und gleichzeitig Arbeitgebern eine verlässliche Regelung für den Kampf gegen Korruption an die Hand gegeben werden. Hierzu werden wir den Arbeitnehmerdatenschutz in einem eigenen Kapitel im Bundesdatenschutzgesetz ausgestalten."*[10]

Der Gesetzentwurf der Bundesregierung und die Änderungsvorschläge der Regierungskoalition

Nach zwei heftig umstrittenen Referentenentwürfen beschloss das Bundeskabinett im August 2010 einen Gesetzentwurf, den es am 3. September 2010 in den Bundesrat eingebrachte. Der Bundesrat nahm im November kritisch Stellung. Allerdings hielt es die Bundesregierung überwiegend nicht für nötig, diese Kritik zu berücksichtigen, und brachte den Gesetzentwurf nahezu unverändert am 15. Dezember 2010 in den Bundestag ein. Im Mai 2011 gab es dann eine Anhörung von Sachverständigen, in der heftige Kritik am Gesetzentwurf geäußert wurde.[11] Der Änderungsantrag der Regierungskoalition vom 10. Januar 2013 (s.o.) hätte zwar einige Verbesserungen, aber auch einige Verschlechterungen im Gesetzentwurf gebracht und nichts daran geändert, dass es besser wäre, keine Regelung zum Beschäftigtendatenschutz zu verabschieden, als diesen Gesetzentwurf (mit oder ohne Änderungsantrag).

Kritik am Gesetzentwurf

An dieser Stelle können nur einige wenige Kritikpunkte kurz und knapp dargestellt werden. Zu weiteren Kritikpunkten und ausführlicher kritischer Würdigung sei auf die oben erwähnte Sachverständigenanhörung und auf die Blog-Beiträge von Beschaeftigendatenschutz.net[12] verwiesen. Hauptsächliche Kritikpunkte an dem Gesetzentwurf in der Fassung des Änderungsantrags für den Innenausschuss sind:

- Statt Beschäftigte vor ausufernder Überwachung zu schützen, würde Arbeitgebern die Überwachung in einigen Bereichen erleichtert. Dies gilt insbesondere bei der

Werner Hülsmann

Werner Hülsmann, Dipl. Inform., selbstständiger Datenschutzberater und Datenschutzsachverständiger, externer Datenschutzbeauftragter, Konstanz, Beiratsmitglied des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V.

Videoüberwachung im Betrieb und bei der Aufzeichnung von Gesprächen in Callcentern, sofern der Arbeitgeber die Beschäftigten auf diese hinweist.

- Mit den neuen Befugnissen würden die Arbeitgeber zu Sonderermittlern werden, die – im Gegensatz zu den offiziellen Strafverfolgungsbehörden – jeglicher rechtsstaatlichen Kontrolle entzogen sind.

- Während die Zulässigkeit staatlicher Rasterfahndung vom Bundesverfassungsgericht zu Recht stark eingeschränkt wurde, hätte der Gesetzentwurf den Arbeitgebern die Durchführung von Rasterfahndungen ohne jeden Anfangsverdacht erlaubt.

- Vergebens sucht man jedoch im Gesetzentwurf bzw. im Änderungsantrag einen wirksamen Schutz vor erzwungenen Einwilligungen, insbesondere vor erzwungenen Einwilligungen in medizinische Untersuchungen bei Einstellungen und Versetzungen.

- Ein Klagerecht für Betriebs- und Personalräte bei Verstößen gegen den Beschäftigtendatenschutz fehlt, denn welcher Beschäftigte möchte schon gegen seinen Arbeitgeber klagen oder diesen auch nur bei der zuständigen Datenschutzaufsichtsbehörde anzeigen?

- Auch ein Mitbestimmungsrecht für Betriebs- und Personalräte bei der Bestellung des betrieblichen oder behördlichen Datenschutzbeauftragten fehlt, obwohl in der Praxis sich viele Datenschutzbeauftragte zu wenig um den Beschäftigtendatenschutz kümmern und auch nicht wenigen die erforderliche Fachkunde in diesem Bereich fehlt.

- Die geplante Ausweitung des Privilegs der Auftragsdatenverarbeitung von Staaten der EU und des Europäischen Wirtschaftsraumes (EWR) auch auf Staaten, für die die EU-Kommission ein „angemessenes Datenschutzniveau" festgestellt hat, würde dazu führen, dass faktisch die Kontrollrechte von Betriebs- und Personalrat sowie betrieblichen oder behördlichen Datenschutzbeauftragten ausgehebelt werden können. Während bisher nur bei Auftragsdatenverarbeitungen innerhalb der EU und des EWR die Weitergabe personenbezogener Daten an den Dienstleister nicht als Datenübermittlung zu sehen ist und daher auch nicht an besondere Bedingungen geknüpft wird, würde dies dann auch für Dienstleister in Länder wie Argentinien, Israel und Neuseeland gelten, bei denen eine Vorortkontrolle alleine schon wegen der Entfernung oder der Sicherheitslage kaum umsetzbar wäre.

- Die geplante Einführung des sogenannten Konzernprivilegs für Beschäftigtendaten würde es Arbeitgebern wesentlich erleichtern, Beschäftigtendaten zwischen rechtlich selbständigen Unternehmen hin und her zu übermitteln, ohne aber die Kontroll- und Schutzrechte entsprechend anzupassen.

- Statt normenklarer Regelungen sind viele schwammige Begriffe enthalten, die zu mehr Rechtsunsicherheit führen, statt – wie erforderlich – für Arbeitgeber, Beschäftigte sowie Betriebs- und Personalräte mehr Rechtssicherheit zu bringen.

Wie geht es weiter?

Wie kurz vor Redaktionsschluss aus gut unterrichteten Kreisen zu erfahren war, war für März 2013 ein Spitzengespräch zwischen dem CDU/CSU-Fraktionsvorsitzenden Volker Kauder, dem IG-Metall-Vorsitzendem Berthold Huber und dem DGB-Vorsitzenden Michael Sommer geplant. In diesem Gespräch sollte ein Kompromiss gefunden werden, um den Gesetzentwurf der Bundesregierung zum Beschäftigtendatenschutz doch noch in dieser Legislaturperiode verabschieden zu können. Nach dem dies öffentlich bekannt wurde, wollte niemand mehr etwas davon wissen. Vielmehr wurde der Gesetzentwurf für diese Legislaturperiode endgültig von der Agenda gestrichen.

Es ist dringend zu empfehlen, einen neuen Gesetzentwurf zum Beschäftigtendatenschutz unter Hinzuziehung von Expertinnen und Experten aus der Praxis und unter Beteiligung der Betroffenen (Beschäftigte, Betriebs- und Personalräte, betriebliche und behördliche Datenschutzbeauftragte) in Ruhe zu entwickeln und gründlich zu erörtern.

Der *Campact-Appell* für Beschäftigtendatenschutz war also erfolgreich! Wer ihn noch nicht kennt, kann ihn hier nachlesen: *https://www.campact.de/arbeitnehmerdatenschutz/appell/5-minuten-info/*.

Campact-Appell zum Gesetz zum Beschäftigtendatenschutz

Referenzen

[17(4)636] Drucksache des Innenausschusses „Änderungsantrag der CDU/CSU und FDP zu dem Gesetzentwurf der Bundesregierung ‚Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes'" (Drucksache17/4230) (http://beschds.files.wordpress.com/2013/01/17_4_636_aenda_cdu-csu_u_fdp-beschds.pdf)

[BeschDSSyn] Gesetzentwurf in der Fassung der Bundestagsdrucksache 17/4230 vom 15.12.2010 mit Änderungen durch die BT Drucksache 17(4)636 des Innenausschusses vom 10. Januar 2013 (http://extdsb.files.wordpress.com/2013/01/gesetzentwurf-beschc3a4ftigten-ds-synopse-2013-01-10.pdf)

[BT-Drs. 17/4230] Bundestagsdrucksache 17/4230 – Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes (http://dipbt.bundestag.de/dip21/btd/17/042/1704230.pdf)

[Düwell 2012] Professor Franz Josef Düwell, Vorsitzender Richter am Bundesarbeitsgericht a.D.: Beschäftigtendatenschutz im Fokus der Rechtsprechung des Bundesarbeitsgerichts und des Bundesverwaltungsgerichts – Der Auftrag des Gesetzgebers und der Beitrag der Gerichte, ISBN: 978-3-95546-020-4, Konstanz 2012

Anmerkungen

1 *vgl. http://beschds.wordpress.com*
2 *Pressemitteilung vom 29.01.2013, http://fiff.de/keine-ueberwachung-am-arbeitsplatz-erfolg-fuer-datenschuetzer*
3 *vgl. http://wp.me/p12h24-h3*
4 *siehe: http://wp.me/p12h24-jS und [BeschDSSyn]*
5 *https://www.campact.de/arbeitnehmerdatenschutz/*
6 *BVerfGE 65, 1*
7 *[Düwell 2012], S. 5*
8 *ebd.*
9 *vgl. hierzu [Düwell 2012]*
10 *Quelle: Koalitionsvereinbarung der CDU, CSU und FDP vom 26.10.2009 S. 106*
11 *vgl. http://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung08/Stellungnahmen_SV/*
12 *http://beschds.wordpress.com*

Datenschutz

The Brussels Privacy Declaration

Privacy is a fundamental human right, but today this right is widely ignored. We are outraged.

We are outraged, because

- we, the citizens, are now kept in hundreds of databases, mostly without our knowledge or consent,
- over 1,200 companies specialise in trading our personal data, mostly without our knowledge or consent,
- every time we browse the internet over 50 companies now monitor every click, mostly without our knowledge or consent,
- we are constantly being categorised and judged by algorithms and then treated according to the "perceived value" we may or may not bring to business without our knowledge and consent, and
- lobbying is currently replacing European citizens' voices and manifest concerns.

We call on the Members of the European Parliament and the governments of all European Member States to enhance and enforce our privacy rights.

We expect the new European rules on data protection to ensure:

- The protection of all personal information including identifiers of hard- and software
- Recognition that every European citizen has the right to effectively control his or her personal information
- Explicit, strong and informed consent for processing of our personal data
- No more coupling of service usage to personal data use (no more 'take-it or leave-it' online)
- Transparency of data processing and data sharing practices.
- 'True' data portability to promote competition and reduce "lock-in" and achieve information self-determination
- Strong protection against secretive profiling of citizens, both on- and offline
- Effective redress mechanisms and sanctions imposed on companies and government bodies that do not respect the law

The future of Europe needs privacy, and we need you to defend this fundamental right now.

Promotors: *Bits of Freedom, the Netherlands; Electronic Privacy and Information Center (EPIC), United States; European Digital Rights, Europe; Privacy International, United Kingdom*

Signatories: *Access, International; Consumer Federation of America, United States; Chaos Computer Club (CCC), Germany; Centre for Digital Democracy (CDD), United States; Open Rights Group, United Kingdom; Panoptykon Foundation, Poland; Vrijschrift, the Netherlands; Initiative für Netzfreiheit, Austria; La Quadrature du Net (LQDN), France; The Julia Group, Sweden; TagMeNot.info, Italy; Association for Technology and Internet, Romania; Abine, Inc., United States; VIBE!AT – Verein für Internet-Benutzer Österreichs, Austria; Privacy France, France; Digitalcourage e. V., Germany; International Modern Media Institute, Iceland; Burgerrechtenbeweging Vrijbit, the Netherlands; Datenschützraum e. V., Germany; Polish Free and Open Source Software Foundation, Poland; Alternative Informatics Association (Alternatif Bilişim Derneği), Turkey; Access to Information Programme Foundation, Bulgaria; unwatched.org, Austria; Chaostreff Salzburg, Austria; Stichting Privacy First, the Netherlands; Hermes Center for Transparency and Human Rights, Italy; datapanik.org, Belgium; German Working Group on Data Retention (AK Vorrat), Germany; Partners for Democratic Change, Serbia; AKVH (Arbeitskreis Vorratsdatenspeicherung OG Hannover), Germany; MOGiS e. V., Germany; Metamorphosis, Foundation for Internet and Society, Skopje, Macedonia; digitalrights.gr, Greece; Liga voor Mensenrechten, Belgium; FIfF e. V. (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung), Germany; Federation of German Consumer Organisations (vzbv), Germany; CRIDS (Centre de Recherche Information, Droit et Sociètè), Belgium;* **and more than 500 individuals.**

Monika Ermert

UN-Unterorganisation uneinig über die Zukunft der Telekommunikation

Konferenz ohne Folgen?

Der Hype um die World Conference on International Telecommunication (WCIT) *im vergangenen Dezember in Dubai war groß und noch dauern die Diskussionen darüber an, was das internationale Zerwürfnis über die Neufassung der* International Telecommunication Regulations (ITR) *bedeutet. 89 Staaten stimmten dem umstrittenen Neuentwurf für den einzigen internationalen Vertrag über Fragen der Telekommunikation zu. 55 lehnten zunächst ab – vor allem mit der Begründung, er öffne stärkerer staatlicher Kontrolle des Internet Tür und Tor. Anfang Februar lud das Bundeswirtschaftsministerium zu einer Nachbetrachtung, und im US-Kongress warnte zur gleichen Stunde der Chef der Federal Trade Commission, diejenigen, die das Internet unter multilaterale staatliche Kontrolle bekommen wollten, würden nicht aufgeben.*

Zusammen mit den USA, der EU und einer mehrheitlich aus Industrienationen bestehenden Gruppe hatte Deutschland der Neufassung der aus dem Jahr 1988 stammenden ITR (siehe Kasten zu den ITR 1988) im Dezember in Dubai seine Stimme verweigert. Ein derartiges Scheitern von Verhandlungen gab es in der Geschichte der für die ITR zuständigen *Internationalen Fernmeldeunion (ITU)* noch nie. Selbst während des kalten Krieges und anderen Zeiten extremer Polarisierung in der Politik, auf dem ITU-Parkett hatten die Staaten in Fragen wie der nach wie vor zentralen Frequenzpolitik stets Kompromisse gefunden – zur Absicherung der Kommunikation über Grenzen hinweg.

1988 hatten die Mitgliedstaaten der Internationalen Fernmeldeunion ***die ursprünglichen International Telecommunication Regulations (ITR)*** *unterzeichnet. Das war bei der World Administrative Telegraph and Telephone Conference (WATTC-88) in Melbourne. Die ITR regelten die Zusammenarbeit der Staaten im Bereich der internationalen Telefonie. Ein zentrales Kapitel legt fest, wie die Netzbetreiber internationale Telefongespräche abrechnen. Insbesondere für viele Entwicklungsländer bedeuteten die Ausgleichzahlungen eine erhebliche Einnahmequelle. Die hohen Minutenpreise für Anrufe ihrer Kunden aus dem Ausland schufen einen Anreiz für eine unausgewogene Bilanz, denn für die Landesbewohner waren die Auslandsgespräche zu teuer. Gleichzeitig rechneten die nationalen Anbieter hohe Terminierungsentgelte*[1] *(und viele Minuten) gegenüber den Netzbetreibern der ausländischen Anrufer ab. Mit der Liberalisierung vieler Telefonmärkte und dem Siegeszug des IP-Protokolls sind die Einnahmen aus den inter-carrier call accounting financial settlements nach und nach versiegt. Die deutsche Telekom etwa rechnet heute nur noch etwa fünf Prozent der Datenverkehre über die alten ITR-Regelungen ab, die FCC (Federal Communications Commission) sprach sogar von nur noch 2 Prozent für die USA. Hinter der Entscheidung der ITU-Mitgliedstaaten, die ITR nach fast drei Jahrzehnten zu novellieren, stand daher auch die Hoffnung mancher Staatsmonopolisten, sich etwas von den verlorenen Erlösen wiederzuholen. Aber auch Anpassungen an die veränderten Marktverhältnisse waren nötig, denn mit der vollständigen Migration zu IP-Netzen würden ansonsten die ITR komplett obsolet werden. Doch gerade die Ausweitung des alten Telefonievertrags auf das Internet sorgte am Ende für das Scheitern der Verhandlungen in Dubai.*

1 *Gebühren, die für die Zustellung eines Gesprächs aus einem fremden Netz berechnet werden*

„US, EU und deren Partner bedauern"

Dieses oft wiederholte Mantra von ITU-Generalsekretär *Hamadoun Touré* hat nach zwei Wochen zäher Verhandlungen in Dubai auch nichts mehr genützt. *Mit Bedauern* hatte US-Botschafter *Terry Kramer* spät in der Nacht vor dem letzten Verhandlungstag die Absage der USA an den Neuentwurf verkündet, rasch gefolgt von der britischen, kanadischen, australischen und weiteren Delegationen. Europa, das geschlossen auftreten wollte, folgte trotz der Bedenken einzelner Staaten dieser Linie.

Den Ausschlag für die Ablehnung in Dubai gab, wie FCC-Chef *Robert McDowell* Anfang Februar bekräftigte, dass das zugesagte, und in der ITU übliche Konsensprinzip verlassen wurde. Konferenzchef *Mohamed Al Ghanim* ließ mehrfach abstimmen. Inhaltlich sei es vor allem die Ausdehnung der ITR von der klassischen Telefonie auf das Internet gewesen, durch die die rote Linie für die USA überschritten worden sei.

Ein Dorn im Auge waren den US-Amerikanern die Erklärungen über die Bekämpfung von unerwünschter Massen-Email *(unsolicited bulk communication, Spam)* und zur *Netzwerksicherheit*, sowie eine nicht zum Vertrag gehörende Zusatzerklärung zur Arbeit der ITU im Bereich *Internet Governance:*

> *ARTICLE 5A*
> ***Security and robustness of networks***
> ***41B*** *Member States shall individually and collectively endeavour to ensure the security and robustness of international telecommunication networks in order to achieve effective use thereof and avoidance of technical harm thereto, as well as the harmonious development of international telecommunication services offered to the public.*
>
> *ARTICLE 5B*
> ***Unsolicited bulk electronic communications***
> ***41C*** *Member States should endeavour to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services.*

Solche allgemein formulierten Grundsätze blieben weit hinter dem zurück, was etwa Russland zu Beginn der Konferenz gefordert hatte. Im vielleicht umstrittensten Beitrag hatte die russische Regierung im Rahmen von Sicherheits- und Netzmanagementaspekten „nationale Abschnitte des Internet" vorgeschlagen.

*Die **neuen ITR** wurden nicht nur in Bezug auf veraltete Definitionen runderneuert – wobei die USA sich mit ihrer Forderung nach einer klaren Beschränkung der erfassten Unternehmen durchsetzten. Durch den Begriff* authorized operating agencies *anstelle von* operating agencies *sollten Internet-Anbieter von vornherein ausgeschlossen werden. Die ITR schaffen auch eine Reihe von ganz neuen Regelungen, insbesondere eine allgemeine Klausel zur Netzwerksicherheit, zu den internationalen Netzen und Netzdiensten, zur Abrechnung klassischer Telefongespräche, zur Telekommunikation in Katastrophenfällen, eine Extra-Klausel zu Spam und neue Abschnitte zur Nachhaltigkeit und E-Waste sowie eine Aufforderung zu Verbesserung des Zugangs von Behinderten zu den Netzen.*

Massive Kritik der westlichen Staaten gab es an einem in die Präambel aufgenommenen Zugangsrecht zur Telekommunikation für alle Staaten. Während die kubanische Delegation sich davon Unterstützung gegen durch Sanktionen der USA verursachte Einschränkungen bei der Internet-Nutzung erhoffte, kritisierten ihre Gegner, Grundrechte könnten jeweils nur Bürgern, nicht aber Staaten verliehen werden. Auch diese Formulierung sorgte für die Ablehnung der ITR durch die USA und deren Verbündete.

Die Abschnitte im einzelnen sind:

- *Purpose and scope of the Regulations*
- *Definitions*
- *International network*
- *International telecommunication services*
- *Safety of life and priority of telecommunications*
- *Security and robustness of networks*
- *Unsolicited bulk electronic communications*
- *Charging and accounting*
- *Suspension of services*
- *Dissemination of information*
- *Energy efficiency/e-waste*
- *Accessibility*
- *Special arrangements*
- *Final provisions*

Insgesamt haben die USA und ihre westlichen Partner zwar das Wort Internet aus dem gesamten Vertragstext herausverhandelt und eine Klausel erwirkt, die festhält, dass die ITR „keine inhaltsbezogenen Aspekte der Telekommunikation betreffen" (Purpose and Scope). Die USA und auch der Mehrzahl der Europäer hielten aber dennoch Spam- und Netzwerksicherheits-Bestimmungen für problematisch – und insbesondere für durch autoritäre Regime auslegbar im Sinne einer schärferen Netzkontrolle.

Von den zusätzlich zu den ITR verabschiedeten Entschließungen fanden insbesondere die „Maßnahmen für Entwicklungsländer, die vom Land eingeschlossen oder kleine Inselstaaten sind" sowie die Erkundung für eine global einheitliche Notrufnummer viel Zustimmung. Heftige Kritik hagelte es dagegen für die Entschließung zum Internet-Mandat der ITU. Zwar sind die Resolutionen nicht verbindlich, dennoch sorgte nicht zuletzt die Art und Weise, in der die Internet-Resolution durchgeboxt wurde, für Zerwürfnisse. Der WCIT-Vorsitzende Mohamed Al Ghanim erklärte die Resolution nach einer als erstes Meinungsbild getarnten Abstimmung kurzerhand für angenommen.

RESOLUTION PLEN/1 (DUBAI, 2012)
Special measures for landlocked developing countries and small island developing states for access to international optical fibre networks

RESOLUTION PLEN/2 (DUBAI, 2012)
Globally harmonized national number for access to emergency services

RESOLUTION PLEN/3 (DUBAI, 2012)
To foster an enabling environment for the greater growth of the Internet

RESOLUTION PLEN/4 (DUBAI, 2012)
Periodic review of the International Telecommunication Regulations

RESOLUTION PLEN/5 (DUBAI, 2012)
International telecommunication service traffic termination and exchange

Wie groß das Misstrauen zwischen den Blöcken ist, zeigte auch die skurrile Debatte über einen Verweis auf die Menschenrechtserklärung. Von Tunesien vorgeschlagen, wurde eine solche Referenz von westlichen Ländern zunächst kategorisch abgelehnt – sie könne die Tür zu nicht von den ITR abgedeckten Bereichen (Internet, Inhalte) öffnen. Doch wenige Tage später waren es EU-Mitglieder, die eine Referenz forderten. Sie mussten sich nun gegen die von Tunesien unterstützten Länder China und die arabischen Staaten verteidigen.

ITR – Einstieg in eine globale Internet-Kontrolle?

Trotz der Verhandlungserfolge der westlichen Allianz in Dubai wetterte McDowell in der Anhörung Anfang Februar, mit den neuen ITR habe der russische Präsident *Wladimir Putin* sein erklärtes Ziel einer „internationalen Kontrolle" über das Internet erreicht. Bei der WCIT sei endgültig der diplomatische Kompromiss eines selbst verwalteten Internet aufgekündigt worden.

McDowell hatte sich schon im Vorfeld der WCIT-Konferenz an die Spitze der US-Scharfmacher gegen die ITR-Verhandlungen gestellt und durch seine alarmistischen Kommentare beide Häuser des US-Kongresses und, eine Rarität, Demokraten und Republikaner hinter der Flagge für ein *freies Internet* versammelt. Eine Google-Kampagne und intensive Lobby-Arbeit der *Internet Society* sorgten für viel Kritik an WCIT und ITU, inzwischen auch für eine in den USA laufende Kampagne zur Abschaffung der ITU oder mindestens zu einer strikten Mandatsbegrenzung für die Organisation.

Noch am Vorabend des letzten Konferenztags war die vom federführenden Bundeswirtschaftsministerium angeführte deutsche Delegation praktisch bereit, die in Dubai ausgehandelten

Kompromisse mit zu tragen. Viele aus Sicht der Delegation kritischen Punkte waren herausverhandelt worden, darunter der Vorschlag, explizit Namen und Nummern in den ITR zu erwähnen, ITU-Standards über die ITR verbindlicher zu machen oder ganz allgemein den Anwendungsbereich des alten *Telefonievertrags* durch breite Formulierungen im Kapitel mit den Definitionen aufzubohren.

Auch unmittelbar vor der Konferenz heiß umstrittene Forderungen der *European Telekommunication and Network Operator Association (ETNO*, zu den Mitgliedern zählt die Deutsche Telekom) wurden in Dubai abgelehnt: Nach der Unterstützung von *Quality of Service*-Angeboten via ITR und zur Einführung eines Verursacherprinzips beim Internet-Datenverkehr (*Calling/Sending Party Pays)*. Und schließlich wurde per allgemeiner Klausel ausgeschlossen, dass sich die neuen ITR auf *Inhaltsfragen* beziehen.

„Wer regiert das Netz?" bleibt ein Zankapfel

Doch die Möglichkeit einer breiten Auslegung gerade beim Kampf gegen Spam und für Netzwerksicherheit bleibe, warnte der Völkerrechtler und deutsche *Internet-Governance*-Experte *Wolfgang Kleinwächter* nach dem Bonner Treffen zu den WCIT-Ergebnissen im Februar. Staatliche Regelungen zur Spam-Bekämpfung könnten bis hin zum Verbot der Zustellung unerwünschter Wahlwerbung reichen, hatten Delegierte westlicher Länder in Dubai gemahnt. Zwar können Regierungen bereits heute Inhalte im Netz ächten – und tun es mit wenigen Ausnahmen auch, man müsse dies aber nicht durch einen internationalen Vertrag legitimieren, so das Argument der ITR-Gegner.

Michael Rotert, Präsident des ECO, des Verbands der deutschen Internet-Wirtschaft, der den WCIT-Prozess als einer von ganz wenigen Wirtschaftsvertretern verfolgte, warnte überdies vor einer möglichen Vorratsspeicherung von Routing-Daten. Bei einer sehr breiten Auslegung hätte sich dies mit Bestimmungen im neu gefassten *Abrechnungskapitel* begründen lassen, fürchtet Rotert.

Kleinwächter sieht überdies den Wunsch einzelner ITU-Mitglieder, etwa Saudi Arabiens, alle Fragen zum Internet und dessen globaler Koordination und Kontrolle bei den Vereinten Nationen zusammenzufassen. Gerade arabische Länder wollen sich nicht mit aus ihrer Sicht obskuren Organisationen wie der für die Koordination des Domain-Managements verantwortlichen *Internet Corporation for Assigned Names and Numbers (ICANN)* herumschlagen.

Kleinwächter ist sicher, der Streit bleibt den Diplomaten erhalten und wird fortgesetzt beim *World Telecom Policy Forum (WTPF)* im Mai und, vor allem, der *Plenipotentiary* Konferenz der ITU in Korea 2014. Die Plenipotentiary Konferenz ist praktisch die verfassunggebende Versammlung der ITU, die alle vier Jahre über Arbeitsprogramm, Budget und Personalfragen entscheidet.

Je nachdem, welche Weichen die Plenipotentiary Konferenz für das künftige ITU-Mandat stellt, könne die Bundesregierung auch 2014 noch entscheiden, ob man die neuen ITR doch noch zeichnen will, hieß es aus Bonn. Ohnehin tritt der Vertrag nicht vor 2015 in Kraft, danach gelten in den Unterzeichnerstaaten die neuen ITR, während bei den Nicht-Unterzeichnern die alten ITR fortbestehen. Nach Ansicht eines Vertreters von *Verizon* gelten zwischen Alt- und Neu-ITR-Ländern die von beiden unterzeichneten Regeln von 1988. Eine große Rolle für die deutsche Haltung zu den ITR wird die Einstellung der anderen EU-Mitgliedstaaten spielen, von denen Schweden, UK und Tschechien erbitterte Gegner waren, Portugal und Griechenland dagegen eine Unterzeichnung sehr wohl erwogen haben.

Die Internet-Resolution (RESOLUTION PLEN/3, siehe unten) ist als Annex nicht Vertragsbestandteil und daher nicht völkerrechtlich bindend. Dennoch wird sie als Marschbefehl für die ITU in Richtung auf mehr staatlichen Einfluss im Netz gesehen.

RESOLUTION PLEN/3 (DUBAI, 2012)

To foster an enabling environment for the greater growth of the Internet

The World Conference on International Telecommu–nications (Dubai, 2012), recognizing

a) *the outcome documents of the Geneva (2003) and Tunis (2005) phases of the World Summit on the Information Society (WSIS);*

b) *that the Internet is a central element of the infrastructure of the information society, which has evolved from a research and academic facility into a global facility available to the public;*

c) *the importance of broadband capacity to facilitate the delivery of a broader range of services and applications, promote investment and provide Internet access at affordable prices to both existing and new users;*

Monika Ermert

Monika Ermert arbeitet seit 1993 als freie Journalistin für verschiedene Tages- und Wochenzeitungen, und ist regelmäßige Autorin für Fachzeitschriften wie die c't (insbesondere heise online) und Intellectual Property Watch. Monika Ermert lebt mit ihrem Lebensgefährten und zweieinhalb Kindern in München.

d) *the valuable contribution of all stakeholder groups in their respective roles, as recognized in § 35 of the Tunis Agenda for the Information Society, to the evolution, functioning and development of the Internet;*

e) *that, as stated in the WSIS outcomes, all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the existing Internet and its future development and of the future internet, and that the need for development of public policy by governments in consultation with all stakeholders is also recognized;*

f) *Resolutions 101, 102 and 133 (Rev. Guadalajara, 2010) of the Plenipotentiary Conference,* resolves to invite Member States

1 *to elaborate on their respective positions on international Internet-related technical, development and public-policy issues within the mandate of ITU at various ITU forums including, inter alia, the World Telecommunication/ICT Policy Forum, the Broadband Commission for Digital Development and ITU study groups;*

2 *to engage with all their stakeholders in this regard,* instructs the Secretary-General

1 *to continue to take the necessary steps for ITU to play an active and constructive role in the development of broadband and the multistakeholder model of the Internet as expressed in § 35 of the Tunis Agenda;*

2 *to support the participation of Member States and all other stakeholders, as applicable, in the activities of ITU in this regard.*

Ein bißchen Multi-Stakeholder

Die Experten von ISOC und FCC rieten mit Blick auf die nächsten Schritte vor allem zu mehr Unterstützung und Werbung für das, was in der internationalen Netzpolitik als *Multi-Stakeholder*-Ansatz Karriere gemacht hat, mit wahlweise der ICANN oder dem *UN Internet Governance Forum (IGF)* als prominent zitierten Beispielen. In ihrer Erklärung zur Informationsgesellschaft beim UN-Weltgipfel in Tunis 2006 hat die Staatengemeinschaft die Regelung internationaler Netzfragen durch alle Interessengruppen aus allen Ländern im Grundsatz bejaht. Praktisch hat sich die US-Regierung des Konzepts nicht zuletzt dafür bedient, den Zugriff von Regierungen auf das ursprünglich komplett von den USA dirigierte *Domain Name System* zu begrenzen – die US-Regierung kontrolliert nach wie vor die zentrale *Rootzone*.

Doch der Multi-Stakeholder-Begriff hat durchaus Spuren hinterlassen, auch die WCIT-Konferenz zeigte das. Auf Druck von Öffentlichkeit, Unternehmenskampagnen, aber auch einer Reihe demokratischer Regierungen konnten Nicht-Regierungsteilnehmer als Sektormitglieder oder als Teil von Regierungsdelegationen teilnehmen. Wesentliche Sitzungen wurden ins Web übertragen – ein Novum. ITU-Generalsekretär Touré traf sich mit zivilgesellschaftlichen Gruppen vor Ort und tägliche Pressekonferenzen sollten für zusätzliche Transparenz sorgen. Vorab hatte man sogar in einer ersten weltweit abgehaltenen Online-Konsultation wenigstens die Kernvorschläge der neuen ITR zur Diskussion gestellt – mit freilich mäßigem Erfolg. Dass das Gros der Verhandlungsdokumente aber nur durch *Leaks* bekannt wurde und Nicht-Regierungsvertreter praktisch kein Rederecht haben, sichert der ITU allerdings nach wie vor den Vorwurf, eben nicht wirklich transparent und partizipationsbereit zu sein.

Auch in Deutschland lernt man noch, was der Begriff Multi-Stakeholder bedeutet. Zwar lud das BMWi vor und nach der WCIT zu kurzen Konsultationstreffen, Einladungen dazu ergingen aber nur an ausgewählte Unternehmen, Verbände und Organisationen, die Presse wurde nicht zugelassen. Von den 40 Teilnehmern beim Februar-Treffen kamen über 30 aus Ministerien, dem Parlament oder der Wirtschaft. Auf dem zivilgesellschaftlichen Auge ist man auch hierzulande noch beinahe blind – und könnte angesichts der bevorstehenden Debatten zur Netzkontrolle weltweit Unterstützung brauchen.

Björn Schembera

You are here – Privatsphäre der Positionsinformation

Es ist der 19. Februar 2011. Tausende machen von ihrem Grundrecht auf Versammlungsfreiheit Gebrauch und demonstrieren gegen einen jährlich stattfindenden Naziaufmarsch in Dresden. Weil ausgehend von den Gegenaktivisten Straftaten vermutet werden, führt die Polizei eine großangelegte Funkzellenauswertung durch, wodurch tausende sich in der Südstadt aufhaltende Personen unter Generalverdacht gestellt werden.

Dieses Beispiel zeigt, wie sensibel Positionsinformationen sind. Aus dem momentanen Aufenthaltsort lassen sich Rückschlüsse ziehen über das Sozialverhalten, persönliche Interessen und viele weitere Eigenschaften einer Person, wie z. B. deren politische Gesinnung. Diese Aspekte werden klassischerweise zur schützenswerten Privatsphäre gezählt. Ein zeitgemäßes Verständnis der Privatsphäre muss deshalb auch das Recht von Individuen, Gruppen oder Institutionen einschließen, „selbst bestimmen zu können, wann, wie und in welchem Ausmaß Information über ihre Position an andere weitergegeben wird."[1]

Mit der Verbreitung von Smartphones ist heutzutage die Nutzung von Positionsinformationen fast schon zur Selbstverständlichkeit geworden: Wir teilen unsere Position über Dienste wie *Google Latitude* Freunden mit, Schüler kommunizieren zunehmend über *Facebook* und versehen Neuigkeiten, Bilder oder

Parties mit einer Positionsangabe, die in den sozialen Netzwerken erscheint.

Smartphones spielen dabei eine zentrale Rolle. In technischer Hinsicht stellen sie eine Erweiterung des klassischen Mobiltelefons dar, wobei sie es um mehrere Sensoren ergänzen, eine hochauflösende Kamera besitzen und auf mobilen Internet-Zugang ausgelegt sind. Hierfür ist natürlich eine wesentlich höhere Rechenleistung nötig. Durch den heute standardmäßig in Smartphones verbauten GPS-Sensor ist es möglich, jederzeit die eigene Position zu bestimmen. In Zusammenspiel mit dem Internet-Zugang, der heute meistens über Flatrates angeboten wird, führt dies zu standortbezogenen Diensten (*Location-based Services,* LBS), worunter Dienste verstanden werden, auf die von mobilen Geräten über ein mobiles Netzwerk zugegriffen wird und die von der Fähigkeit Gebrauch machen, die Position dieser Geräte zu bestimmen.[2]

Ein LBS benötigt ein Smartphone, ein Positionierungssystem, sowie einen *Location Server* (LS), um eine ortsbezogene Anwedung anbieten zu können, wie z. B. einen POI *(Point of Interest)*-Finder. Der LS verwaltet die Positionsdaten der mobilen Geräte und hat Informationen zumindest über den momentanen Aufenthaltsort, evtl. aber sogar über Bewegungsprofile des Nutzers.

Dobson und Fisher zeichnen bereits 2003 eine düstere Vision und nennen diese *Geoslavery*.[3] Eingebettet in ein Herr-Knecht-Modell besitzt der Überwacher Kontrolle über die Positionsinformation, d.h. Zeitpunkt, Position, Geschwindigkeit und Richtung eines oder mehrerer Überwachter. Die Technologie sei verfügbar, einige auf Freiwilligkeit basierende Produkte schon auf dem Markt.

Das oben genannte Beispiel mit *Google Latitude* ist insofern problematisch, da über ein spezielles Konto, den Google-Account, die Positionsinformation mit anderen Informationen verknüpft wird. An dieses Konto sind auch noch andere Dienste (E-Mail, Suchmaschinenergebnisse, Kalender, ...) angebunden. So kann einem Nutzer beispielsweise positionsbezogene Werbung eingeblendet werden, wenn aus seinem E-Mailkonto oder seinem Suchverhalten hervorgeht, dass er sich für ein gewisses Produkt interessiert.

Aufgrund der Komplexität von mobilen Anwendungen oder deren Nutzungsbedingungen kann dies im Hintergrund ohne explizite Einwilligung des Nutzers passieren. Zwar ist das gemäß §98 des Telekommunikationsgesetzes als Teil der informationellen Selbstbestimmung untersagt, kam jedoch in der Vergangenheit durchaus schon vor. So wurde 2011 bekannt, dass alle Apple-Produkte auf der iOS-Plattform lokal im Gerät die Positionsdaten speicherten.[4] Zu einem weiterern Vorfall bei Apple kam es im Februar 2012, bei dem Anwendungen ungefragt auf die Adressdaten zugriffen.[5]

Es handelt sich also bei jedem Teil eines LBS, vom mobilen Gerät über den Location Server bis zum Service um einen kritischen Punkt bezüglich der Privatsphäre. Die technischen Aspekte sollen nun beleuchtet werden, um im Folgenden einige Gegenmaßnahmen vorzustellen.

Mobiles Objekt (MO)

Das *Mobile Objekt*, sei es nun Smartphone oder Tablet, ist ein kritischer Punkt im System, weil es den Nutzer als digitaler Helfer ständig begleitet. Der Nutzer muss bewusste Kontrolle über Hard- und Software ausüben können, was insbesondere die Kontrolle über die Sensoren, die Kamera und die Internet-Verbindung umfasst.

Hier liegt die Problematik vor allem im Betriebssystem, das meist ein proprietäres ist. So sind die verbreitetsten Systeme *Symbian*, *iOS*, *Blackberry OS* und *Windows Mobile* allesamt Closed Source und den Herstellern muss vertraut werden – dass sie nicht immer als integer eingestuft werden können, zeigen die o.g. Beispiele von Apple.

Googles Betriebssystementwicklung für mobile Endgeräte, genannt *Android*, geht einen anderen Weg: Zwar ist das Betriebssystem Open Source, wirklich nutzen lässt sich dieses System jedoch nur mit einem Google-Account, was wieder die oben genannte Verknüpfung von personenbezogenen Daten auf verschiedenen Ebenen zur Folge haben kann. Ebenso lassen sich die Anwendungen oft nur über die hauseigene Vertriebsplattform *Google Play* herunterladen, wozu wiederum ein Google-Account Vorraussetzung ist.

Die Kampagne *Free your Android*, die vom FoeBud (heute digitalcourage) und FSF[6] initiiert wurde, gibt eine Hilfestellung, wie man das eigentlich freie Betriebssystem Android von Google *befreit*. Konkret wird die Nutzung von *CyanogenMod* empfohlen[7], einem Android-Abkömmling, der komplett ohne Google-Anwendungen auskommt und auf den meisten Android-Mobiltelefonen läuft. Zur Installation ist das *Rooten* des Geräts notwendig, wodurch die Garantie erlischt.

Eine weitere Entwicklung in Richtung freier Software auf mobilen Geräten machen die Ubuntu-Entwickler mit *Ubuntu for Phones*, welches auf der CES im Januar 2013 als Prototyp vorgestellt wurde. Das Projekt steht jedoch noch im Aufbau, lauffähige Versionen werden nicht vor 2014 erwartet und es ist

Björn Schembera

Björn Schembera ist Diplom-Informatiker und lebt in Stuttgart.

noch ungewiss, in welche Richtung sich das Projekt entwickeln wird.[8]

Location Server (LS)

Der *Location Server* verwaltet die Positionen aller auf ihm angemeldeten Benutzer. Dies macht ihn zu einem sensiblen Punkt, da dort die Informationen mehrerer Nutzer verfügbar sind. Neben den reinen Orts- und Zeitinformationen könnten hier auch Daten zwischen mehreren Nutzern korreliert werden.

Zwar beteuert beispielsweise Google für seinen Dienst *Latitude*, dass die Bewegungsprofile nicht gespeichert werden, aber es lässt sich auch eine Kompromittierung des Dienstes denken, oder ein Arbeitgeber, der Dienst-Handys an seine Belegschaft ausgibt und sie ohne ihr Wissen verfolgen lässt. Zur Absicherung des *Location Server* gibt es einige Konzepte, die hier in Kürze vorgestellt werden sollen:[9]

Eine grundsätzliche Absicherung des *Location Server* kann durch Zugriffskontrolle erfolgen, die aus anderen Bereichen wohlbekannt ist und wozu eine Zugriffsliste geführt wird, die besagt, welche Person welche Aktion auf den Positionsinformationen durchführen darf. Hierbei ist problematisch, dass die Kontrolle der Zugriffsliste sich nicht in der Hand des eigentlichen Nutzers befindet. Darüber hinaus können die Positionsinformationen verschlüsselt auf dem LS abgelegt werden, was jedoch dazu führt, dass räumliche Anfragen über mehrere Objekte unmöglich werden.

Ein anderes Verfahren ist *k-Anonymity,* wonach die eigene Position von der Position k–1 anderer Nutzer des LBS ununterscheidbar werden soll – eine Person wird durch eine Gruppe anonymisiert, wobei die Schwierigkeit darin liegt, eine Gruppierung zu finden, die ausreichend Sicherheit bietet. Des Weiteren lässt sich die exakte Position künstlich unscharf bzw. ungenau machen. Die Position entspricht dann einer Aufenthaltswahrscheinlichkeit innerhalb eines gewissen Radius. Mittels Kooradinatentransformation ließe sich die echte Position in ein anderes Koordinatensystem übertragen und so die Privatsphäre erhöhen.

Beide Ansätze lassen sich kombinieren zu einer Verteilung der Positionsinformationen auf mehrere unabhängige *Location Server.* Jeder Server beherbergt dann nur einen Teil der Informationen, was eine gewisse Sicherheit bei nicht vertrauenswürdigen *Location Servern* bringt.

Außer der Zugriffskontrolle existieren alle Konzepte nur prototypisch. Bis sie als Produkt zur Verfügung stehen, wird einige Zeit vergehen, außerdem muss dies gewollt sein sowohl von den Herstellerinnen und Herstellern als auch den Nutzerinnen und Nutzern.

Location-based Service (LBS)

Natürlich muss der Service selbst, der die auf dem LS abgelegten Positionsinformationen bezieht und verarbeitet, vertrauenswürdig sein. Er bekommt Zugriff auf alle von Nutzerin oder Nutzer zu Verfügung gestellten Daten.

Diesem Dienst muss ein grundsätzliches Vertrauen entgegengebracht werden, da er alle vom Nutzer autorisierten Daten verarbeitet. Die beste Möglichkeit, sich hier gegen Missbrauch zu schützen, ist die Nutzung von Freier Software. Nur wenn der Quellcode offen liegt, kann der Nutzer oder die Community nachvollziehen, was wirklich geschieht. Da die LBS jedoch meist auf entfernten Servern arbeiten, ist eine Kontrolle hier oft nicht möglich.

Grundsätzlich müssen LBS kritisch betrachtet werden, da diese mit den Positionsdaten von Individuen arbeiten und jene somit potenziell in deren Besitz sind. Für das mobile Objekt und den Location Server gibt es Konzepte, diese Teile abzusichern – so gibt es mittlerweile für Smartphones die Betriebssystem-Alternative CyanogenMod. Der kritische Punkt ist meist der LBS selbst, da dieser auf einer eigenen Infrastruktur die Positionsdaten verarbeitet und das Ergebnis dann an den anfragenden Nutzer schickt.

Neben den technischen Konzpten müssen auch die gesellschaftlichen Implikationen näher betrachtet werden. Zielführend kann es nicht sein, standortbezogene Dienste grundsätzlich abzulehnen – wichtig ist der kritische Umgang damit. Auf Firmen und deren Versprechungen in punkto Datensicherheit ist nur selten Verlass, wie viele Beispiele zeigen.

Ebenso wichtig ist es, dass wir wieder die bewusste Kontrolle über unser Handeln erlangen, worunter ich auch die bewusste Kontrolle von Geräten verstehe, die uns im Alltag zur Seite stehen sollen. Dafür muss bei einer großen Mehrheit jedoch erst ein Problembewusstsein geschaffen werden. Ebenso muss dieses Problembewusstsein auch im Bereich der Wissenschaft und der Industrie durchgesetzt werden. Technik ist per se weder gut noch schlecht, es kommt auf deren konkrete Nutzung an – wir müssen klare Trennlinien ziehen zwischen der Anwendung von Technik, die dem Menschen nützt, und Technik, die nur der Profitmaximierung oder anderen Partikularinteressen verpflichtet ist.

Um wieder auf das eingangs genannte Beispiel mit der Demonstration zu kommen: Dass man Technik auch meistens in der umgekehrten Richtung nutzen kann, zeigt sich exemplarisch an *Sukey*.[10] Dieses im Rahmen der britischen Studentenbewegung 2011 entwickelte Tool soll Demonstrantinnen und Demonstranten helfen, sich (meist illegalen) Polizeikesseln, die deren Bewegungsfreiheit einschränken, zu entziehen.[11] Dazu nutzt die App neben manuell eingegebenen textuellen Daten auch die vom GPS-Sensor gelieferten Daten, um eine interaktive Karte zu erstellen, wo gerade ein Polizeikessel entstehen könnte. Hier zeigt sich exemplarisch die produktive Nutzbarmachung einer Technologie.

Anmerkungen

1 *M. Duckham, L. Kulik. Location privacy and location-aware computing. In J. Drummond, R. Billen, D. Forrest, E. Joao, editors, Dynamic & Mobile GIS: Investigating Change in Space and Time, chapter 3, pp. 34–51. CRC Press, Boca Raton, FL, 2006.*

2 *K. Virrantaus, H. Tirri, J. Veijalainen, J. Markkula, A. Katanosov, A. Garmash, V. Terziyan. Developing GIS-Supported Location-Based Ser-*

vices. In Proc. of WGIS 2001, volume 2, p. 66. IEEE Computer Society, 2001.

3 *J. E. Dobson, P. F. Fisher. Geoslavery. Technology and Society Magazine, IEEE, 22(1):47–52, 2003.*

4 *http://www.heise.de/tp/artikel/34/34601/1.html , Zugriff 31.1.2013*

5 *http://www.guardian.co.uk/technology/2012/feb/15/apple-iphone-address-book-privacy , Zugriff 31.1.2013*

6 *http://fsfe.org/campaigns/android/android.html , Zugriff 31.1.2013*

7 *http://www.cyanogenmod.org/, Zugriff 31.1.2013*

8 *O. Diedrich, J. Wirtgen. Smartphone-Underdogs. C't 4/13, S. 17, 2013*

9 *M. Duckham, L. Kulik., a.a.O.*

10 *http://www.opensukey.org , Zugriff 31.1.2013*

11 *http://www.heise.de/tp/blogs/6/149205, Zugriff 31.1.2013*

Stefan Hügel

Log 1/2013

Ereignisse, Störungen und Probleme der digitalen Gesellschaft

Immer wieder gibt es Ereignisse, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau von Bürgerrechten stehen. Wir dokumentieren hier einige davon. Die Aufzählung ist sicherlich nicht vollständig; mit einigen besonders bedeutsamen Ereignissen wollen wir aber auf die weiterhin besorgniserregende Entwicklung hinweisen.

November 2012

4. November 2012: Google löscht acht rechtswidrige Suchergebnisse, die auf das angebliche Vorleben von Bettina Wulff verweisen. Drei der Ergebnisse stammen von der umstrittenen christlichen Seite kreuz.net. Die Anwälte von Bettina Wulff hatten die Löschung von 3000 Einträgen aus dem Google-Suchindex und zusätzlich 80 Begriffen aus der automatischen Vervollständigung von Suchanfragen gefordert (Quellen: Spiegel, Heise).

5. November 2012: Die Federal Trade Commission der USA kritisiert die fehlende Möglichkeit des *Do Not Track* für Verbraucher und erhöht damit den Druck auf den W3C-Standardisierungprozess. Sie befürworte zwar grundsätzlich Selbstregulierung, denke aber angesichts des mangelnden Fortschritts über gesetzliche Regelungen nach (Quellen: Politico, Heise).

5. November 2012: Einem Bericht zufolge hat Skype Nutzerdaten an das private Sicherheitsunternehmen *iSight Partners* weitergegeben. Es handelt sich um Daten eines Niederländers, der 2010 im Alter von 16 Jahren an DDoS-Attacken der *Operation Payback* mitgewirkt haben soll. Kurz darauf wurde der Mann festgenommen. iSight Partners wurde danach von der Firma Paypal beauftragt, die ebenfalls Ziel der damaligen Attacken in Folge der Einstellung des Geschäftsverkehrs mit Wikileaks waren (Quellen: nu.nl, Heise).

6. November 2012: Vor dem Bundesverfassungsgericht in Karlsruhe beginnt die Verhandlung über eine Verfassungsbeschwerde gegen die Antiterrordatei, in der Informationen zu Terrorverdächtigen und ihrem Umfeld zentral zusammengeführt werden. Die Datei verletze nach Ansicht des Beschwerdeführers, eines pensionierten Richters, eine Reihe von Grundrechten, darunter das Grundrecht auf informationelle Selbstbestimmung. Ferdinand Kirchhof, Vizepräsident des Bundesverfassungsgerichts sieht bei der Antiterrordatei „verfassungsrechtliche Probleme". Bundesdatenschutzbeauftragter Peter Schaar sieht bei der Datei „erhebliche Kontrolldefizite" und verweist auf die verfassungrechtlich gebotene Trennung von Polizei und Nachrichtendiensten (Quellen: Bundesverfassungsgericht, Heise).

9. November 2012: Forschungsprojekte, an denen auch das Bundeskriminalamt (BKA) und die Bundespolizei beteiligt sind, haben das Ziel, mit Hilfe von multimodalen biometrischen Gesichtserkennungssystemen auf Basis von 3D-Bildern Personen aus Foto- und Videodateien zu identifizieren. Dies geht aus der Antwort auf eine kleine Anfrage des Bundestagsabgeordneten Andrej Hunko (Die LINKE) hervor. Gleichzeitig ist das Deutsche Forschungszentrum für künstliche Intelligenz (DFKI) in Saarbrücken am EU-Projekt *iCOP (Identifying and Catching Originators in P2P Networks)* beteiligt (Quellen: Andrej Hunko MdB, Heise).

9. November 2012: Der Teilnehmer der Demonstration *Freiheit statt Angst*, der 2009 von Polizeibeamten zusammengeschlagen wurde, erhält ein Schmerzensgeld von € 10.000. Aus Sicht des Anwalts des Opfers sei die Entschädigung im Vergleich zu ähnlich gelagerten Fällen ungewöhnlich hoch, aus Opfersicht aber eher bescheiden. Die verantwortlichen Beamten wurden bereits zuvor in einem Strafverfahren zu je 120 Tagessätzen verurteilt (Quellen: taz, Heise).

9. November 2012: Nach Ansicht des Leiters der deutschen Niederlassung des Überwachungstechnik-Spezialisten und Herstellers der Software *FinFisher, Gamma International,* rette dessen Software Leben und helfe dabei, Kriminelle zu fassen. Er nannte aber keine konkreten Beispiele. Gamma liefere keine Software an Diktaturen und sei auch nicht für die Überwachung in Ägypten und Bahrain verantwortlich. Im ersten Fall sei ein geplantes Geschäft nicht zustande gekommen, im zweiten Fall sei eine gehackte Demoversion verwendet worden (Quelle: Heise).

12. November 2012: Verantwortlichen des Projekts *INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment)* zufolge ziele das Projekt nicht auf eine Unterwanderung des Datenschutzes sondern vielmehr auf dessen Stärkung. Es würden auch Werkzeuge zum Schutz sensibler Daten vor Missbrauch entwickelt. Sicherheitsbehörden dürften aber persönliche Daten Verdächtiger und Krimineller ohne Wissen oder Einwilligung zur Strafverfolgung oder zur Gefahrenabwehr nutzen (Quellen: Andrej Hunko MdB, Heise).

13. November 2012: Bundeswirtschaftsminster Rösler kritisiert auf dem 7. IT-Gipfel in Essen das geplante Cyber-Sicherheitsgesetz und die damit verbundene Meldepflicht im Fall von IT-Angriffen. Er setze auf freiwillige Selbstverpflichtungen der TK-Branche und sehe Diskussionsbedarf angesichts der Gefahr für die Wettbewerbsfähigkeit der deutschen Wirtschaft (Quelle: Heise).

14. November 2012: Der Zugang zum Internet ist nach der Feststellung des britischen Berufungsgerichts ein Menschenrecht. Es sei „heutzutage unvernünftig, jemanden zu verbieten, von zu Hause aus auf das Internet zuzugreifen". Ein 55jähriger Mann war verurteilt worden, weil er mit einer versteckten Handykamera eine 14jährige beim Duschen fotografiert hatte. Unter anderem wurde ihm lebenslänglich der Besitz eines Computers verboten. Dagegen legte er erfolgreich Berufung ein, da er dadurch von der Welt abgeschnitten werde. Von dem Urteil werden weitgehende Folgen für die Praxis der Internet-Verbote erwartet (Quellen: Guardian, Heise).

14. November 2012: Immer häufiger wird Google von Staaten zur Herausgabe von Nutzerdaten aufgefordert. Im ersten Halbjahr 2012 gab es 21.000 entsprechende Verfügungen; im gleichen Zeitraum des Vorjahrs waren es noch 16.000 Verfügungen gewesen. Deutschland steht dabei mit 1546 Verfügungen auf Platz 5; an der Spitze stehen die USA mit 7969 Verfügungen, gefolgt von Indien, Brasilien und Frankreich (Quellen: Google-Transparenzbericht, Heise).

14. November 2012: Die Leitlinien zur Videoüberwachung von 2010 werden von einer Reihe von Einrichtungen und Organen der EU nicht hinreichend beachtet. Das hat der Datenschutzbeauftragte der EU, Peter Hustinx, bei einer Kontrolle festgestellt. Nur eine der kontrollierten Institutionen kläre mit allen erforderlichen Informationen über die Videoüberwachung auf; bei den Anderen gäbe es „noch bedeutenden Spielraum für Verbesserungen" (Quellen: Europäischer Datenschutzbeauftragter, Heise).

15. November 2012: Nach Plädoyers des Justizministers von Hessen, Jörg-Uwe Hahn (FDP), und des Justizsenators von Berlin, Thomas Heilmann (CDU), wollen die Justizminister der Länder die Möglichkeit der Fahndung über Facebook prüfen, so ein einstimmiger Beschluss auf dem Treffen der Justizministerkonferenz in Berlin (Quelle: Heise).

18. November 2012: Bei mehr als der Hälfte – 29 von 52 – untersuchter Web-Seiten für Kinder hat der VZBV (Verbraucherzentrale Bundesverband) Unterlassungsverfahren eingeleitet. Werbung und redaktionelle Inhalte würden nicht klar genug getrennt, Besucher mit Spielen auf Unternehmensseiten umgeleitet und Handy-Nummern abgefragt, um ihnen kostenpflichtige Abonnements zu verkaufen (Quellen: Spiegel, Heise).

24. November 2012: Am Flughafen Frankfurt am Main werden ab sofort im regulären Betrieb Nackt-Scanner des Unternehmens L3 Communications eingesetzt. Die Nutzung sei entsprechend der Vorgaben der EU freiwillig, gesundheitliche Auswirkungen seien nicht zu befürchten. Bundesdatenschutzbeauftragter Peter Schaar wies darauf hin, „dass weder Körperkonturen noch Geschlechtsmerkmale, künstliche Körperteile oder medizinische Hilfsmittel angezeigt werden" dürften (Quelle: Heise).

27. November 2012: In New York werden bei der Parade zu Thanksgiving Konfetti verstreut, die aus zerkleinerten polizeilichen Dokumenten hergestellt worden sind. Sozialversicherungsnummern, Namen von Polizisten und Details einer Eskorte für Präsidentschaftskandidat Mitt Romney waren darauf noch erkennbar. Wie die Dokumente unter das Konfetti geraten konnten, wird untersucht (Quelle: Heise).

27. November 2012: Die geplante Neuregelung der Auskunft über Bestandsdaten von IT-Anschlussinhabern ist nach Ansicht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein erneut verfassungwidrig. Der Entwurf unterscheide nicht ausreichend zwischen der Herausgabe von Bestandsdaten und von IP-Adressen und Sicherheitsmerkmalen. Dies verletze die Grundrechte auf informationelle Selbstbestimmung und auf Wahrung des Telekommunikationsgeheimnisses (Quelle: Heise).

29. November 2012: Hersteller von Spionage-Software unterhalten Recherchen des Guardian und des *ICIJ (Internationales Konsortium für investigativen Journalismus)* zufolge Briefkastenfirmen, beispielsweise auf den Britischen Jungferninseln. Beteiligt sei auch die Gamma Group International, Hersteller der Spionagesoftware FinFisher, mit der Firma *Bizcorp Management Ltd.* in Singapur. Über den Zweck dieser Firma lehnte ein Sprecher die Auskunft ab. Ob die Briefkastenfirmen von Gamma auch eingesetzt wurden, um FinFisher an Bahrain oder Ägypten zur Zeit des Mubarak-Regimes zu verkaufen, ist unklar (Quellen: Guardian, Heise).

Dezember 2012

1. Dezember 2012: Vor dem Hintergrund von Ermittlungen bei der Suche nach einer undichten Stelle bei der Polizei durchsuchen Staatsanwaltschaft und Polizei Wohnung und Redaktion eines Journalisten der Berliner Morgenpost. Er wird verdächtigt, einen Beamten des LKA bestochen zu haben. Der Journalistenverband *DJU (Deutsche Journalistinnen- und Journalisten-Union)* bezeichnet die Durchsuchung als „vollkommen unverhältnismäßig und offenbar rechtswidrig" (Quellen: Deutsche Journalistinnen- und Journalisten-Union, Heise).

Stefan Hügel

Stefan Hügel ist Vorsitzender des FIfF, arbeitet als IT-Berater und lebt in Frankfurt am Main.

3. Dezember 2012: Ein Gesetzentwurf zur Novellierung des Polizeigesetzes – „Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung" – wird im Landtag von Sachsen-Anhalt behandelt. Der Entwurf sieht eine deutliche Verschärfung vor, so legt beispielsweise § 33 (1) fest: „Die Polizei kann von jedem Diensteanbieter (§ 3 Nr. 6 des Telekommunikationsgesetzes) verlangen, Kommunikationsverbindungen zu unterbrechen oder zu verhindern …"; eine richterliche Bestätigung muss erst danach „unverzüglich" eingeholt werden. Später wird das Gesetz aufgrund heftiger Kritik überarbeitet, die grundsätzlichen Ziele sollen aber beibehalten werden (Quellen: Landtag von Sachsen-Anhalt, Heise).

5. Dezember 2012: Ein internationaler Zusammenschluss von Bürgerrechtsinitiativen, darunter *EDRi (European Digital Rights)*, die niederländische Bürgerrechtsorganisation *Bits of Freedom*, der *Chaos Computer Club*, *Digitalcourage* und die *Digitale Gesellschaft* wendet sich gegen Vorstellungen des niederländischen Justizministers Ivo Opstelten, einen niederländischen Staatstrojaner auch außerhalb der Landesgrenzen einzusetzen. Pläne für einen solchen Staatstrojaner werden im Parlament in Den Haag beraten. Das Bündnis warnt vor ernsten Gefahren für Menschenrechte und IT-Sicherheit weltweit (Quellen: Bits of Freedom, Heise).

10. Dezember 2012: Facebook lässt über neue Regelungen abstimmen, die unter anderem vorsehen, eben diese Abstimmungen abzuschaffen. Da das für eine bindende Abstimmung erforderliche Quorum von 30 % bei weitem nicht erreicht wird, wird dies damit die letzte Abstimmung bei Facebook sein. Bei der vorigen Abstimmung hatten sich ebenfalls nur 0,04 % der Nutzer beteiligt (Quelle: Heise).

12. Dezember 2012: Das Unternehmen *LeadLander* bietet Dienste an, die die Identifizierung von Besuchern von Web-Seiten über deren soziale Netze erlaubt. Offenbar werden die Besucher durch den Abgleich von sozialen Netzen und Geodaten ermittelt. Auf diese Weise werden beispielsweise Namen und E-Mail-Adressen ermittelt, um gezielt Werbung zuzusenden. Neben LeadLander bieten inzwischen auch weitere Unternehmen solche Dienstleistungen an. Thilo Weichert, Datenschutzbeauftragter in Schleswig-Holstein, weist darauf hin, dass Werbe-E-Mails, die nach dem gezielten Ausspähen persönlicher Daten über Web-Seiten versendet werden, in Deutschland rechtswidrig sind (Quelle: Heise).

12. Dezember 2012: Einem Bericht der Süddeutschen Zeitung zufolge sollen im Bundesgesundheitsministerium jahrelang sensible Daten gestohlen worden sein – unter anderem E-Mails der Minister Philipp Rösler und Daniel Bahr. Offenbar wurden diese Daten – Beschlüsse, Gesetzentwürfe und weitere Daten – durch die Apotheken-Lobby für ihre Arbeit genutzt. Dem Bericht nach hatten sich Mitarbeiter bereits gewundert, dass Vertreter der Apothekerschaft häufig sehr gut über Initiativen und Entwürfe des Ministeriums informiert waren (Quellen: Süddeutsche Zeitung, Heise).

17. Dezember 2012: Nach einem Bombenfund im Hauptbahnhof von Bonn erklärt Bundesinnenminister Hans Peter Friedrich, die Videoüberwachung im öffentlichen Bereich verstärken zu wollen. Gegenüber dem Spiegel sagt er: „Wir brauchen eine effiziente Videoüberwachung und Videoaufzeichnung auf öffentlichen Plätzen und Bahnhöfen." FDP und Opposition reagieren skeptisch: „Mit seinem reflexhaften Ruf nach schärferen Gesetzen und mehr Videoüberwachung macht es sich Innenminister Friedrich zu leicht", erklärt Renate Künast von den Grünen (Quellen: Spiegel, Süddeutsche Zeitung, Heise).

17. Dezember 2012: Generalbundesanwalt Harald Range hat verfassungrechtliche Bedenken gegen den Einsatz von Staatstrojanern und will deswegen darauf verzichten. Eine solche Maßnahme sei nur dann zu rechtfertigen, „… wenn sichergestellt werden kann, dass ein weitergehender Eingriff in die Vertraulichkeit und die Integrität des geschützten Systems unterbleibt. Eine solche Begrenzung des Eingriffs kann jedoch nach Ansicht des Generalbundesanwalts beim Bundesgerichtshof derzeit technisch nicht hinreichend sicher gewährleistet werden", heißt es in der Antwort der Bundesregierung auf eine Kleine Anfrage der Fraktion der SPD (Quellen: Deutscher Bundestag: Drucksache 17/11598, Heise).

18. Dezember 2012: Aufgrund von Bedenken, die EU-Richtlinie zur Vorratsdatenspeicherung könnte der EU-Grundrechtecharta widersprechen, legt der Österreichische Verfassungsgerichtshof dem Europäischen Gerichtshof (EuGH) Fragen zur Auslegung der Grundrechtecharta vor (Quellen: Österreichischer Verfassungsgerichtshof, Heise).

18. Dezember 2012: Eine Verordnung in Kolumbien legt fest, dass Verbindungs- und Standortdaten durch die Diensteanbieter fünf Jahre auf Vorrat gespeichert werden müssen. Zusätzlich muss eine Abhörschnittstelle für die Kommnikation über das Internet bereitgehalten werden. Die *Electronic Frontier Foundation* (EFF) kritisiert die Verordnung (Quellen: Electronic Frontier Foundation, Heise).

18. Dezember 2012: Wegen Verstoßes gegen den *Children's Online Privacy Act* (COPPA) reicht das *Center for Digital Democracy* gegen den Fernsehsender *Nickelodeon* und den Spielhersteller *PlayFirst* Beschwerde ein. Die App *Spongebob Diner Dash* soll Daten von Kindern ohne elterliche Zustimmung sammeln (Quelle: Heise).

19. Dezember 2012: Die pauschale Sperrung von *Google Sites* in der Türkei verstößt gegen das Recht auf freie Meinungsäußerung. Das hat der Europäische Gerichtshof für Menschenrechte entschieden. Der Dienst war 2009 gesperrt worden, nachdem auf einer dort gehosteten Web-Seite der Staatsgründer Kemal Atatürk verunglimpft worden sein soll (Quelle: Heise).

21. Dezember 2012: Entgegen anderslautender Erwartungen ist die Welt am 21. Dezember 2012 offenbar nicht untergegangen. Entsprechende Vorhersagen waren auf den Maya-Kalender zurückgeführt worden. Die Frage, ob es sich bei der uns bekannten Welt nicht ohnehin nur um eine Simulation handelt, wurde dabei nicht abschließend beantwortet (Quelle: Eigener Augenschein).

21. Dezember 2012: Der Britische Premierminister hält an seiner Initiative fest, nach der auf Rechnern in Haushalten mit Kindern Filter gegen Pornographie eingerichtet werden sollen. Kinder seien „den dunkelsten Ecken" des Internets ausgesetzt. In

einer Konsultation des Bildungsministeriums hatte sich zuvor die große Mehrheit gegen derartige Filter ausgesprochen (Quellen: Department for Education, Daily Mail, Heise).

24. Dezember 2012: Bei der von der Belgischen Staatsbahn betriebenen Web-Seite *b-europe.com* standen ca. 1,46 Millionen Kundendatensätze mit Anschriften, Sprachen, Geburtsdaten, E-Mail-Adressen und Telefonnummern frei zugänglich im Netz. Ein Sprecher erklärte dazu, die Datenbank sei unverlinkt auf dem öffentlichen Server untergebracht und nur mit einem „Trick" zu finden – der *Trick* bestand offenbar darin, die entsprechende URL zu kennen. Diese war in einem belgischen Nutzerforum aufgetaucht (Quellen: netzpolitik.org, Heise).

25. Dezember 2012: Berichten zufolge hat der Beauftragte der EU-Kommission für Internet-Freiheit, Karl-Theodor zu Guttenberg, bisher rund 20.000 Euro Reisekosten für seine Tätigkeit in Rechnung gestellt. Von öffentlichen Ergebnissen seiner Arbeit ist nichts bekannt; er übe seine Tätigkeit hauptsächlich im persönlichen Gespräch mit Kommissarin Neelie Kroes aus (Quellen: Spiegel, Heise).

27. Dezember 2012: Die Schwester des Facebook-Gründers Mark Zuckerberg ist wegen eines unbeabsichtigt veröffentlichten Familienfotos im Netz verärgert. Sie selbst hat offenbar das Bild auf Facebook hochgeladen, ohne es aber öffentlich machen zu wollen. Ob sie ihre Privatsphäre-Einstellungen beim Einstellen des Fotos verändert hatte, ist nicht bekannt (Quelle: Heise).

Januar 2013

2. Januar 2013: Die Verlängerung des umstrittenen *Foreign Intelligence Surveillance Act (FISA)* zur Überwachung der internationalen Kommunikation um weitere fünf Jahre wird nach dem Repräsentantenhaus auch vom US-amerikanischen Senat bestätigt. Im Rahmen der Auslandsaufklärung können so weiterhin ohne richterliche Genehmigung Telefonate abgehört und E-Mails abgefangen werden (Quelle: Heise).

7. Januar 2013: Die Kandidatin der Piratenpartei für die Landtagswahlen in Niedersachsen, Katharina Nocun, reicht eine Beschwerde gegen die Bundesregierung bei der EU-Kommisson ein. Die Unabhängigkeit des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sei verletzt, da die Behörde dem Bundesinnenministerium unterstellt ist. Die meisten der beamteten Datenschützer setzten ihre Laufbahn im Bundesinnenministerium fort und arbeiteten weisungsgebunden (Quellen: kattascha.de, Heise).

7. Januar 2013: Der niedersächsische Innenminister Schünemann wird turnusgemäß Vorsitzender der Innenministerkonferenz der Länder. In einem Papier fordert er eine neue nationale Strategie gegen den Terror (Quellen: Innenministerkonferenz, Heise).

11. Januar 2013: Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität nimmt seine Arbeit auf. Es soll sich auf organisierte Kriminalität konzentrieren, mit den Schwerpunkten sexuelle Ausbeutung von Kindern und Finanzdelikte. Zusätzlich soll es Attacken auf kritische Infrastrukturen und Informationssysteme bekämpfen (Quellen: netzpolitik.org, Heise).

13. Januar 2013: Dem australischen Geheimdienst *ASIO (Australian Security Intelligence Organisation)* soll die Befugnis gegeben werden, IT-Systeme Unbeteiligter zu infiltrieren, um auf diesem Weg Zugang zu Rechnern von mutmaßlichen Terroristen oder Kriminellen zu erhalten. Dies solle nur in Ausnahmefälle möglich sein; eine richterliche Erlaubnis ist dafür aber nicht erforderlich. Der Datenschutzbeauftragte des Staates Victoria hatte zuvor tiefe Einschnitte in die Grundrechte der Betroffenen durch die Befugnis moniert (Quellen: news.com.au, Heise).

15. Januar 2013: Die US-amerikanische *National Rifle Association (NRA)* veröffentlicht einen Monat nach dem Amoklauf von Newtown eine App, die unter anderem einen virtuellen Schießstand simuliert. Zuvor hatte sie Computerspiele für die Gewalt verantwortlich gemacht. Die App ist ab einem Alter von vier Jahren freigegeben (Quelle: Heise).

16. Januar 2013: Das Bundeskriminalamt (BKA) schafft offenbar die Software FinFisher der Firma Gamma an, um sie bis zur Fertigstellung des eigenen Staatstrojaners zur Quellen-Telekommunikationsüberwachung zu nutzen. Gamma steht wegen des Verdachts in der Kritik, ihre Software an Diktaturen zu liefern (Quellen: netzpolitik.org, Heise).

19. Januar 2013: Die in den USA für die Flughafensicherheit zuständige *Transportation Security Administration (TSA)* will 174 an Flughäfen installierte Nacktscanner der Firma *Rapiscan* wieder entfernen. Es sei nicht möglich gewesen, Software zu entwickeln, die die Darstellung der Körper weniger realistisch macht. Die Geräte standen bereits im Verdacht, eine zu hohe Röntgenstrahlung zu entwickeln (Quelle: Heise).

20. Januar 2013: Bei den niedersächsischen Landtagswahlen wird die bisherige Regierung aus CDU und FDP abgewählt. Mit einer Stimme Mehrheit werden SPD und Grüne die nächste Landesregierung bilden. Damit scheidet auch der in Bürgerrechtskreisen umstrittene Innenminister Uwe Schünemann aus seinem Amt aus; er wurde unter anderem zweimal mit dem *BigBrother-Award* ausgezeichnet. Die Piratenpartei verfehlt mit 2,1 % die Fünf-Prozent-Hürde deutlich (Quellen: Zeit, Spiegel).

23. Januar 2013: 8438-mal stellen US-amerikanische Behörden 2012 Anfragen zu Nutzerdaten von Google. Betroffen waren 14.791 Nutzerkonten. Damit sind die USA für ein Drittel der 21.389 weltweiten Anfragen zu insgesamt 33.634 Nutzerkonten verantwortlich. Deutschland liegt mit 1550 Anfragen zu 1944 Konten auf Platz vier (Quellen: Google-Transparenzbericht, netzpolitik.org, Heise).

24. Januar 2013: Der Bundesgerichtshof urteilt, dass bei einem Ausfall der Internet-Verbindung grundsätzlich ein Anspruch auf Schadensersatz besteht. Dem Anschluss wird eine „zentrale Bedeutung" für die Lebensführung zugemessen (Quellen: Bundesgerichtshof, netzpolitik.org, Heise).

24. Januar 2013: Seinem Lobby-Bericht zufolge hat Google sein Budget für Lobbying in den USA im Jahr 2012 von 9,6 Millionen US-$ auf 18,22 Millionen US-$ nahezu verdoppelt (Quellen: United States House of Representatives, Heise).

Sebastian Jekutsch

Betrifft: Faire Computer

Dies ist die erste Ausgabe der Rubrik „Betrifft: Faire Computer“. Sie soll zu einer regelmäßigen Rubrik in der FIfF-Kommunikation werden, in der wir über neueste Entwicklungen im Bereich sozialverträglicher IT-Produktion berichten. Damit – und mit dem rechtzeitig zum 29C3 fertig gewordenen Flyer nebst neuem Logo – hat das Thema „Fair IT“ beim FIfF längerfristig Einzug gehalten. Kritisch Informieren war schon immer die Stärke des FIfF, und so besteht unsere Arbeit zunächst darin, unsere IT-Techniker- und -Anwenderwelt zu informieren: über die Zustände bei der Herstellung der Geräte, von denen wir abhängen und mit denen wir unser Geld verdienen.

Im vergangenen Vierteljahr sind erneut schwere Vorwürfe gegen Markenfirmen erhoben worden. Sowohl bei einem Samsung-Zulieferer, bei Samsung selbst, als auch beim Vertragsfertiger Foxconn – in einem Werk wo zum Zeitpunkt der Untersuchung für Nintendo gearbeitet wurde – wurde der für unsere „westliche“ Welt vielleicht schwerwiegendste Vorwurf laut: **Kinderarbeit**. Es geht um 16-jährige Schüler und Studentinnen, die in China als Praktikanten von den Lehrern völlig fachfremd in die IT-Werkshallen vermittelt werden, wo sie die gleiche Arbeit machen wie die Angestellten: 12-Stunden Tag- und Nachtschicht am Fließband. Laut auch von China ratifizierter Arbeitsnorm der Internationalen Arbeitsorganisation (ILO) dürfen weder Minderjährige schwere oder ungesunde Arbeit verrichten noch Praktikanten fachfremd eingestellt werden.

Im Bereich der Rohstoffgewinnung zeigt der Abschnitt 1502 des U.S.-amerikanischen Dodd-Frank-Act, der heimische Firmen zwingt, Geschäfte in der D.R.Kongo und angrenzenden Staaten zu veröffentlichen, nun positive Wirkung, nachdem er zunächst wie ein Embargo wirkte und lediglich illegalen Schmuggel förderte: Es soll erstes **„konfliktfreies“ Zinnerz** aus dem Kongo geben, d.h. bei der Förderung und dem Transport des Gesteins verdienen weder Milizen noch autonome Regierungstruppen Geld, etwa durch Wegzoll oder bewaffnete Inbesitznahme. Im Laufe dieses Jahres soll das zertifizierte Lötzinn auch bei den IT-Fertigern ankommen. Initiiert haben das Programm AVX und Motorola.

Diese Gelegenheit hat das Projekt **FairPhone** genutzt, seine Strategie zu konkretisieren und angekündigt, als erster ein Smartphone anzubieten, welches eben dieses konfliktfreie Zinn beinhaltet. Damit wäre ein kleiner Schritt getan. Zwar folgt aus Konfliktfreiheit nicht Fairness – denn das Einkommen der Kleinschürfer verbessert sich zum Beispiel nicht – aber die korrupten Strukturen zu Lasten der Bevölkerung werden umgangen. Dazu möchte FairPhone Partnerschaften mit einem Hersteller und einem Provider eingehen; die Initiative selbst wirkt dabei vor allem vermittelnd. Sie möchten im Juni ihr Gerät vorstellen und im Herbst 10.000 Exemplare zu 250 bis 300 Euro verkaufen.

Da ist die faire Maus von Nager-IT (in einer früheren FIfF-Kommunikation noch als „Phefe“ vorgestellt) schon weiter: Seit Anfang Dezember kann man sie kaufen, für € 34,90 inkl. dritter Maustaste und Versand, siehe *www.nager-it.de*. Die auf der Website dokumentierte Herstellerliste und Lieferkette zeigt: Das meiste wird in Deutschland hergestellt, zentrale Bestandteile wie etwa der Chip mit der Sensorlogik können derzeit aber nur unter

erste Seite des neuen Flyer „Fair IT“

unbekannten – also vermutlich unfairen – Arbeitsbedingungen aus Fernost gefertigt und geliefert werden. Ich habe eine solche **teilfaire Maus** inzwischen im Dauereinsatz. Vielleicht wäre es eine schöne Idee, einige Exemplare mit FIfF-Logo bedrucken zu lassen und unseren Mitgliedern anzubieten?

Wer mehr zu dem Thema wissen möchte, kann sich bei unserer Maillingliste anmelden: *http://lists.fiff.de/mailman/listinfo/fiff-fairit*. Dort kommen Nachrichten wie oben zeitnaher, die Quellen werden natürlich angegeben und es wird ein wenig diskutiert, auch über die Frage, was wir tun können, um die Entwicklung positiv zu beeinflussen. Die Liste hat schon 43 Mitglieder, nicht nur aus FIfF-Kreisen.

Sebastian Jekutsch ist FIfF-Mitglied aus Hamburg.
Kontakt: *sj@fiff.de*

Digitalisierte Gesellschaft – Wege und Irrwege

Manfred Nagl

Zwischen Guckkasten und Rummelplatz

Konstanten und Wandel in der Welt der Kindermedien

Ein Referat, das im Kontext des Tagungsthemas schon in der Titelformulierung manchen geradezu vorgestrig erscheinen mag, bedarf zunächst – wenn nicht gar der Legitimation – so doch einiger Erläuterungen. Es wird in der Tat im Folgenden nur am Rande explizit von digitalen Medien die Rede sein. Dennoch hoffe ich, Ihnen für die weitere Diskussion des Tagungsthemas die eine oder andere Anregung geben zu können.

Kindermedien sind – vom Bereich der Kinderliteratur einmal abgesehen – nach wie vor wenig beachtete Stiefkinder der Forschung. Dies gilt vor allem für die Kindermedien als Gesamtphänomen. Darunter verstehe ich die Gesamtheit der Einzelmedien, die vornehmlich oder ausschließlich für Kinder produziert werden, ebenso wie die Medien, die von Kindern – oft gegen den Willen vieler Erwachsener – in eigener Regie bevorzugt genutzt werden.

Das verbreitete Desinteresse ist umso erstaunlicher, als sich der technologische Wandel zum einen in immer kürzeren Phasen vollzieht, man denke nur an die Entwicklung der Ton- und Bildträgermedien in den letzten hundert Jahren, und sich zum anderen gerade der Kindermediensektor bei näherer Betrachtung oft als besonders innovativ erweist. Die kulturelle Unbefangenheit und Vorurteilslosigkeit des jungen Publikums macht es zum geeigneten Versuchslabor für neue Medienentwicklungen.

Vielleicht ist dies mit ein Grund dafür, dass die Diskussion um Nutzen und Schädlichkeit neuer Medien sich bevorzugt auf den Aspekt ihrer Wirkung auf Kinder und Jugendliche fokussiert, mit besonderer Vehemenz geführt wird und gerne alarmistische Züge annimmt.

Vielleicht kann hierbei ein Streifzug durch die Entwicklung der für Kinder produzierten bzw. von ihnen genutzten Medien einige Anregungen geben. Die dabei immer wieder zutage tretenden Besorgnisse und Ängste und die mit heißer Emphase geführten Debatten um die Gefahren der neuen Medien sollen weder lächerlich gemacht noch verharmlost werden. Es geht, wie sich zeigen wird, dabei schließlich um nicht mehr und nicht weniger als den Kultur- und Wertetransfer von der jeweiligen Erwachsenengeneration zur nächsten. Ich hoffe vielmehr, dass eine Exkursion in die abgekühlteren Regionen der Mediengeschichte hilfreich ist für eine umsichtigere und weniger reflexhafte Diskussion der Probleme.

Rummelplatz und Guckkasten

Im Ganzen gesehen lässt sich sowohl die historische Entwicklung wie das aktuelle Terrain der Kindermedien als Wechselspiel zwischen **Rummelplatz und Guckkasten** charakterisieren. Diese medialen Typen haben einerseits den Vorzug, als reale Medien mit beträchtlicher Vergangenheit zu existieren, andererseits repräsentieren sie zugleich auch wichtige aktuell im Spiel befindliche Medientypen.

Der Rummelplatz steht dabei für den Typus der Präsenz- oder Live-Medien, der Guckkasten dagegen für den Typus der Apparate- bzw. Speichermedien (manche sprechen auch von Fenster- oder Rahmenmedien). Betont sei, dass es sich dabei zwar um elementare, aber nicht miteinander unvereinbare, quasi antagonistische Medienalternativen und Rezeptionsweisen handeln, sondern eher um die jeweils idealtypischen Extreme an den beiden Enden einer Skala graduell unterschiedlichster Ausprägungen, und dass Mischformen nicht nur möglich, sondern häufig sind. Spezielle Medien bzw. Medieninhalte für Kinder gibt es in Europa nachweisbar seit der Frühen Neuzeit, also etwa seit der Mitte des 16. Jahrhunderts. Davor gab es Medien, die auch, aber nicht ausschließlich, an Kinder adressiert waren. In analphabetischen Gesellschaften haben Erwachsene keinen Rezeptionsvorsprung gegenüber Kindern.

Die Medienwissenschaft, die aus der Beschäftigung mit auf moderner Technik basierten Massenmedien entstanden ist, verführt leicht zu dem Vorurteil, dass vorindustrielle Gesellschaften sich demnach durch Medienmonotonie und Medienarmut ausgezeichnet hätten. Bei näherem Zusehen wird jedoch eine erstaunliche Vielzahl von Informationsträgern und Informationsvermittlern sichtbar. Zu den wichtigsten gehörten:

Medien in der nicht- und teilalphabetisierten Epoche:

- **Mündliche „volksläufige" Erzähltradition**
  (Märchen, Legenden, Sagen, Mythen, Anekdoten, Reime, Legenden, Rätsel, Sprichwörter, Schwänke, Witze u. a.)
- **Mündliche kirchliche Erzähl- und Präsentationsformen**
  (Liturgie, Predigt und Messrituale, Prozessionen, Exempel, Legenden, Passions- und Mysterienspiele)
- **Kirchen, Kirchenmalerei, kirchlicher Schmuck**

- **Feste** (Komödianten, Spielleute, Sänger, Gaukler, Artisten, Tierbändiger und Quacksalber, Wahrsager, Erzähler, Mysterienspiele, kirchliche Schauspiele)

- **Öffentliche Strafrituale und Hinrichtungen**

Insbesondere romanische Kirchen waren regelrechte „Bildermaschinen", quasi Guckkästen, bei denen sich der Betrachter in deren Innerem befand. Sie waren bis in den letzten Winkel mit Bildern aus der biblischen Schöpfungs- und Heilsgeschichte ausgemalt. Aus heutiger Sicht ebenso auffällig wie befremdlich ist dabei die seit dem 12. Jahrhundert allenthalben zu Tage tretende Vorliebe für explizit detaillierte Darstellung grausamer Szenen religiös fundierter Gewalt („Abrahams Opfer", „Kain und Abel", „Kindesmord zu Bethlehem", Passion Christi, Martyrien, Apokalypse, „Jüngstes Gericht" und Höllendarstellungen). Diese Themen finden sich zudem nicht nur in der kirchlichen Wandmalerei (und später in Bildern und Skulpturen), sondern ebenso in Passions- und Mysterienspielen, in den Predigt-Exempeln und Traktaten, Legenden und anderen erbaulichen Texten. Bildliche Darstellungen waren lediglich die für Kinder am leichtesten zugänglichen Medien.

Abbildung 1: „Bildermaschine" Hocheppan mit Katharinakapelle und Kreidenturm, ca. 1300-1310 – CC BY-SA 3.0 , ManfredK

Gewaltdarstellungen

Im Kontext der heutigen Mediendiskussionen fällt dem in dieser Weise befangenen Betrachter die allgegenwärtige, explizite, aus heutiger Sicht oft geradezu lustvolle Darstellung von religiös begründeter Gewalt auf, die die vorindustriellen Medien bis in das 17. Jahrhundert hinein zu prägen scheint.

Und was vielleicht noch bedeutsamer ist: Eingebettet waren diese Medienmotive in eine nicht minder gewaltbestimmte reale Welt, in der – abgesehen von häufigen kriegerischen Ereignissen – schwerste körperliche Züchtigung, das Zusehen oder die Mithilfe beim Töten von Tieren, öffentliche Prangerstrafen zum Alltag gehörten und die ebenso grausamen wie beliebten öffentlichen Hinrichtungsspektakel – auch für Kinder – festliche Höhepunkte darstellten. Man lebte in ständiger Furcht vor der Zuchtrute eines zürnenden und strafenden Gottes, vor der Wiederkehr armer Seelen und Dämonen, vor Hexen und dem Teufel, vor dem baldigen Weltuntergang und dem Jüngsten Gericht. Natürlich gab es nicht *nur* solche gewaltgesättigten Darstellungen, aber sie waren keine Ausnahmen. Die Kirche forcierte den Märtyrerkult als Mittel gegen die wachsenden Häresiebewegungen. Jede Kirche, jeder Altar beherbergte Reliquien und hatte einen oder mehrere Schutzpatrone bzw. Schutzpatroninnen und die hatten in der Regel eine Märtyrer-Biographie.

Abbildung 2: Rundscheibe Enthauptung Johannes des Täufers, Niederlande, um 1500

Die Kunsthistorikerin Silke Tammen zieht folgendes Fazit:

> *„Heilige werden einzeln oder in großen Gruppen geköpft, aufgespießt, mit Pfeilen gespickt, ausgepeitscht, auf Räder geflochten, geröstet und in Öl gesotten, ihre entblößte Haut wird verbrannt, abgezogen und mit eisernen Striegeln zerrissen, Gedärme werden herausgewunden, Augen ausgestochen, Zungen ausgerissen, Brüste amputiert."*[1]

Abbildung 3: Höllenrachen (Mysterienspiel „Passion von Arras", 1430)

An den überaus beliebten Passions- und Mysterienspielen, die oft die eigentlichen Attraktionen im Kirchenjahr waren, nahmen Kinder nicht nur als Zuschauer, sondern auch als Akteure teil – besonders als höllisches und himmlisches Gesinde. Im Zentrum der inszenatorischen und spektatorischen Aufmerksamkeit stan-

Abbildung 4: Der Teufel als Kinderräuber (Geoffroy de La Tour Landry: Der Ritter vom Turn. Der Spiegel der tugent vnd Ersamkeit. Augsburg 1495)

den besonders der Auftritt des Teufels, die Sintflut, die Öffnung der Höllenpforte, die Qualen der armen Seelen im Fegefeuer, die Bestrafung der Sünder, der Weltuntergang und das Jüngste Gericht. Märtyrer wurden – verkörpert durch Puppen – gefoltert, enthauptet, verbrannt. Die Höllenpforte wurde meist durch einen Drachenschlund dargestellt, der Feuer und Rauch ausspie, und dem dann Satan entstieg, bevor er durch Christus wieder in

Abbildung 5: Der Kinderfresser (Flugblatt Augsburg um 1590)

seine Schranken verwiesen wurde. Der leibhaftige Teufel war allgegenwärtig. Noch in den Schultheaterstücken des 16. Jahrhunderts treibt er leibhaftig sein abschreckendes Unwesen.

Der in den 1490er Jahren vermutlich erste gedruckte Erziehungsratgeber für Eltern, der „Spiegel von Tugend und Ehrsamkeit", besteht in der Hauptsache aus Exempeln schlechten Verhaltens, bei denen der Teufel die Unbelehrbaren zur Raison bringt.

Dagegen ist der erste Beleg eines speziell an Kinder adressierten Druckerzeugnisses – ein Einblattdruck, also ein Flugblatt – aus dem Jahr 1590 ein vergleichsweise moderates Erziehungsmittel. Es handelt sich dabei um die Darstellung eines sogenannten *Kinderfressers*, einer schrecklichen Riesengestalt, die ungehorsame Kinder verschleppt und auffrisst.

Das Motiv war bis ins 18. Jahrhundert hinein ein überaus beliebtes Flugblatthema und in ganz Westeuropa verbreitet. Elemente dieser Kinderschreckfigur haben sich übrigens bis ins 20. Jahrhundert gehalten. Vor dem *Nachtkrapp* oder *Nachtgiger* wurden Kinder noch in den 1950er Jahren gewarnt, und auch von den Krampussen und Pelzmärtles, den furchterregenden Begleiter des Christkinds oder Nikolaus, wissen wir aus Autobiographien, dass sie bei Kindern geradezu traumatische Angstzustände hervorrufen konnten.

Aus heutiger Sicht fragt man sich, ob dieser anscheinend völlig unbefangene Einsatz von Gewalt als Erziehungsmittel nicht zumindest im Hinblick auf jüngere Kinder auch problematisiert wurde. Aber bis ins 17. Jahrhundert hinein lautet die Antwort eindeutig „Nein". Soweit kritische Stimmen belegbar sind, wenden sie sich nicht gegen die Grausamkeit, sondern Nacktheit und Schönheit bei der Darstellung von weiblichen Heiligen, weil

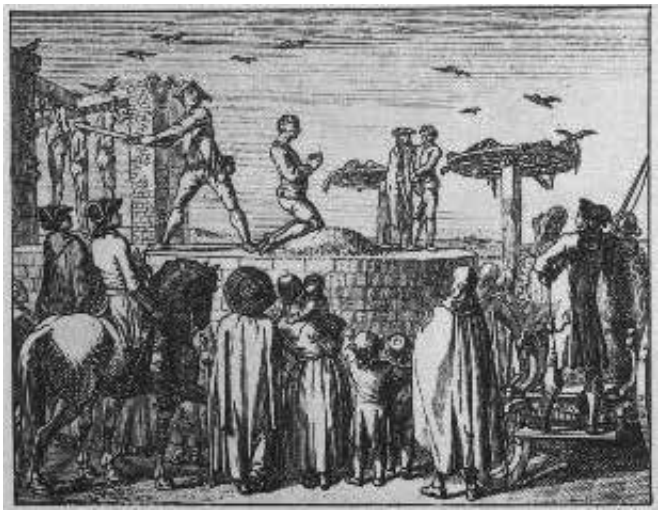


Abbildung 6: „Kinder, gewöhnt euch, der Obrigkeit zu gehorchen, denn [...] ihre Strafen sind furchtbar." (Johann B. Basedows „Elementarwerk". 1774, Tabelle XXXIV)

diese insbesondere noch ungefestigte Jugendliche zu unziemlichen Gedanken anregen könnten.

Noch im letzten Drittel des 18. Jahrhunderts glaubte beispielsweise einer der prominentesten philanthropischen Pädagogen, Johann Basedow, sonst einer der unermüdlichsten Anwälte neuer eigengesetzlicher und altersgerechter Erziehungsmetho-

den, nicht auf drastische Abschreckung verzichten zu können. In einer 1774 publizierten Sammlung von Anschauungstafeln für den Elementarunterricht zeigt er unter anderem eine öffentliche Enthauptung und versieht sie mit dem Merksatz: „Kinder, gewöhnt euch, der Obrigkeit zu gehorchen, denn [...] ihre Strafen sind furchtbar." (Zur Entschuldigung wie Erklärung lässt sich allerdings anführen, dass spektakuläre öffentliche Hinrichtungen damals noch reale gerichtliche Praxis waren.)

Als vorsichtiges und vorläufiges Fazit lässt sich allenfalls festhalten, dass in der christlichen Kultur früherer Zeiten Gewaltdarstellungen offensichtlich unverzichtbare Bedeutung haben: einerseits als Opfergewalt (Märtyrer) und andererseits als Droh- und Strafgewalt Gottes (Gottesgerichte, Fegefeuer, Hölle usw.). Der religiöse Kontext, in den Gewalt damals eingebunden war, erlaubte es, Gewalt sehr explizit zu thematisieren, gleichzeitig aber auch kollektiv zu kontrollieren. Über die jeweils individuelle Rezeption lässt sich freilich nur spekulieren. Dass die Gewaltdarstellungen gerade auf Kinder einen nachhaltigen Eindruck machten, war beabsichtigt und darf als evident angenommen werden.

Abbildung 7 : Bänkelsänger mit Publikum (1740)

Abbildung 8 : Titelseite eines Bänkelsangheftes (1851)

Laterna Magica und Bänkelsang

Im Laufe des 17. Jahrhunderts tauchen zwei neue Medien auf, die für Kinder besonders attraktiv waren: Der *Bänkelsang* und die *Laterna Magica.* Der Bänkelsang war ein typisches Rummelplatzmedium und gleichzeitig ein früher multimedialer Medienverbund, in dem Präsenz- und Speichermedien verschränkt waren. Nahezu alle erhaltenen Bilddokumente zum Bänkelsang zeigen Kinder als besonders fasziniertes Publikum. Seinen Namen hat der Bänkelsang von der mobilen Bühne, auf der sich die Akteure – Sänger und Erklärer, Musiker – präsentierten. Die Speichermedien waren eine Bildertafel und illustrierte Heftchen, mit Text, Dokumentation und moralischer Nutzanwendung. Im 20. Jahrhundert machten die neuen Bild- und Tonmedien und die Sensationspresse dem Bänkelsang den Garaus.

Abbildung 9: Laterna-Magica-Vorführung durch professionelle Schausteller (1765)

In der zweiten Hälfte des 17. Jahrhunderts wird die Laterna Magica entwickelt. Sie verbreitet sich innerhalb weniger Jahrzehnte in ganz Westeuropa als Jahrmarktsattraktion. Technisch gesehen ist die Zauberlaterne der Vorläufer aller späteren Bildprojektoren – vom Dia-, über den Filmprojektor bis zur Power-Point-Präsentation.

Die Entwicklung dieses Mediums ist unter mehreren Aspekten auch heute noch interessant: So ist die Laterna Magica das erste der modernen technischen Apparatemedien, bei dem nicht nur die Informationsproduktion (wie beim Theater oder Druckerzeugnissen), sondern auch die Rezeption nur mit Hilfe einer technisch-physikalischen Apparatur möglich ist. Darin ist die Zauberlaterne ein Vorgänger der Stereoskopie, der Fonografie, des Telefons, der Kinematografie, des Rundfunks und Fernsehens und des Computers. Und die Laterna Magica war anfangs ein Guckkastenmedium im Rummelplatzkontext. Die Vorführung regelrechter Bildprogramme wurde durch Erzähler, Musiker, Sänger, Possenreisser usw. umrahmt und ergänzt.

In der Entwicklung und dem Erfolg des Mediums manifestiert sich nicht nur der allgemeine Hunger nach künstlichen Bildern, sondern nach farbigen und bewegten, „lebenden" Bildern im Besonderen. An der Optimierung des Mediums wurde in die-

Abbildung 10: Laterna-Magica-Bild: Mondlandschaft (um 1900)

ser Hinsicht unermüdlich und erfolgreich gearbeitet: Bald gab es bewegliche Schiebe-, Hebel- und Drehbilder. Mit mehreren Projektoren, Dreifachobjektiven und der Projektion auf künstlichem Nebel wurden schon um die Wende vom 18. zum 19. Jahrhundert geradezu filmische Effekte erzielt – vergleichbar etwa mit den aufwändigen Dia-Ton-Shows, mit denen bei uns noch vor wenigen Jahren Abenteuerreisende sich wieder ihre Reisekosten zu verdienen suchten. (Sie erinnern sich sicherlich.)

Abbildung 11: Deckelbild einer Laterna-Magica-Schachtel (um 1900)

Auf dem Rummelplatz und mit der Laterna Magica beginnt aber auch die visuelle Welteroberung für das gemeine Volk; die bunte Bebilderung nahezu aller Erfahrungs- und Phantasiebereiche. Das häufig kreisrunde Format der Bildprojektion wurde geradezu zum Erkennungsmerkmal für den grenzüberschreitenden wissenschaftlichen Blick – ins mikroskopisch Kleine, teleskopisch Ferne oder ethnografisch Fremde.

Im Laufe des 19. Jahrhunderts wird aus dem aufwändigen Expertenmedium ein industriell und seriell standardisiert gefertigtes Massenmedium für den individuellen häuslichen Privatkonsum (als Vorform des Heimkinos). Ende des 19. Jahrhunderts ist die *Zauberlaterne* ein weltweit verbreitetes und beliebtes häusliches Kindermedium in bürgerlichen Kreisen.

Auch darin ist die Laterna Magica Vorläuferin einer Entwicklung gewesen, die für nachfolgende Medien geradezu symptomatisch wird: der Weg vom öffentlichen Expertenmedium zum individuellen Privatmedium. Die Phonographie, der Film, der Computer – selbst ein so peripher erscheinendes Medium wie das Kasperltheater nehmen diesen Karriereverlauf.

Aber noch in einem weiteren Punkt erweist sich die Laterna Magica als zukunftsweisend. Von Anfang an zeichneten sich Verbreitung und Rezeption des Mediums durch einen zwiespältigen Doppelcharakter von Belehrung und Unterhaltung, einen Antagonismus von Aufklärung und Manipulation aus.

Dieser Antagonismus – legitime Belehrung kontra missbräuchliche Unterhaltung – wiederholt sich von da an bei nahezu allen seither auf den Markt gekommen Medien: dem Guckkasten im engeren Sinn, dem daraus entwickelten Papiertheater, den Bilderbogen, den Familien- und Kinderzeitschriften, der Stereoskopie, den Sammelbildern, den Gesellschafts- und Individualspielen, der Phonographie, dem Film, dem Rundfunk und Fernsehen und last not least dem Internet.

Lesewut und *Vielleserei*

Seit der Entwicklung der modernen Pädagogik im Zuge der Aufklärungsbewegung des 18. Jahrhunderts ist die neuzeitliche Medienerziehung durch eine Reihe von kaum auflösbaren Antagonismen gekennzeichnet. Statt stumpfem Drill und Einpauken propagierten die philanthropischen Pädagogen das lustvolle intrinsische Lernen aus Interesse und Neugier. Dazu sollten unterhaltende Elemente den Lernstoff attraktiv machen. Andererseits war bloße Unterhaltung verpönt, ja ernsthaftem Lernen abträglich. Auch dieser Konflikt zwischen Unterhaltung und nützlichem Wissenserwerb prägt bis heute die Mediendiskussion. Einerseits sollte die Einbildungskraft der Kinder für das Lernen dienstbar gemacht werden, andererseits galt eben diese Phantasie als unberechenbar und gefährlich für kontrollierte Lernprozesse. Das gravierendste Dilemma aber ergab sich aus der möglichst frühen Befähigung der Kinder zu eigenverantwortlicher Medienrezeption einerseits – damals ging es dabei vor allem um die Lesefähigkeit – und der Vermeidung einer verfrühten Konfrontation mit Medieninhalten andererseits, die dem jeweiligen kindlichen Entwicklungsstadium als nicht angemessen oder gar schädlich erachtet wurden.

Anders gewendet: Man etablierte Kindheit als spezifischen und schutzwürdigen Lebens- und Erfahrungsraum, aber gleichzeitig wurde dieser Schonraum durch die Befähigung der Kinder zu eigenständiger, unkontrollierter Lektüre bedroht. Die sich daraus ergebende Gefahr einer schädlichen Verfrühung, ja im Grunde eines *Verschwindens* eben jener Kindheit, die man gerade ausgerufen hatte, ist seither ein Dauerproblem der Medienpädagogik. Und dieser Aspekt beherrschte damals die Diskussionen um *Lesewut* und *Vielleserei*:

> *„Den verderblichsten Einfluß hat die Lesesucht auf die Jugend, theils weil in derselben das unerfahrne Herz am empfänglichsten für Eindrücke jeder Art, theils weil die Einbildungskraft ohnehin das Thätigste ihrer Seelenvermögen ist. Wirft dann ein unglücklicher Umstand, Schlechtigkeit der Bücherausleiher oder Verkäufer,*

Nachlässigkeit der Erzieher, Unachtsamkeit der Aeltern, ein auf Sittenverderbniß berechnetes Buch, das Machwerk eines geilen Wollüstlings, in ihre Hand; wird ihre Einbildungskraft mit unanständigen Vorstellungen, mit verschönernden Gemälden viehischer Triebe, mit Verzierungen des Verbrechers vertraut gemacht – wer rettet dann das schirmlose Herz vor der vergifteten Phantasie? … Was der Mütter treue Liebe, was des Vaters fromme Sorge, was des Lehrers warmer Eifer Jahre lang baute, reißt oft der Fluch eines einzigen verbrecherischen Buches in einer Stunde nieder.[2]

Die Strategie der Medienproduzenten war dagegen wesentlich unkomplizierter. Sie bestand darin, gleichzeitig den sowohl unterhaltenden (d.h. für Kinder attraktiven) wie lehrhaften (also wertvollen) Charakter ihrer Produkte zu betonen. Gleichgültig, ob es sich um die Laterna Magica, Familien- und Kinderzeitschriften, um Spiele, um die Stereoskopie und Sammelbilder, Schallplatten oder den Film handelte. Und völlig falsch war diese Behauptung schon deshalb nicht, weil Kinder geradezu unvermeidlich bei allem, was sie tun, etwas lernen. (Um ein aktuelles Beispiel zu bemühen: Ravensburger vermarktet sein digitales Lesestiftsystem *Tiptoi* vor allem als neues, optimales Lerninstrument. Der Umsatz wird zu 80 Prozent mit Spielen gemacht.)

Durch die Fülle der neuen Medien und neuer Marketingstrategien, bei denen die Werbung ein immer wichtigere Rolle spielte, etablierte sich spätestens gegen Ende des 19. Jahrhunderts eine massenhafte, industriell produzierte und strikt kommerziell ausgerichtete populäre Massenkultur, in der Kinder und Jugendliche vielfach eine Schlüsselrolle als *early adopters*, als Konsummotivatoren der Eltern, aber zunehmend auch als autonome Konsumenten spielten. (Die Süßigkeitautomaten begannen ihren Siegeszug vor allem als Kindermedium; ebenso die Phonographie – mit Sprechpuppen und Kindertonträgern. Und das frühe Kino, so bilanziert die Filmhistorikerin Corinna Müller, verdankte „vor allem Kindern und Jugendlichen" seinen Aufstieg.)

Zur Sammelsucht und Konsumwut verführende Sammelbildserien, zu unkontrolliertem Konsum verleitende Süßigkeitsautomaten, frivole Theaterstücke, derb-humoristische Postkarten und Photoserien, *Mutoskopautomaten* mit pikanten Bildserien, erotisch anzügliche Witzblätter, Musikautomaten und Grammophone mit schlüpfrigen Gassenhauern, schreiende Plakate, Groschenhefte mit grellen Titelbildern und nicht weniger sensationell aufgemachte Filme bedrohten aus der Sicht der bürgerlichen Kulturträger nicht nur die Kinder, sondern die Kontinuität des kulturellen Wertesystems insgesamt. Hinzu kam eine in dieser Größenordnung und Intensität neue atemberaubende großstädtische Rummelplatzkultur, bei der die neuen Vergnügungsparks mit ortsfesten Zirkussen, gigantischen Fahrgeschäften, sensationellen Schaubuden, Varietés, Kuriositätenkabinetten, Schausportwettkämpfen, Völkerschauen, Tingeltangel, Glücksspielautomaten und Kintopps kulturell quasi permanent exterritoriale Zonen innerhalb der bürgerlichen Kultur bildeten. (Von der Wissenschaft wurde dieser Bereich als bedeutsamer Sektor der Kinderkultur bisher kaum zur Kenntnis genommen.)

Zwei Gruppen schienen aus bürgerlicher Sicht durch die neuen, strikt kommerziell ausgerichteten Verführungen besonders gefährdet: die städtische, proletarische Unterschicht allgemein und Kinder und Jugendliche im Besonderen. Die Befürchtungen kulminierten zwischen Jahrhundertwende und 1. Weltkrieg in einem in diesem Ausmaß und dieser Intensität nie dagewesen „Kampf gegen Schund und Schmutz". Wobei *Schund* für ästhetisch Wertloses und Minderwertiges, *Schmutz* für moralisch Verwerfliches stand.

Groschenhefte und Kino

Hauptziele der Kampagnen waren dabei die modernen großstädtischen Lebensverhältnisse im allgemeinen und zwei neue Medien im besonderen: die Groschenhefte und das Kino. Die Groschenhefte bieten jeweils pro Heft abgeschlossene Geschichten mit festen Serienhelden und setzen damit Kinder und Jugendliche erstmals in der Kulturgeschichte in die Lage, sich in nennenswertem Umfang ihre Lektüre in eigener Regie, unkontrolliert von Erwachsenen zu beschaffen. Das zweite Medium ist das Kino, damals noch *Kintopp* genannt, es bietet mit seinen permanenten Tagesvorstellungen einem Kinder- und Jugendpublikum einen sozialen Raum, in dem weder die Medienrezeption, noch das allgemeine Verhalten unter pädagogischer Kontrolle stehen.

Zu den bereits bekannten in der Lesewutdebatte entwickelten Argumenten, unter denen das der Gefahr schädlicher Verführungen durch Medien das wichtigste ist, kommen nun zwei weitere: die drohende Entstehung einer dem Einfluss der Erwachsenen entzogenen gefährlichen Selbstorganisation von Kindern und Jugendlichen, und die Gefahr des Entstehens einer völlig kulturabstinenten, ja kriminellen Generation. So beobachtete man beispielsweise die Bildung von Verehrergruppen um bestimmte Heftserienhelden: Was wir heute als Fanclubs bezeichnen würden, wurde damals als Keimzelle krimineller Kinder- und Jugendbanden dämonisiert.

Drei zeitgenössische Zeugnisse zur Illustration der durch diese Medien ausgelösten Irritationen: Das erste Beispiel bezieht sich auf spezielle Kinovorstellungen für Kinder und illustriert anschaulich das Gefühl eines Generationsbruchs, der Entfremdung, des schon stattgefundenen Abgleitens der jungen Generation in eine

Manfred Nagl

Prof. Dr. **Manfred Nagl:** Jahrgang 1940, Professor für Medien- und Kommunikationsmanagement an der Hochschule der Medien Stuttgart (HDM), im Ruhestand. Zahlreiche Publikationen zu Themen des Bibliothekswesens, der Kultur- und Mediengeschichte.

den Erwachsenen fremde und sie aufs Höchste beängstigende Welt. Der Zeitzeuge, ein Pfarrer, berichtet wie ein Ethnologe über eine den Erwachsenen weder zugängliche, noch verständliche und doch mitten in dieser Gesellschaft existierende Welt.

> *„Diese Kinder, die die ersten Reihen füllen, geben dem Vorführungsraum […] ein charakteristisches Gepräge. Die Erwachsenen sind hier nur Besucher, sie aber fühlen sich wie zuhause. Mit den Kellnern, die mit den Tabletts von Reihe zu Reihe gehen, stehn sie auf gutem Fuße, denn einen oder zwei Groschen für Leckereien haben die meisten von ihren Eltern erbettelt oder sich irgendwie verdient. Früher wanderten sie in die Sparbüchse, heute ist das unmodern, der Kinematograph ist unersättlich. Wenn solche Schaulust die Kinder erst einmal gepackt hat und sie die Ungebundenheit im Dreivierteldunkel gekostet haben, dann fällt es schwer, dieses Fieber zu dämpfen. Knaben unter 12, ja unter 10 Jahren machen hier ihre ersten Rauchversuche ungestört vom Personal […] Neulich war ich absichtlich zu einer Vorstellung lange vor Beginn gegangen. Drei Viertelstunden saß ich als einzelner Erwachsener in dem noch durch wenige Lampen erhellten Raum mit Dutzenden von Mädchen und Knaben, die sich ungestört unterhielten, ohne dass jemand vom Personal auch nur den Kopf hineingesteckt hätte. Da bin ich mir ganz klar darüber geworden, dass es für diese Schulkinder keine Geheimnisse mehr gibt und dass jedes Kind, das mit dieser Horde in Verbindung kommt, nach wenigen Besuchen verdorben wird. Und schließlich ist doch nicht nur in der Großstadt jedes Kind schon öfter im „Kintopp" gewesen."*[3]

Das zweite Beispiel zielt auf die die damals neuen Groschenhefte à la „Buffalo Bill", „Nick Carter, der Weltdetektiv" oder „Lustige Backfischstreiche", von deren verrohender, ja kriminalisierender Wirkung der Autor fest überzeugt ist.

> *„Ein Nutzen der Schundliteratur ist in keiner Richtung erkennbar. Vielmehr muß mit aller Bestimmtheit festgestellt werden, daß der Schaden, den sie anrichtet, unabsehbar ist. Nicht nur daß der Geschmack von Millionen rettungslos verdorben wird, auch ihre Sinne werden aufgereizt und zugleich abgestumpft. Schauen wir weiterhin tatenlos zu, so wird eine Generation heranwachsen, die keine größeren Vergnügungen kennt, als sich durch alle Verirrungen menschlicher Leidenschaften, durch alle Abgründe viehischer Grausamkeit und durch die ganze Schreckenskammer der abscheulichsten Verbrechen führen zu lassen."*[4]

Noch apokalyptischer gestimmt warnte 1910 der damals sehr populäre Berliner Publizist Richard Nordhausen vor den Folgen einer unkontrollierten Teilhabe der jungen Generation an den neuen Formen der urbanen Massenkultur, deren Folgen für ihn in dem Schreckbild einer kommenden Generation gipfeln, die der jetzt amtierenden buchstäblich das Messer an die Kehle setzen wird.

> *„Ohne Gott und Herrn führen die Unreifen ihr Leben. Keine Autorität wird anerkannt. Alle Genüsse der Reifen stehen auch den Minderjährigen zu, und in alle ihre Laster dürfen sie sich versenken […] In unseren großen Städten ziehen wir die Tartaren der Zukunft heran, die diese hochgepriesene Kultur zerstampfen werden. Wir rüsten mit Macht gegen äußere Feinde und ahnen nicht, daß unsere eigene Brut bereits das Messer wider uns erhebt."*[5]

Comics

Eine neue Stufe der Eskalation – oder vielleicht sollte man besser sagen: der Irritation – erfuhr die Debatte über die Gefährdung von Kindern und Jugendlichen und die Kontinuität unserer Kultur in den 1950er Jahren mit der Verbreitung der modernen Comics. Mit den Comics trat erstmals ein Medium auf den Plan, das sich durch einen spezifischen neuen Code auszeichnete. Die Kinder erlernten ihn spielerisch und schnell, den meisten Erwachsenen im Nachkriegsdeutschland blieb er dagegen zeitlebens unverständlich und ihre Reaktion zielte deshalb auf die Perhorreszierung des Mediums selbst, nicht nur bestimmter Inhalte.

> *„Die Comics sind eine Quelle allgemeinen Analphabetentums; sie schaffen eine Atmosphäre der Grausamkeit und des Abwegigen; sie vermitteln verbrecherische oder sexuell anomale Ideen; sie schwächen die natürlichen Kräfte, ein gesundes und anständiges Leben zu führen."*[6]

> *„Was die Atombombe der Welt antun kann, nämlich ihr Ende herbeiführen, das kann das Comic book der Welt der Literatur antun – nämlich das Lesen ausrotten."*[7]

Am Vorabend des Aufstiegs der digitalen Kindermedien bricht Anfang der 1980er Jahre nochmals eine besonders heftige Debatte los, die schließlich zu einer erneuten Verschärfung der Jugendschutzverordnungen führte. Diesmal geht es um die sogenannten *Horror-Videos*. Die Debatte ist auch deshalb interessant, weil sich in ihr eine Umkehrung der ursprünglichen Funktion des Kinderzimmers manifestiert. Früher war das Kinderzimmer ein vor dem Schmutz der Straße geschützter und elterlich kontrollierter Raum. So wurde etwa das Heimkino als medialer Schonraum gegen das öffentliche Kino propagiert. In der Videodebatte hat sich die Rolle des Kinderzimmers offensichtlich umgekehrt: Was bisher nur in Schmuddel- und Bahnhofskinos zu sehen war, überschwemmt nun per Videokassette die Kinderzimmer. Dieses Hauptargument in der Debatte ist aber

Abbildung 12: Titelstory (Der Spiegel, Nr. 11/12.3.1984)

nur dann schlüssig, wenn das Kinderzimmer zu einem unkontrollierten Terrain für kindlichen Medienkonsum geworden ist.

Die vorerst letzte Stufe: Digitalisierte Medien

Wir haben hier den Auftakt einer Debattenkonstellation, die in der Diskussion um die digitalisierten Medien insofern noch an Intensität gewonnen hat, weil hier das Problem kaum mehr zu kontrollierender Eigenwelten der Kinder- und Jugendlichen, ihre in der Regel weit überlegene Nutzerkompetenz und der geringe Erfolg herkömmlicher Zensurmaßnahmen nochmals an Dringlichkeit gewonnen haben.

Vorerst letzte Stufe: Mit den mobilen Handheld-Medien schließlich ist das Kinderzimmer in seiner neuen Funktion als unkontrollierter Medien-Freiraum ins Display gerutscht und mobil geworden.

> **Vergewaltigung, Enthauptung, Prügeleien, Verstümmelung ... Handy-Schock – wenn der Schulhof zum Horrorkino wird**
>
> *Die Bilder sind so schrecklich, menschenverachtend und ekelhaft, daß man ihren Anblick kaum ertragen kann. Menschen werden verstümmelt, vergewaltigt, enthauptet, eine Frau beim Sex mit einem Pferd gezeigt. Solche Bilder gab es auch früher schon. Sie wurden unter der Hand in schmuddeligen Sexshops und Porno-Kinos gehandelt, waren damit für Kinder und Jugendliche nahezu unerreichbar. Heute sehen 10-, 12- oder 15jährige Schüler solche Bilder jeden Tag auf ihrem Handy – und viele machen sich einen Spaß daraus, die Horrorfotos mit dem Mobiltelefon an Freunde weiter zu verschicken.*
>
> *Der Handy-Schock! Ein neuer Sex- und Gewalttrend an unseren Schulen erschüttert Eltern und Lehrer, beschäftigt mittlerweile auch Staatsanwälte.*[8]

Im Grunde begann schon mit dem *Walkman* Anfang der 1980er Jahre die Ära der mobilen Medien, mit denen quasi das Kinderzimmer als unkontrollierter Aktivitätsraum einerseits mobil und ständig verfügbar, andererseits aber für Eltern noch unzugänglicher wurde.

Schluss: Immaterialität der Medien

Ich möchte zum Schluss noch auf einen bisher nur wenig diskutierten Aspekt eingehen, bei dem das Fazit etwas weniger ratlos ausfällt.

Ein Nebeneffekt der Digitalisierung ist die fortschreitende Dematerialisierung der Hardware und ihrer Funktionen. Die Geräte können zwar alles, aber sie zeigen kaum noch anschauliche, nachvollziehbare Funktionsabläufe. Für das herkömmliche Technikverständnis und damit für einen nicht unwichtigen Teil der Weltaneignung bietet die digitale Technologie kaum noch Anschauungsmaterial. Ob die Einlassung mit der Welt der Algorithmen für die Mehrheit der Nutzer dagegen erfolgversprechend und kompensatorisch wäre, ist eine offene Frage. Im schlimmsten Fall könnte es zu einem eher magischen Weltverständnis nach der Art schlechter Science Fiction führen: „Plötzlich begannen irgendwo, tief im Innern des riesigen Rauschiffs mächtige Maschinen zu summen." Auf einen anderen diskussionswürdigen Aspekt hat kürzlich die Journalistin Elke Schmitter im *Spiegel* hingewiesen. Unter der programmatischen Überschrift „Dateien kann man nicht lieben" fragt sie, ob nicht die Immaterialität medialer Abspiel, Speicher- und Kopiervorgänge, also das Verschwinden ihrer Warenform auch das Verständnis und die Achtung von fremden Eigentum und Urheberansprüchen schwinden lässt.

Auch wenn die Guckkastenmedien mit den heutigen portablen Handheld-Medien ein neues Level erreicht haben, wenn sie dank der Digitalisierung praktisch alle anderen Speichermedien aufsaugen können, stärken gerade sie, so scheint es mir, durch ihre technische Künstlichkeit gleichzeitig das Bedürfnis nach den Rummelplatzmedien. Der totalen immateriellen Verfügbarkeit der Musik im Netz steht zum Beispiel eine neue Blüte der Live-Konzerte gegenüber. Die neun größten Freizeit- und Erlebnisparks in Westeuropa hatten 2010 mehr als 32 Mio. Besucher. Dazu kommen Messen mit Spielangeboten, Tourneen mit sensationellen Themenschauen, und selbst die Live-Animationen für Kinder im Urlaub sind zu Schlüsselangeboten der Tourismusbranche geworden. Möbelhäuser und Einkaufszentren locken mit Live-Events für Kinder. Und notfalls organisieren Jugendliche ihren Rummelplatz auch selbst – per Handy, Netz und iPad als *Blogger Party* oder *Games Convention*.

Es gibt kaum ein halbwegs erfolgreiches PC-Spiel, zu dem es nicht ein üppiges Angebot an analogen Spielfiguren gibt, keine populäre Medienfigur, bei der nicht versucht wird, einen möglichst umfangreichen Produktverbund daraus zu machen. Auch der Umsatz von konventionellem elektronischem Spielzeug steigt weiter von Jahr zu Jahr – trotz sinkender Kinderzahl. Für den Zeitschriftenhandel mussten spezielle Tröge entwickelt werden, um die derzeit weit über hundert verschiedenen Kinderzeitschriften präsentieren zu können, die vor allem über ihre Zugabespielzeuge – neudeutsch *Gimmicks* genannt – miteinander konkurrieren. Und selbst die Adventskalender werden mehr und mehr zu dreidimensionalen Baukästen. Die Sammelbilder-Aktion von Rewe mit dem Worldwide Fund for Nature (WWF) löste 2011 – also eineinhalb Jahrhunderte nach der Erfindung dieses Mediums – in Deutschland erneut einen regelrechten Sammelbilder-Hype aus, strapazierte die Nerven der Eltern sammelwütiger Kinder und sorgte dafür, dass 2012 kaum eine Lebensmittel-Kette ohne Sammelaktion auszukommen glaubte.

Der Boom solcher auf den Reiz des Anfassbaren, Haptischen spekulierender Produkte könnte auch eine kompensatorische Kehrseite der immer perfekteren Download-Kultur sein. Ob man nicht auch Algorithmen lieben kann, sei einmal dahingestellt. Aber ganz offensichtlich machen sie alleine nicht satt.

Anmerkungen

1 *Silke Tammen: Gewalt im Bilde. In: Gewalt im Mittelalter. München 2005, S. 317*
2 *Heinrich Zschokke: Eine Warnung vor den Gefahren der Lesesucht 1821*
3 *Walther Conrad: Kirche und Kinematograph. Eine Frage. Berlin 1910, S, 35*
4 *Ernst Schultze: Die Schundliteratur, 1911, S. 41*
5 *Richard Nordhausen in: Der Tag, Ausg. B, 15.8.1910*
6 *Richard Bamberger: Jugendlektüre. Wien 1965*
7 *Anonymus in: Jugendliteratur, 2. Jg./1956, Nr. 7, S. 349*
8 *Bild.de, http://www.bild.de/news/aktuell/news/por-no-alarm-schuelerhandys-252674.bild.html, 25.03.2006 (gekürzt)*

Anja Lorenz

Wie das Social Web Individuum und Gesellschaft verändert

Es heißt nicht grundlos New Media *oder mittlerweile* Social Media*: Die derzeitigen Möglichkeiten, die vor allem das Social Web mit sich bringt, eröffnen es nahezu jedem, sich an der Verbreitung von Informationen – passiv wie aktiv – zu beteiligen. Diese Partizipationsmöglichkeiten bringen fraglos positive Effekte, aber auch negative Phänomene zum Vorschein.*

Das Social Web als Medium: Eine Sammlung von (durchaus auch provozierten?) Missgeschicken

Die Verbreitung von Informationen lag lange Zeit in der Hand von wenigen Einzelnen: Verlage, Nachrichtenanstalten, die in den Webtechnologien kundigen Internetseitenbetreiber etc. Mittlerweile sind 76 % der Menschen in Deutschland online [1] und das nicht nur passiv: Immer mehr Internet-Nutzer stellen selbst Inhalte ins Netz. YouTube berichtete Mitte 2012 davon, dass pro Minute durchschnittlich 72h Videomaterial auf die Plattform geladen wird [2]. Auf Twitter werden am Tag eine halbe Milliarde Tweets verfasst [3]. So wird das Internet immer mehr vom *Medium für die Massen* zum *Medium von den Massen*, in denen jeder ohne größere Hindernisse Informationen verbreiten kann.

Und genau diese Möglichkeiten führen nicht nur zu den bekannten positiven Auswirkungen, wie beispielsweise die zunehmend breitere politische Mitbestimmung oder der freie Zugang zu Inhalten *(Open Access).* Es gibt auch eine Reihe bedenklicher Phänomene, für die man unter Buzzwords wie *Filterbubbles, Shitstorms, Informationsvandalismus* oder *Cybermobbing* zahlreiche Beispiele finden kann. So scheint es leicht zu sein, einer Berliner Straße den fiktiven Beinamen *Stalins Badezimmer* zu geben, obwohl sie diesen nie hatte [4]. Ebenso fanden falsche Fotos des Marsroboters *Curiosity* [5] oder vom Hurrikan *Sandy* in New York, die eigentlich aus dem Film *The Day after Tomorrow* [6] stammten, auf Twitter schnell Verbreitung. Neben diesen eher lustigen Anekdoten wird diese schnelle Informationsverbreitung spätestens dann bedenklich, wenn sie sich auf Kanäle ausweitet, denen wir bisher vertraut haben. So schrieb beispielsweise *Der Tagesspiegel:* „Nach dem Attentat von Denver: Machen sich Facebook-Verweigerer verdächtig? Der Attentäter war nicht bei Facebook aktiv. Forscher glauben, dass Online-Abstinenz auf Störungen hindeuten kann." [7] Näher betrachtet hatte die zitierte Studie aber kaum Beweiskraft für diese Behauptung [8]. Ein anderes Beispiel ist die ehemals geplante Forschungskooperation der Schufa mit dem Hasso-Plattner-Institut (HPI), bei der die Bonitätsbewertung anhand von Daten in sozialen Netzwerken untersucht werden sollte. Aufgrund immenser Kritik vor allem im Social Web [9] stoppte das Institut das geplante Projekt, das zweifelsohne mit einem nicht unerheblichen Drittmittelvolumen und nicht zuletzt der wissenschaftlichen Kontrolle und Veröffentlichung einer solchen Bewertung verbunden gewesen wäre.

Um ein Bild über die Ausprägungen dieser Phänomene zu erhalten, wurden in vorherigen Arbeiten unseres kleinen Projekts *Social Web Pathologies* wissenschaftliche Beiträge zu derartigen Phänomenen in einem Literaturreview zusammengetragen (eine Übersicht zu den Publikationen zusammen mit weiteren Informationen sowie Kontaktdaten ist auf der Linkliste zum Artikel zu finden: *http://www.diigo.com/list/anjalorenz/sowepafiff2012).* Auf der FIfF-Jahrestagung wurden im Rahmen eines Workshops Wahrnehmungen und Einschätzungen einiger Teilnehmer zu diesem Problempunkten diskutiert.

Wie werden die Tendenzen von FIfF-Mitgliedern und Tagungsteilnehmern gesehen? Hintergrund und Ergebnisse des Workshops *Neue LebensWelt-Krisen* auf der FIfF-Jahrestagung

Die Teilnehmer der FIfF-Jahrestagung standen unserer kritischen Betrachtungsweise des Social Webs sehr offen gegenüber – anders als auf anderen Konferenzen, bei denen diese Sichtweisen von einigen Personen als Angriff auf eigene Arbeitsweisen wahrgenommen werden. Daher war es für den Workshop besonders interessant, die Einschätzung der Tagungsteilnehmer zu bisherigen und vor allem zukünftigen Entwicklungen in Erfahrung zu bringen. Dies geschah mit Hilfe der Road-Mapping-Methode (bspw. beschrieben in [10]): Für die verschiedenen Domänen der systemischen Sozialforschung (Wirtschaft, Politik, Kultur und Soziales) wurden in einem ersten Teil wichtige Meilensteine und Schritte in der bisherigen Entwicklung an Thementischen gesammelt. In einem zweiten Teil wurden mögliche Folgen und zukünftige „Wege" zusammengetragen. Die Teilnehmer selbst rotierten dabei nach einer vorgegebenen Zeit, sodass möglichst jedes Thema von jedem Teilnehmer betrachtet werden konnte. Die folgenden Abbildungen und Aussagen entstammen die-

Anja Lorenz

Anja Lorenz ist wissenschaftliche Mitarbeiterin an der Professur Wirtschaftsinformatik der Technischen Universität Chemnitz sowie im eScience-Forschungsnetzwerk Sachsen. Neben ihrer Forschung zu digitalen Lernmaterialien und der kooperativen Arbeit insbesondere von Lehrenden mithilfe von Social Software hat sie zusammen mit Christian Schieder auch die potentiell negativen Auswirkungen des Lebens und Arbeitens im Social Web untersucht.

sem Workshop und werden zunächst unkommentiert vorgestellt. Motiviert durch den Workshop-Titel und die Fokussierung auf potentiell negative Phänomene im vorangegangenen Vortrag standen vor allem die negativen Phänomene im Verlauf des Workshops im Fokus.

Teil 1: Bisherige Entwicklungen

Die zusammengetragenen Beobachtungen zu bisherigen Entwicklungen unterschieden sich nicht wesentlich von denen, die in der Literatur oder mittlerweile auch in journalistischen Beiträgen zum Social Web zu finden sind (zudem leuchtet es ein, dass die Punkte, die zuvor in dem Vortrag zum Literaturreview genannt wurden, auch von den Workshop-Teilnehmern zumindest als erste Ansatzpunkte genannt wurden):

Das Volumen und die Beschleunigung des Informationsflusses sowie die zunehmende Unsicherheit und fehlende „Regeln" wurden mit verschiedenen Folgen für fast alle Bereiche festgestellt. Dabei scheint das Maß eine wichtige Rolle zu spielen: Die gleichen Eigenschaften von Kommunikationsmedien, die sie zu sehr effizienten und effektiven Werkzeugen machen, führen bei einer übermäßigen Ausschöpfung zu Problemen. So haben *in der Wirtschaft* zwar Internet, E-Mail und Soziale Netzwerke zu schnellen Kommunikationswegen und flexibler Gestaltung von Arbeitsplatz und -zeit geführt, die Informationsflut und die ständige Verfügbarkeit vermischen aber auch Arbeits- und Freizeit immer mehr, und der Druck, auch außerhalb der Bürozeiten auf Anrufe, E-Mails oder andere Anfragen zu reagieren, steigt (siehe Abbildung 1). Auch *in der Politik* bringen Social Media stärkere Transparenz und direktere Kommunikation mit den Wählern aber auch Manipulation, übersteigerte Selbstdarstellung und unkontrollierbare Reaktionen der Öffentlichkeit mit sich. Die Diskussionen um die Veränderungen *in der Kultur* zeigten, wie auch bei anderen Themen, dass sich die vier Bereiche nicht immer voneinander trennen lassen. So führt das verbreiterte Unterhaltungsangebot dazu, dass professionelle Schauspieler und Sänger jeden Abend nicht nur mit Kinofilmen und TV, sondern auch mit den „Amateuren" auf YouTube konkurrieren. Langjährige Ausbildung und qualitativ hochwertige Inszenierungen scheinen an Bedeutung zu verlieren, mehr noch: das breite Publikum scheint die Leistung professioneller Künstler kaum noch zu erkennen. Des Weiteren wurden an dieser Stelle die Einschränkung und Filterung des vermeintlich weit gefächerten Angebots durch Empfehlungen in sozialen Netzwerken (unter dem Stichwort *Filterbubble* bekannt) diskutiert. Bei den *Veränderungen des gesellschaftlichen Lebens* stand vor allem die potentiell größere Reichweite privater Informationen im Vordergrund (siehe Abbildung 2): Das Mobbing in Schulen ist auch schon vor den digitalen Kommunikationsmedien ein Problem gewesen, aber nun könnten auch Personen außerhalb der Klasse – vielleicht spätere Arbeitgeber – darüber in den sozialen Netzwerken lesen. Zu diesem Bereich wurden aber auch sehr viele positive Effekte genannt, wie kurze und schnelle Kommunikationswege, freie Informationen oder die scheinbare Gleichrangigkeit verschiedener Meinungen.

Teil 2: Zukünftige Entwicklungen

Nach einer Pause sollten die Teilnehmer Vermutungen über die Zukunft äußern, wobei zwischen utopischen, realistischen und dystopischen Entwicklungen unterschieden wurde. Zur besseren Lesbarkeit zeigt Tabelle 1 eine Übersicht der genannten Punkte aus dem Workshop.

Das Social Web wird *in der Wirtschaft* nach Einschätzung der Teilnehmer im besten Sinne zu Arbeitserleichterungen und zur Wahrnehmung der Arbeitnehmer als Mensch und Individuum führen. Als realistisch werden die gezielte Ansprache von Kunden und potenziellen Fachkräften sowie die Flexibilisierung der Arbeit durch zunehmende Mobilität, Office Sharing oder die Arbeit im Home Office genannt. Negative Tendenzen werden vor allem darin gesehen, dass Privat- und Arbeitsleben immer weniger voneinander getrennt werden können und der Druck auf Beschäftigte durch die permanente Erreichbarkeit steigt. „Wirtschaftsmobbing" (die Begriffe in Anführungszeichen entstammen der Diskussion und entsprechen eventuell nicht den in der Literatur auffindbaren Definitionen), also die gezielte Falschinformation zu Erfolgen und Konkurrenten über Social Media, könnten zunehmen und das mangelhafte Bewusstsein für die Konsequenzen scheinbar simpler Transaktionen könnte verstärkt zu Phänomenen wie „Bad Banking", also enthemmtem globalem Handel führen. Die Dominanz von „Big Playern" gegenüber kleineren

Abbildung 1: Bisherige Entwicklungen der Kommunikationsmedien im Bereich der Wirtschaft

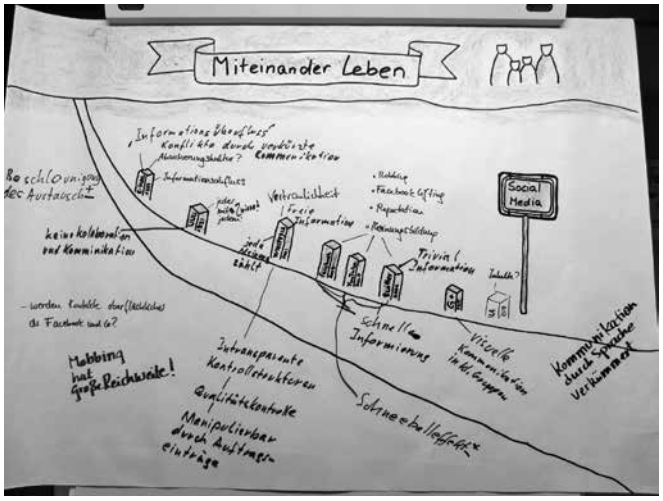


Abbildung 2: Bisherige Entwicklungen der Kommunikationsmedien im gesellschaftlichen Bereich

Domäne	Dystopie	Realität	Utopie
Wirtschaft	• [Chancen von] Big Player vs. Kleiner Einzelhandel; Lohndumping durch Vergleichbarkeit • Bad Banking: [Digital] enthemmter u. a. globaler Handel inkl. Bankenaufsicht • *Wirtschaftsmobbing*: Falschinformation via Social Media • Permanente Erreichbarkeit: Druck auf Beschäftigte • Privat- und Arbeitsleben sind nicht mehr getrennt	• Kundenanalyse → gezielte Ansprache • [Gezielte] Bewerberportale • Permanente Erreichbarkeit • Mobile Arbeit • Office Sharing • Home Office	• Anerkennung der Arbeitnehmer als Mensch • Permanente Erreichbarkeit • Arbeitserleichterung
Politik	• Zensur • Manipulation • Blende/Fassaden aufbauen • Überwachung und Folgen • Unüberschaubarkeit • Aufwand für Unabhängige und Nachwuchs	• Arabischer Frühling • Transparenz • Occupy Wallstreet • Politische Aktionen und Aufrufe	• Mitbestimmung • Austausch • Kein Parteizwang
Kultur	• Ausschluss von Sparten (vs. Boulevard) • Couchkultur • Ausbeutung von Nachwuchs → Arbeitsbedingungen der Etablierten • Lohndumping • Kürzung zugunsten von *Stars* • Hemmschwelle zur Kritik fehlt	• Bessere *Vergleichbarkeit* & [mehr] Konkurrenz, u. a. auch für die Bildung • Breites Bildungs- und Kulturangebot • Crowd Sourcing • Allgegenwärtige Diskussion um Geschmäcker	• Crowdfunding • Zeit- und ortsunabhängiger Zugriff auf Experten
Soziales	• Isolation • Gläserne Menschen • Mobbing • Verhaltensanpassung an gesellschaftliche Erwartungen • Abhängigkeit • Realitätsverlust • Totale Überwachung • Permanente Erreichbarkeit • Virtuelle Unsterblichkeit	• Weltweit arbeiten und leben • Globale Vernetzung • Digitale Auszeit	• Voll digitalisierter Haushalt

Tabelle 1: Einschätzungen zukünftiger Entwicklungen durch die Workshop-Teilnehmer

Unternehmern sowie Lohndumping aufgrund der Vergleichbarkeit der Arbeitskosten wurde ebenso den zukünftigen und potentiell negativen Entwicklungen zugeordnet. Derzeitige *politische Entwicklungen* lassen eine Häufung politischer Aktionen und Aufrufe durch Social Media, wie bei Occupy Wallstreet oder dem arabischen Frühling, erwarten (siehe Abbildung 3, S.42). Als positive Entwicklung sehen die Teilnehmer das Potential zur gesteigerten Transparenz, Mitbestimmung, den gegenseitigen Austausch und die Loslösung von Parteizwängen. Zensur, Manipulation, Fassadenmalerei, Überwachung, Verschleierung und die Einstiegshürden für unabhängige Positionen und den politischen Nachwuchs wurden dagegen als Schattenseiten genannt. Als utopische und realistische Entwicklungen *im kulturellen Bereich* wurden Crowdfunding/-sourcing, der schnelle und direkte Zugriff auf Experten, allgegenwärtige Diskussionen, bessere Vergleichsmöglichkeiten, aber auch die Vielzahl konkurrierender Angebote genannt (siehe Abbildung 4, S.42). Dagegen könnten Sparten immer weniger Chancen haben, sich gegen breite Trends durchzusetzen und weniger bekannte Künstler würden zugunsten von „Stars" keine Förderung erhalten. Der schnelle Zugriff auf verschiedene „Angebote" der Künstler könnte zudem zu einem gegenseitigen Preiskampf und damit zu einem immensen Lohndumping führen. Schließlich könnte das *gemeinschaftliche Leben* einerseits von der globalen Vernetzung und der weltweiten Verfügbarkeit profitieren, da das private Leben im Idealfall besser mit dem Arbeitsleben vereinbar wäre. Die vermehrte Verfügbarkeit auch privater Informationen im Social Web macht aus den Nutzern allerdings auch „gläserne Menschen", was eine Überwachung und die Verhaltensanpassung an gesellschaftliche Erwartungen fördern könnte. Zudem wirkt die permanente Erreichbarkeit nicht nur in das berufliche, sondern auch in das private Leben hinein.

Fazit

An dem Workshop nahmen acht Teilnehmer teil, die dabei sehr unterschiedliche Hintergründe mitbrachten: Neben wissenschaftlichen Mitarbeitern und dem Tagungsreferenten Professor Kuhlen waren auch Software-Entwickler, ein Journalist sowie

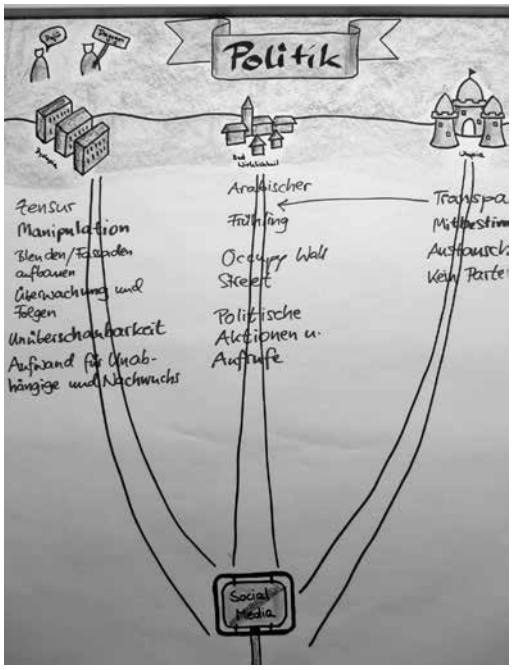


Abbildung 3: Zukünftige negative, realistische und positive Entwicklungen im Bereich der Politik

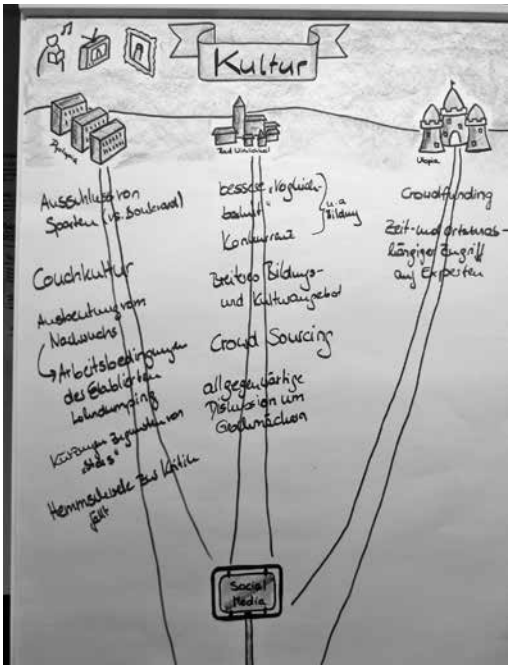


Abbildung 4: Zukünftige negative, realistische und positive Entwicklungen im Bereich der Kultur

eine Studentin am Workshop beteiligt. Damit sind die Ergebnisse zwar keinesfalls verallgemeinerbar, zeigen aber doch interessante Meinungen und unterschiedliche Facetten der Entwicklungen im Social Web auf.

Besonders auffällig war, dass bei der Diskussion zukünftiger Entwicklungen die Teilnehmer oft Schwierigkeiten hatten, die Phänomene einer utopischen oder dystopischen Perspektive zuzuordnen. Abhängig von Umsetzung, Maß und betrachtetem Personenkreis konnten die gleichen Entwicklungen sowohl positiv als auch negativ bewertet werden. Eben diese Zwiespältigkeit bestätigt aber nur die anfänglichen Beobachtungen zu den aktuellen Entwicklungen des Social Web, nämlich, dass neben den vielen positiven Auswirkungen des Social Web auch die (potenziell) negativen Phänomene im Auge behalten werden müssen.

Danksagung

Aufbau und Methodik des Workshops waren stark angelehnt an einen Teil des *Experten-Workshops L3T's Work* zur Zukunft von Lern- und Lehrmaterialien *(http://l3t.eu/zukunft/),* der im Mai/Juni 2012 in Bad Reichenhall stattfand. Ich danke besonders Sandra Schön (Mitorganisatorin von L3T's Work) sowie weiteren Workshop-erfahrenen Kollegen wie Ellen Trude, Ralf Appelt oder Oliver Tacke, die mir für die Vorbereitung des FIfF-Workshops wertvolle Hinweise gegeben hatten.

Referenzen

[1] *B. van Eimeren and B. Frees, „Ergebnisse der ARD/ZDF-Onlinestudie 2012: 76 Prozent der Deutschen online – neue Nutzungssituationen durch mobile Endgeräte", Media Perspektiven, vol. 7–8, pp. 362–379, 2012.*

[2] *YouTube Team, „It's YouTube's 7th birthday... and you've outdone yourselves, again", Broadcasting Ourselves ;): The official YouTube Blog, 2012. [Online]. Available: http://youtube-global.blogspot.de/2012/05/its-youtubes-7th-birthday-and-youve.html. [Accessed: 05-Jan-2013].*

[3] *D. Terdiman, „Report: Twitter hits half a billion tweets a day", CNET, 2012. [Online]. Available: http://news.cnet.com/8301-1023_3-57541566-93/report-twitter-hits-half-a-billion-tweets-a-day/. [Accessed: 05-Jan-2012].*

[4] *A. Kopietz, „Wikipedia: Wie ich Stalins Badezimmer erschuf", Berliner Zeitung, 24-Mar-2011. [Online]. Available: http://www.berlinonline.de/berliner-zeitung/berlin/337069/337070.php. [Accessed: 18-Aug-2011].*

[5] *T. Phillips, „Are those pictures of Mars from the Curiosity rover?", Is Twitter Wrong?, 2012. [Online]. Available: http://istwitterwrong.tumblr.com/post/29049627659/are-those-pictures-of-mars-from-the-curiosity-rover. [Accessed: 05-Jan-2013].*

[6] *@YourAnonNews, „The Statue of Liberty right now – pic.twitter.com/WaXBbZUc | #sandy", Twitter, 2012. [Online]. Available: https://twitter.com/YourAnonNews/statuses/262978471049973760. [Accessed: 05-Jan-2012].*

[7] *K. Schulze, „Nach dem Attentat von Denver: Machen sich Facebook-Verweigerer verdächtig?", Der Tagesspiegel, 2012. [Online]. Available: http://www.tagesspiegel.de/weltspiegel/nach-dem-attentat-von-denver-machen-sich-facebook-verweigerer-verdaechtig/6911648.html. [Accessed: 05-Jan-2012].*

[8] *D. Rettig, „Ballaballa – Warum sich Facebook-Verweigerer nicht verdächtig machen", Alltagsforschung.de, 2012. [Online]. Available: http://www.alltagsforschung.de/ballaballa-warum-sich-facebook-verweigerer-nicht-verdachtig-machen/. [Accessed: 05-Jan-2012].*

[9] *Tagesschau, „Nach massiver Kritik: Internet-Projekt der Schufa geplatzt", tagesschau.de, 2012. [Online]. Available: http://www.tagesschau.de/inland/schufa132.html. [Accessed: 05-Jan-2013].*

[10] *S. Schön and M. Ebner, „Die Zukunft von Lern- und Lehrmaterialien: Wettergebnisse bei zwölf ausgewählte Thesen zur Entwicklung in den nächsten 18 Monaten", bildungsforschung, vol. 9, no. 1, pp. 105–140, 2012.*

[11] *S. Schön and M. Ebner, „Die Zukunft von Lern- und Lehrmaterialien: Wettergebnisse bei zwölf ausgewählte Thesen zur Entwicklung in den nächsten 18 Monaten", bildungsforschung, vol. 9, no. 1, pp. 105–140, 2012.*

Jutta Weber

Automatisierte Verantwortungslosigkeit?

Kampfdrohnen als Mittel der High-Tech-Kriegsführung

Unter dem Begriff ‚Revolution of Military Affairs' (RMA)[1] *wurde und wird eine neue Doktrin der Kriegsführung propagiert, die in hohem Maße neue Entwicklungen der Informationstechnik und Informatik nutzt: satellitengestützte vernetzte Waffensysteme, so genannte Präzisionswaffen und ‚intelligente' Systeme wie lasergesteuerte Raketen und unbemannte, modulare Robotersysteme. RMA verheißt die Idee völlig transparenter Kriegsschauplätze jenseits des ‚fog of war', und er speist die Hoffnung auf punktgenau operierende, ferngelenkte und sogar (teil-) autonome ‚intelligente' Tötungssysteme sowie modulare Multi-Missionssysteme, die nicht nur schneller, billiger und flexibler sind als bisherige Systeme, sondern auch besser einsetzbar in der asymmetrischen Kriegsführung. Die neue Doktrin war und ist verbunden mit dem Fortschrittsversprechen, nicht nur die eigenen SoldatInnen vor dem Tod auf dem Schlachtfeld zu bewahren, sondern auch ZivilistInnen. Glaubt man dem Militär, fordert die chirurgisch operierende, ‚präzisere' High-Tech-Kriegsführung weniger Opfer. Doch welche Konsequenzen hat nun diese neue High-Tech-Kriegsführung und die mit ihr ermöglichte (Teil-)Automatisierung des Krieges? Was bedeutet es, wenn die physische wie psychologische Distanz zwischen den Gegnern wächst und SoldatInnen im sicheren und bequemen ‚control room' mit Hilfe ferngesteuerter Roboter auf einem tausende von Kilometern entfernten Schlachtfeld töten? Welche Logik unterliegt dieser ‚Revolution in Military Affairs' und der netzwerkzentrierten Kriegsführung? Ist es wirklich möglich, den ‚fog of war' aufzuheben oder erzeugt diese Kriegsführung neue Formen der alten Unübersichtlichkeit?*

Angesichts der Entwicklung von tele-operierten, aber auch autonomen Kampfdrohnen stellt sich die Frage, wie sich die militärischen, politischen und juristischen Szenarien ändern, wenn diese in den neuen – meist asymmetrischen – Kriegen zum Einsatz kommen. EthikerInnen, FriedensaktivistInnen und das Militär diskutieren bereits vehement, ob ein Einsatz dieser Technik überhaupt mit dem Völker- und Kriegsrecht vereinbar ist.[2] So arbeiten z. B. autonome *UCAVs (Unmanned combat air vehicle)* mit Objekterkennungssystemen, die mithilfe eines Freund-Feind-Erkennungssystems zunächst nur zwischen Angehörigen der eigenen Truppen und allen anderen unterscheiden können. Eine Unterscheidung zwischen SoldatInnen, sich ergebenden Soldaten und Zivilisten – eine zentrale Voraussetzung für die Einhaltung des Kriegsrechts – ist nicht möglich.

Jutta Weber, Fotos: FAI Fulda

Und wie steht es mit der Entwicklung *autonomer* Kampfdrohnen? Das Maß der Autonomie – auch bei bereits eingesetzten UCAVs – ist nicht einfach einzuschätzen. General Atomics gibt immerhin schon 2007 an, dass ihr MQ-9 Reaper im Besitz von "*robust sensors to automatically find, fix, track and target critical emerging time sensitive targets*" ist.[3] Aber es ist unklar, ob es bereits vollständig autonome Systeme gibt, deren Software auf der Grundlage von vorgegebenen Informationen und Determinanten Tötungsentscheidungen autonom ermöglicht. Angesichts der Vorgaben durch das Kriegs- und Völkerrecht betonen Militärs bis heute, dass es in letzter Instanz immer einen Menschen im Mensch-Maschine-System geben muss, welcher die letzte Entscheidung fällt:

> "*Because the DoD complies with the Law of Armed Conflict, there are many issues requiring resolution associated with the employment of weapons by an unmanned system. For a significant period into the future, the decision to pull a trigger or to launch a missile from an unmanned system will not be fully automated, but it will remain under the full control of a human operator.*"[4]

Diese Aussage lässt es aber wiederum wahrscheinlich erscheinen, dass mit der US-amerikanischen UCAV-Technologie bereits ein autonomer Einsatz möglich wäre. Nur die Frage der Legalität und die Diskussion um die Sicherheit stehen dem (offiziellen) Einsatz im Wege.

Das Interesse an autonomen und damit wesentlich schneller agierenden UCAVs erweckt den Verdacht, dass wir es mit einer (weiteren) Unterminierung des Kriegs- und Völkerrechts zu tun haben. Zudem treibt es ein Wettrüsten im Bereich der Militärrobotik an. Und selbst wenn es aktuell noch keine autonomen Kampfdrohnen gibt, so deuten die Absichtserklärungen des US-Amerikanischen Verteidigungsministeriums darauf hin, dass diese nicht mehr lange auf sich warten lassen werden:

> "*[i]n response to the Warfighter demand, the Department has continued to investigate aggressively in developing autonomous systems and technologies. That investment has seen unmanned systems turned from being primarily tele-operated, single-mission platforms to platforms into increasingly autonomous, multi-mission platforms. The fielding of increasingly sophisticated reconnaissance, targeting, and weapons delivery technology has not only allowed unmanned systems to participate in shortening 'the sensor-to-shooter kill chain', but it has also allowed them to complete the chain by delivering precision weapons on target.*"[5]

Wenn UCAVs mit Software ausgestattet werden, die selbsttätig über Zielerkennung und Zielzerstörung entscheidet, stellt sich die grundlegende Frage nach der Verantwortlichkeit von Kriegshandlungen: Wer hat den Tod von ZivilistInnen oder von sich ergebenden SoldatInnen zu verantworten, wenn es zu einem Fehlverhalten des Systems kommt? Angesichts dieser Entwicklung sehen viele EthikerInnen und FriedensforscherInnen das Kriegsrecht in Gefahr: "*If the nature of a weapon, or other means of war fighting, is such that it is typically impossible to identify or hold individuals responsible for the casualities that it causes then it is contrary to this important requirement of jus in bello.*"[6] Wenn die Verantwortlichkeit jedoch nicht mehr länger als zentrale Thematik gesehen wird, dann kann dies schwerwiegende Konsequenzen für die Art der Kriegsführung mit autonomen Waffensystemen (AWS) haben. Wie schon erwähnt, beharren US-Militärs angesichts der problematischen Völkerrechtsaspekte der neuen Technologie darauf, dass UCAVs nur unter menschlicher Beobachtung und Anweisung arbeiten dürfen.[7]

Nun fragt sich, warum autonome Systeme entwickelt werden, wenn man tatsächlich nur ferngesteuerte Systeme einsetzen möchte. Durch Automatisierung werden die Systeme massiv beschleunigt – eine ausgesprochen attraktive Vorstellung für MilitärstrategInnen: "*The vision is the USAF [United States Air Force; JW] postured to harness increasingly automated, modular, globally connected, and sustainable multi-mission unmanned systems resulting in a leaner, more adaptable, and efficient air force …*"[8] Konsequenterweise führt der Einsatz von automatischen Waffensystemen zur Aufrüstung auf der Gegenseite, zur Entwicklung von Anti-Robotik-Systemen und damit zu einer Spirale der Aufrüstung. Hier stellt sich die Frage, wann diese Entwicklungsspirale außer Kontrolle gerät.

Doch es gibt weitere Gründe für die Begehrlichkeit nach autonomen Kampfdrohnen. Bisher haben ferngesteuerte Systeme eine massive technische Schwachstelle: Sie sind von einer Kommunikationsinfrastruktur abhängig, die wiederum vom Feind angegriffen bzw. gehackt werden kann.[9] Jüngstes Beispiel hierfür ist das Abfangen einer US-amerikanischen Drohne auf dem Hoheitsgebiet des Iran durch dessen Streitkräfte im Dezember 2012. Im Kriegsfall ist es denkbar, dass gekaperte Waffen gegen eigene Truppen und ZivilistInnen gerichtet werden. Autonome Kampfdrohnen sind von einer angreifbaren Kommunikationsinfrastruktur weitgehend unabhängig.

Autonome Kampfdrohnen werfen nicht nur brisante völkerrechtliche Fragen auf. Sie führen auch zu einer problematischen Beschleunigung heutiger Kriegsführung, die die Chance, falsche Entscheidungen zurückzunehmen, erheblich einschränkt. Interessant ist, wie das Problem der Verantwortung beim Einsatz autonomer Waffensysteme diskutiert wird. Generell diskutieren EthikerInnen erst einmal darüber, ob die Verantwortlichkeit beim Programmierer bzw. bei der Programmiererin, bei der Maschine oder beim kommandierenden Offizier liegt. Da autonome Systeme durchaus auch so genanntes unvorhersehbares Verhalten an den Tag legen können, argumentieren manche, dass die Verantwortung für die Handlungen bei der Programmiererin bzw. beim Programmierer oder bei den Herstellern liegen sollte. Folgt man aber EU-Recht, können Hersteller, die angemessene Information über die Gebrauch und die Risiken ihrer Produkte – hier also der autonomen Waffen – zur Verfügung gestellt haben, nicht so leicht für etwaige Fehler zur Verantwortung gezogen werden – z. B. wenn das falsche Ziel zerstört wird. Auch bei einem als autonom konzipierten System kann die Programmierin nicht für eventuell negative Folgen verantwortlich gemacht werden, insofern das System dezidiert so ausgelegt war. Programmierer können rechtlich nur dann zur Verantwortung gezogen werden, wenn autonome Systeme international verboten würden, zum Beispiel durch einen Zusatz zur Genfer Konvention.[10]

Manche Autoren meinen auch, die autonome Maschine selbst verantwortlich machen zu müssen. Doch letztlich wird eine Maschine immer von Menschen programmiert bzw. vorprogrammiert. Diese legen die Parameter für Zielerkennung und Auswahl des Zerstörungs- bzw. Tötungszieles fest – insofern kann die Maschine nicht im buchstäblichen Sinne zur Verantwortung gezogen werden. Auch die Optionen für unvorhersehbares Handeln werden letztlich von menschlichen Programmierern angelegt.

Vor dem Hintergrund dieser Debatte beharrt das Militär auf der Verantwortung des kommandierenden Offiziers, wie man es schon im Falle von Langstreckenwaffen kennt. Dies ist eine unbefriedigende ‚Lösung' des Problems, da autonome Systeme ihre Ziele auf Basis ihrer einprogrammierten Parameter, Variablen und Kategorien berechnen. Das Handeln des autonomen Systems entzieht sich aber der Kontrolle des Offiziers, weshalb er schlecht für etwaige Folgen ‚unter seinem Kommando' verantwortlich gemacht werden kann.[11]

Angesicht der Tatsache der immensen ethischen und juristischen Probleme militärischer Roboter und ihrer möglichen Ächtung durch Internationales Humanitäres Recht fördern *US Army Research Office* und *US Office of Naval Research* Forschungsvorhaben über Ethik in Bezug auf militärische Roboter sowie an sogenannter ‚ethischer' Software.[12] Ronald Arkin beispielsweise, ein Robotiker am Georgia Institute of Technology, behauptet in Rahmen seiner vom Militär finanzierten Forschung, dass die zukünftigen Roboter ethischer seien als Menschen, da sie nicht von Emotionen oder Selbsterhaltungstrieben beeinflusst würden.[13] Im Rahmen des traditionellen Fortschrittsparadigmas argumentiert er, dass zukünftige Roboter ein besseres technisches Equipment hätten – wie beispielsweise bessere Sensoren, Prozessoren, Regeln und Gedächtnis – und somit besser entscheiden könnten, ob ein Ziel legitim oder illegitim sei. Er betont, dass Roboter nicht unter Erfüllungsdruck stünden (‚*scenario of fulfilment*'): Sie interpretierten ihren Input nicht entsprechend eines bestimmten Schemas, einer fixen Erwartung oder eines vorgegebenen Denkrahmens, glaubt man Arkin. Doch ist dies genau das Prinzip, nach dem Softwareprogramme arbeiten: nach vorgegebenen Schemata, Werten und Perspektiven, die, einmal einprogrammiert und in Aktion, nicht mehr hinterfragt werden. Sogar verhaltensbasierte Robotik, die (teilweise) auf Emergenz und die Kopplung von System und Umwelt baut, kommt nicht ohne Vorprogrammierung aus. Roboter sind nicht fähig, sich selbst, ihre Programmierung oder ihre Handlungen in Frage zu stellen, während Menschen dieses Potenzial prinzipiell durchaus besitzen. Arkin behauptet zwar nicht, dass Roboter perfekt werden, aber dass sie über den Menschen hinaus wachsen würden. Einem trivialen quantitativen Denkschemata folgend betont er, dass Roboter mehr Informationen in kürzerer Zeit bearbeiten können

und sie insofern mehr Zeit hätten, ihre Handlungen zu begründen.[14] Die dazugehörige Kompetenz wird einfach unterstellt.

Angesichts der massiven Verletzungen der Kriegsrechte unter Einsatz von High-Tech-Waffentechnologien während der ‚Operation Iraqi Freedom'[15] spricht sich Arkin für eine automatisierte Ethik aus: Um die mangelnde ethische Kompetenz der US-SoldatInnen auszugleichen und High-Tech-Kriegswaffen nicht in Frage stellen zu müssen, soll die Ethik automatisiert werden.

Darüber nachzudenken, was man tun muss, um Kriegsführung für Zivilisten und sich ergebende Aufständische sicherer zu machen, scheint völlig aus dem Blickfeld zu geraten. Diese Position basiert auf problematischen epistemologischen und ontologischen Argumenten. Beispielsweise nimmt es Arkin als selbstverständlich an, dass Robotersysteme wenigstens im Besitz genauso vieler Informationen wie Soldaten seien. Die Bedeutung von ‚Information' diskutiert er nicht, ebenso wenig, ob Information hier auch identisch mit Bedeutung, Wissen oder Verständnis ist. Er spricht zudem von Systemen, die unethischem Verhalten widerstehen und sogar erklären könnten, warum. Wenn dieser Widerstand von dem kommandierenden Offizier außer Kraft gesetzt würde, sei dieser verantwortlich für die folgenden Aktionen des Systems. Dieser Ansatz suggeriert entweder hoch intelligente Systeme, von denen jeder seriöse KI-Forscher zugibt, dass diese in den nächsten Jahrzehnten nicht realisiert werden können,[16] – oder aber dieser Mechanismus des Widerstandes arbeitet auf sehr reduktionistischem Level. Die dritte Annahme von Arkins Ansatz ist die Möglichkeit autonomer Waffensysteme, zwischen Soldaten, sich ergebenden Soldaten und Zivilisten zu unterscheiden – ein Ansatz, der genauso unrealistisch ist und dessen Realisierung bestenfalls in ferner Zukunft liegt.

Implizit nimmt Arkin ganz selbstverständlich an, dass jede mögliche komplexe Situation in Echtzeit formalisiert und errechnet werden kann – ein sehr altes Märchen der Künstlichen Intelligenz. Probleme der Navigation, Objekterkennung sowie das Problem der Maßstabgerechtheit (paralleles Errechnen vieler Verhaltensweisen in einem Problem) in komplexen realen Welten diskutiert er nicht. Diese Probleme der Robotik werden in naher Zukunft wohl nicht gelöst werden. Nichtsdestotrotz jedoch bringt Arkin im Bewusstsein dieser Problematiken vor, dass es einem System niemals möglich sein dürfte, tödliche Entscheidungen zu fällen, die nicht zuvor vollständig mit ethisch korrekten Vorschriften abgedeckt wurden. Aber wie geht man sicher, dass ein System die Regeln in den gegebenen Situationen auf die richtige Art und Weise anwendet?

Ein weiteres von Arkin gemiedenes Problem ist die formale Verifikation, das Problem der Möglichkeit von vehementen Softwarefehlern. Wie kann man sicher stellen, dass es keine Fehler in der Software autonomer Tötungssysteme gibt? Eine formale Verifikation von Software für Systeme so komplex wie die der Kampfroboter ist in Anbetracht knapper verfügbarer Zeit – wenn nicht sogar prinzipiell – unmöglich. Wie also kann jemand über ‚ethische' Kriegsroboter nachdenken? Die unkritische Diskussion über ethische Software für Killer-Roboter ruft den Eindruck hervor, dass es hier um die Legitimation und Akzeptanz problematischer Kriegstechnologien durch demokratische Staaten geht, nicht aber um das Lösen eines humanitären Problems, verursacht von hightech-automatisierter Kriegstechnik, die nicht nur eine Lebensgefahr für die Zivilbevölkerung darstellt, sondern auch die militärische Situation zwischen Gegenspielern destabilisiert. Durch den massiven Drohneneinsatz kommt es zu einem weiteren Wettrüsten, der Ausbreitung dieser Waffen und der Unterminierung des Völker- und Kriegsrechts.

Noel Sharkey, ein britischer Robotiker, verlangt dagegen mehr Verantwortungsgefühl seitens der InformatikerInnen und IngenieurInnen. Es sei deren Aufgabe, die ungelösten und profunden Probleme der militärischen Robotik sichtbar zu machen und an die Öffentlichkeit zu bringen. Sie sollten sich dem Sponsoring des Militärs entziehen und die Rettungsmärchen der Künstlichen Intelligenz kritisieren. Sharkey schreibt:

> *"Computer professionals and engineers have a duty to ensure that the funding bodies, policy makers and – if possible – end users know the current limitations of AI technology, including potential mishaps in the complexity of unpredictable real-world events. Do not be tempted to express your opinions or future predictions of AI as if the technology were already in place or just around the corner. The consequences of playing the funding game are too serious. Ultimately, we must ask if we are ready to leave life-or-death-decisions to robots too dim to be called stupid."*[17]

Traditionell vermeiden internationale professionelle Verbände wie IEEE oder ACM Themen, in denen Militärs und IngenieurInnen bzw. InformatikerInnen miteinander verwoben sind. Im ‚Code of Ethics' beispielsweise erklärt man sich verantwortlich für die eigenen IT-Systeme, Produkte und Artefakte und versichert, dass sie keine Gefahr für die Sicherheit des Wohlstandes der Gesellschaft darstellten. Der Code der ACM sagt sogar, *„when designing or implementing systems, computing profes-*

Jutta Weber

Dr. **Jutta Weber** ist Technikphilosophin und Professorin für Medienwissenschaften an der Universität Paderborn. Sie studierte Philosophie und Politikwissenschaft in München und Tübingen und forschte u. a. in Uppsala, Wien, Bremen und Lancaster. Ihre Arbeitsschwerpunkte sind Medien, Kultur & Gesellschaft; Technikforschung in der Informatik, KI und Robotik; Surveillance Studies sowie Gender Studies. Sie ist u. a. Mitglied der EU-Forschungsnetzwerks Living in Surveillance Societies (LISS) und des DFG-Graduiertenkollegs Automatismen.
www.juttaweber.eu

sionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare."[18]

Es scheint zu einfach, das Problem einer ethischen Lösung dieses komplexen Problems allein auf die Schultern der IngenieurInnen abzuwälzen (von Schomberg 2007). Und dennoch ist es nötig, diese Probleme zu diskutieren. Der ‚Code of Ethics' scheint hierfür nicht ausreichend zu sein. Bis heute ist das Feld autonomer Kampfsysteme von der Ethik im Allgemeinen gewissermaßen ignoriert worden, weswegen es wünschenswert wäre, wenn sich auch RobotikerInnen für eine zufriedenstellende, professionelle techno-ethische Regulierung dieses Feldes einsetzen würden.

Wir wissen, dass die Beurteilung von Technologie und Ethik effektive Mittel zur Konstruktion unserer technologischen Zukunft darstellt. Techno-ethische Analysen und Regulierungen können wichtige Instrumente der Mitgestaltung sein. Sie beeinflussen unter anderem zukünftige Entwicklungen und Forschungsstrategien und bereiten die legale Sicherheit der Forschung, der Entwicklung und der Kommerzialisierung neuer Produkte und Systeme vor.[19] Diese Aspekte sollten im Gedächtnis bleiben, gerade bezüglich der Diskussion um techno-ethische Thematiken.

In der Robotik – wie auch in vielen anderen Technowissenschaften – haben wir keine eindeutigen Grenzen zwischen dem technowissenschaftlichen, militärischen, ökonomischen und industriellen Komplex. Beispielsweise gibt es nur wenige US-Robotiklabore, die nicht direkt oder indirekt durch das US-Militär gesponsert sind. Dies ist auch ein Problem in Europa, wenn dort der militärische Einfluss (bisher) auch geringer ist.

Die politischen und ethischen Probleme der UCAVs hängen auf das Engste mit der Frage der Waffenkontrolle zusammen. Man könnte meinen, dass Waffenkontrolle seit Ende des Kalten Krieges in 1989 von geringerer Bedeutung sei, aber nach einem kurzen Rückgang militärischer Ausgaben für Forschung und Entwicklung sind diese seit Mitte der 1990er wieder rasant gestiegen – vor allem in den USA. Das US-Militärbudget umfasst derzeit nahezu die Hälfte aller weltweiten militärischen Investitionen, nachdem es zwischen 2000 bis 2008 durch die Bush-Administration eine Verdopplung erfahren hat.[20]

Während der Präsidentschaft von Barack Obama wurde das Budget des US-Militärs nicht radikal gesenkt.[21] Im Fiskaljahr 2009 hat der US-Kongress ursprünglich nur für ‚zukünftige Kampfsysteme' (FCS) allein 3.6 Milliarden Dollar bewilligt (Washington Post, 13.10.2008). Mittlerweile wurden die FCS abgelehnt, jedoch wurde die Forschung an Sensoren, an unbemannten Luft- und Bodenfahrzeugen, an *Non-Line-of-Sight Launch Systems* und an modifizierten FCF-Netzwerken zur *New Army Brigade Combat Team Modernization Strategy* umgelegt.[22]

Auf ökonomischer Ebene werden die UCAVs als Schlüsseltechnologie für den zukünftigen globalen Markt betrachtet. Die USA hat ihre MQ-UCAVs bereits an Frankreich, Italien und weitere Länder verkauft und werden sie weiter verkaufen. Mehrere Milliarden Dollar haben die USA jährlich in ihre Drohnen investiert. Beispielsweise kosten die erwähnten MQ-9 Reaper-Systeme mit jeweils vier Luftfahrzeugen ca. 70 Millionen Dollar. Experten schätzen, dass ab 2015 jährlich für ungefähr 5 Milliarden Dollar UCAVs ver- und gekauft werden.[23] In Anbetracht der massiven techno-ethischen Probleme sollte Europa eine präventive Waffenkontrolle von Drohnen einführen, die die Entwicklung dieses Marktes reguliert, ein Wettrüsten verhindert und der damit auch steigenden Zahl der Zivilopfer entgegenwirkt. Stattdessen argumentiert der deutsche Verteidigungsminister mit der angeblichen ethischen Neutralität und der höheren Präszision, um den möglichen Erwerb der Reaper-Kampfdrohnen durch die deutsche Bundesregierung voranzutreiben.

Unklar ist auch, ob Robotersysteme unter die bereits existierenden Kategorien der Waffenkontrolle fallen. Jürgen Altmann beschreibt dieses Problem der UCAVs im Hinblick auf den *Conventional Forces in Europe Treaty* wie folgt:

> *"The Treaty on Conventional Armed Forces of 1990 limits the holdings in five major weapons classes for the NATO member states and Russia; its definitions of battle tanks, armoured combat vehicles, artillery, combat aircraft and attack helicopters intentionally do not mention personnel on board, so that crewless versions would fall under the same rubrics, would count in the national holdings, would have to be notified to the Treaty partners, would be subject to inspection etc. However, one can foresee a debate which types of armed UAVs would constitute a combat aircraft. Whereas the definition is quite general, arguments might be made that converted surveillance drones or very small crewless aircraft do not fall under this heading. The situation with respect to 'combat helicopters' is similar. […] Thus, a grey area of uncounted and unlimited combat systems might develop. A fundamental problem is that similar limitations of conventional armaments are not in force in other continents."*[24]

Eine der größten Gefahren dieser autonomen Kampfsysteme ist, dass sie den Kriegseinstieg erleichtern. In den westlichen Demokratien müssen PolitikerInnen Überzeugungsarbeit leisten, um einen Krieg gesellschaftlich akzeptabel zu machen. Das könnte sich ändern, wenn Krieg glaubhaft als vollautomatisierte und für ZivilistInnen ungefährliche Aktion dargestellt werden kann.

Interessante Fragen stellen auch Philosophen wie Paul Virilio oder Friedrich Kittler, die danach fragen, wie sich unser Selbstverständnis und die Beziehung zwischen Menschen und Maschinen im Allgemeinen ändern werden, wenn Waffensysteme ihre Ziele und deren Vernichtung (Menschen eingeschlossen) selbst bestimmen. Die Autonomie von Waffensystemen bringt eine (weitere) Depersonalisierung und Anonymisierung von Macht und Kontrolle mit sich. Autonome Waffensysteme könnten, so argumentieren Virilio und Kittler, den Status von Subjekten erwerben, da sie schließlich die Instanzen darstellen würden, die die Macht verkörpern.[25] Dies würde eine deutliche Umverteilung der Macht zwischen Menschen und Maschinen bedeuten und den letzteren tatsächlich den Autonomiestatus verleihen.

Eine genauere Analyse dieser komplexen und bedrohlichen Prozesse ist dringend nötig. Eine interdisziplinäre Wissenschafts- und Technikforschung sollte die Konsequenzen und ungewollten Nebeneffekte dieser Technologien, ihre soziotechnische und politische Dimension herausarbeiten. Gleichzeitig gilt es, sich für

ein Moratorium aller Kampfdrohnen und einen Bann autonomer Waffensysteme einzusetzen.

Eine ausführlichere Fassung dieses Beitrags erscheint unter dem Titel ‚Autonome tötende Maschinen' in dem Band ‚Autonome Automaten. Künstliche Körper und artifizielle Agenten in der technisierten Gesellschaft', hg. von Jochen Bung, Malte Gruber und Sascha Ziemann, Band 12 der Beiträge zur Rechts-, Gesellschafts- und Kulturkritik, Berlin: trafo Verlag 2013 (im Druck).

Anmerkungen

1 *Cohen, Eliot A. (1996): A Revolution in Warfare, in: Foreign Affairs 95, Nr. 2, 1996, S. 37-54;*
Tilford Jr., Earl H. (1995): The Revolution in Military Affairs: Prospects and Cautions, Carlisle Barracks;
Kaufmann, S. (2006). Land Warrior. The Reconfiguration of the Soldier in the 'Information Age'. Science, Technology and Innovation Studies, 2 (Nov. 2006), 81-102

2 *Blackmore, Tim (2005). War X. Toronto: University of Toronto Press;*
Sparrow, R. (2007). Killer Robots. Journal of Applied Philosophy, 24(1), 62-77;
Kaplan, Caren (2008). 'Everything is Connected': Aerial Perspectives, the 'Revolution in Military Affairs,' and Digital Culture. Proceedings of the "Electronic Techtonics: Thinking at the Interface Conference" (pp. 130-139). HASTAC, Lulu Press;
Asaro, P. (2008). How Just Could a Robot War Be? In P. Brey, A.Briggle, & K. Waelbers (Eds.), Current Issues in Computing And Philosophy. Amsterdam: IOS Publishers;
Weber, Jutta (2010). Armchair Warfare 'on Terrorism'. On Robots, Targeted Assassinations and Strategic Violations of International Law. In: Jordi Vallverdú (ed.): Thinking Machines and the Philosophy of Computer Science: Concepts and Principles, IGI Global, 206-222

3 *General Atomics. (2007). MQ-9 Reaper. Predator-B Hunter-Killer UAV. Quelle (14.10.2009): www.defense-update.com/products/p/predatorB.htm*

4 *Department of Defense (2009). Unmanned Systems Integrated Roadmap, 2009-2034. Quelle (14.10.2009): www.acq.osd.mil/uas/docs/UMSIntegratedRoadmap2009.pdf*

5 *ebd. [18]*

6 *Sparrow, R (2007); siehe oben*

7 *Marsiske, H.-A. (2007), An der langen Leine. Roboter im Sicherheitsdienst. c't – magazin für computertechnik, 9.*

8 *United States Air Force. (2009). Unmanned Aircraft Systems Flight Plan 2009-2047. Unclassified. Updated version. Washington, DC: Author. Quelle (10.12.2009): www.govexec.com/pdfs/072309kp1.pdf*

9 *Altmann, J. (2003). Roboter für den Krieg? Wissenschaft und Frieden, 21(3), 18-22;*
Weber, J. (2009). Robotic Warfare, Human Rights & the Rhetorics of Ethical Machines. In R. Capurro & M. Nagenborg (Eds.), Ethics and Robotics, (pp. 83-103). Heidelberg, Germany: AKA, Amsterdam: IOS Press

10 *Nagenborg, M., Capurro, R., Weber, J. & Pingel, C. (2007). Ethical Regulations on Robotics in Europe. AI & Society, (pp. 349-366)*

11 *Sparrow, R. (2007). 71, siehe oben*

12 *Arkin, R. (2007). Governing Lethal Behaviour: Embedding Ethics in a Hybrid/Deliberative/Reactive Robot Architecture. Mobile Robot Laboratory, College of Computing, Georgia Institute of Technology. Retrieved October 14, 2009, Quelle www.cc.gatech.edu/ai/robot-lab/online-publications/formalizationv35.pdf;*
Canning, J. S. (2006). Concept of Operations for Armed Autonomous Systems. The Difference between 'Winning the War' and 'Winning the Peace'. Retrieved October 14, 2007, Quelle www.dtic.mil/ndia/2006disruptive_tech/canning.pdf;
Lin, P., Bekey, G. & Abney, K. (2009). Robots in War. Issues of Risk and Ethics. In R. Capurro, & M. Nagenborg (eds.), Ethics and Robotics, (pp. 49-68). Amsterdam: AKA / IOS Press

13 *Arkin, R. (2008). On the Ethical Quandaries of a Practicing Roboticist: A first-hand Look. Retrieved October 14, 2009, Quelle www.cc.gatech.edu/ai/robot-lab/online-publications/ArkinEthicalv2.pdf*

14 *Arkin R. (2007). 6f, siehe oben*

15 *Surgeon General's Office. (2006). Mental Health Advisory Team (MHAT) IV Operation Iraqi Freedom 05-07, Final Report, Nov. 17, 2006. Retrieved October 14, 2009, Quelle http://www.house.gov/delahunt/ptsd.pdf*

16 *Sharkey, N. (2007). Automated Killers and the Computing Profession. Computer, 40 (11), 124, 122-123;*
Tamburrini, G. (2009). Robot Ethics: A View from the Philosophy of Science. In R. Capurro & M. Nagenborg (Eds.), Ethics and Robotics, (pp. 11-22). Amsterdam: IOS Press

17 *Sharkey, N. (2007). ebd.*

18 *ACM Code of Ethics and Professional Conduct 1992, 1*

19 *Schaper-Rinkel, P. (2006). Governance von Zukunftsversprechen: Zur politischen Ökonomie der Nanotechnologie. PROKLA 145 "Ökonomie der Technik", 36(4), 473-496*

20 *Kumar Behera, L. (2008). The US Defence Budget for 2008. IDSA strategic comments. Quelle (14.10.2009): www.idsa.in/publications/stratcomments/LaxmanBehera210207.htm*

21 *Mayer, J. (2009, October 26). The Predator War. What Are the Risks of the CIA's Covert Drone program? The New Yorker, (pp. 36-45)*

22 *www.fcs.army.mil*

23 *Nikolei, H.-H. (2005). Milliardenmarkt Drohnen. Retrieved January 1, 2006*
Quelle www.n-tv.de/544984.html

24 *Altmann, J. (2009). Preventive Arms Control for Uninhabited Military Vehicles. In R. Capurro, & M. Nagenborg (Eds.), Ethics and Robotics, (pp. 69-82). Amsterdam: IOS Press, 74–75*

25 *Kittler, F. (1988). Signal-Rausch-Abstand. In H. U. Gumbrecht, & K. L. Pfeiffer (eds.), Materialität der Kommunikation, (pp. 342-359). Frankfurt a.M., Germany: Suhrkamp;*
Virilio, P. (2000). Strategy of Deception, (Transl. by C. Turner). New York: Verso

Rainer Kuhlen

Was haben *Eigentum* und *Wissenschaftsfreiheit* mit dem Urheberrecht zu tun?

Mit Reförmchen ist es nicht länger getan[1]

Eigentum und Wissenschaftsfreiheit sind zweifellos unaufgebbare Grundrechte. Zweifelhaft aber, ob sie über das Urheberrecht verteidigt werden müssen. Inhalt und Schranken dieser Rechte müssen jeweils als sozial konstruiert durch positive Gesetze bestimmt werden. Faktisch ist das Urheberrecht in den letzten 20 Jahren eher ein Handelsrecht geworden, bei dem vor allem die Interessen der kommerziellen Verwertung durch die Informations-/Verlagswirtschaft verfolgt werden, weniger der Nutzen für die einzelnen Menschen bzw. für Wirtschaft, Gesellschaft und Kultur: Das trifft auch und besonders für die Bereiche Bildung und Wissenschaft (BuW) zu.

Auch wenn seit 2005 offiziell als politisches Ziel die Bildung eines bildungs- und wissenschaftsfreundlichen Urheberrechts gilt, ist das Urheberrecht seitdem doch eher ein BuW behinderndes Recht geworden. Ein weiteres Basteln an den vielen, BuW einschränkenden Schrankenregelungen scheint kaum noch Sinn zu machen. Daher wird aus der Wissenschaft, vom Aktionsbündnis Urheberrecht für Bildung und Wissenschaft und von den Wissenschaftsorganisationen sowie der Kulturministerkonferenz eine umfassende Bildungs- und Wissenschaftsklausel angemahnt. Bislang verweigert sich die Regierungspolitik dieser Forderung, auch wenn die im Bundestag vertretenen Parteien sich dem immer mehr annähern. Die Ziele einer solchen umfassenden Klausel werden dargestellt. Am Ende werden einige Perspektiven mit der zentralen These aufgezeigt, dass kommerzielle Geschäftsmodelle nur über informationelle Mehrwerte, nicht über die Informationsobjekte selbst möglich sein werden, und nur wenn auf den wissenschaftlichen Informationsmärkten grundsätzlich die freie Verfügbarkeit von Wissen und Information als Gemeingüter (*Commons*) anerkannt ist.

Soziale Konstruktion von Eigentum und Wissenschaftsfreiheit

Das gegenwärtige Urheberrecht begründet sich weitgehend über das Konzept des geistigen Eigentums der UrheberInnen, ohne dass bislang systematisch zufriedenstellend geklärt ist, ob und wie *Eigentum* auf immaterielle Objekte, die Wissen und Information repräsentieren, übertragen werden kann. Es darf also durchaus die Frage gestellt werden, ob *Eigentum* ein angemessenes Konzept zur Begründung des Urheberrechts sein muss, zumindest was den exklusiven Anspruch von Eigentum angeht. Es macht eher Sinn, anstatt des bislang in der europäischen und deutschen Tradition überwiegend dogmatischen, quasi naturrechtlichen Verständnisses von Eigentum, ein funktionales zur Geltung zu bringen.

Die funktionale Sicht auf Eigentum bzw. auf den Schutz des Eigentums durch das Copyright wird klassisch durch die Formulierung der US-amerikanischen Verfassung ausgedrückt: "To promote the Progress of Science and the Usefuls Art"[2]. Im deutschen Grundgesetz wird zumindest die Primäraussage „Das Eigentum und das Erbrecht werden gewährleistet" relativiert durch die folgenden beiden Sätze „Eigentum verpflichtet. Sein Gebrauch soll zugleich dem Wohle der Allgemeinheit dienen." Der reale Eigentumsanspruch ist ein soziales Konstrukt und kein Naturereignis. Und Jeffersons Verständnis "[...] this [giving exclusive rights] may or may not be done, according to the will and

convenience of the society"[3] ist im Grunde immer noch auch für die gegenwärtige Gesetzgebung bestimmend.

Erinnert sei nur an die an Jefferson erinnernde Aussage von *Carlo Schmid* im Ausschuss für Grundsatzfragen des Parlamentarischen Rates, in dem 1948 das deutsche Grundgesetz gezimmert wurde: „Die Formulierung [‚Inhalt und Schranken werden durch die Gesetze bestimmt' – Satz 2 von Art. 14 Abs. 1] solle den Gedanken zum Ausdruck bringen, es gebe keine aus der Natur fließende Definition des Inhalts des Eigentums, und das Eigentum, nämlich konkret das Ausmaß, in dem ein Individuum über Sachen verfügen könne, und was es bedeute, ein eigentümliches Recht an einer Sache zu haben, sei notwendig vom Gesetzgeber her zu bestimmen."[4]

Der Eigentumsschutz in Art. 14, Abs. 1 GG ist unverrückbar, ebenso allerdings auch dessen zitierte Einschränkung in Abs. 2 mit dem Gebot der Sozialpflichtigkeit von Eigentum. Wie jeder Artikel im Grundgesetz bedarf es der Ausführungsbestimmungen in positiven Gesetzen, in diesem Fall von Gesetzen wie dem Urheberrecht oder dem Patentrecht. Der Staat kann in keinem Fall das Recht auf Eigentum und den Schutz dieses Eigentums gänzlich verweigern oder gar aus dem Rechtekanon streichen. Diese Garantie ist aber kein unbedingter Freibrief auf jede auch nur denkbare Verwertungsmöglichkeit. Wegen der Sozialbindung auch des geistigen Eigentums ist von der Gesetzgebung keine allumfassende Verwertungszusicherung einzuräumen. Wenn eine Verwertungsform die sozialen Belange der Nutzung von publizierten Werken so weit einschränken würde, dass von einem Nutzen für die Allgemeinheit (Gemeinwohl-Postulat) nicht mehr oder nur noch sehr eingeschränkt die Rede sein kann, kann eine solche Verwertungsform vor dem Grundgesetz nicht standhalten.

Nach BVerfG müssen Inhalt und Schranken des Eigentums erst durch das Gesetz selbst bestimmt werden. Einen *vorgegebenen und absoluten Begriff des Eigentums* gibt es nicht. In der Formulierung des Bundesverfassungsgerichts: „Inhalt und Funktion des Eigentums sind der Anpassung an die gesellschaftlichen und wirtschaftlichen Verhältnisse fähig und bedürftig."[5] Der Gesetzgeber hat an sich einen großen Spielraum zwischen der Institutsgarantie des Eigentums und der Sozialbindung des Eigentums nach Art. 14 Abs. 2 GG. Im Ausgleich der Eigentümerinteressen mit dem Wohl der Allgemeinheit liegt laut Bundesverfassungsgericht „die Absage an eine Eigentumsordnung, in der das Individualinteresse den unbedingten Vorrang vor den Interessen der Gemeinschaft hat."[6] Erweiterte Spielräume gibt es für den Gesetzgeber auch bei der Interpretation und Regelung von Wissenschaftsfreiheit bzw. positiver und negativer Publikationsfreiheit.

All das ist aber in den letzten 20 Jahren lediglich Theorie geworden. Seit gut 20 Jahren stehen beim Urheberrecht das Individualinteresse und das Interesse der kommerziellen Verwertung im Vordergrund. Nicht zuletzt auch hat die EU über ihre Richtlinie einer anderen Funktionalisierung von geistigem Eigentum Vorschub geleistet. In Erwägungsgrund 1 der EU Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums 2004 heißt es: „[…] es muss ein Umfeld geschaffen werden, das Innovationen und Investitionen begünstigt. Vor diesem Hintergrund ist der Schutz geistigen Eigentums ein wesentliches Kriterium für den Erfolg des Binnenmarkts. Der Schutz geistigen Eigentums ist nicht nur für die Förderung von Innovation und kreativem Schaffen wichtig, sondern auch für die Entwicklung des Arbeitsmarktes und die Verbesserung der Wettbewerbsfähigkeit."[7]

Muss das so sein? Ich denke nein. Das Urheberrecht könnte gut ohne Rekurs auf geistiges Eigentum auskommen. Bezeichnenderweise kommt im Urheberrechtsgesetz *geistiges Eigentum* auch nicht vor. Von *Eigentümer* wird nur gesprochen, wenn der Besitzer eines Werkes gemeint ist.[8] Das Recht spricht im Übrigen von Rechten. Aber schützt das Urheberrecht wirklich noch in erster Linie die Rechte der UrheberInnen (geschweige denn das der NutzerInnen)?

Zwar schützt das Urheberrecht nach dem Wortlaut des Gesetzes weiterhin die Persönlichkeits- und Verwertungsrechte der UrheberInnen. Faktisch ist das Urheberrecht aber längst ein Handelsrecht geworden, bei dem vor allem die Interessen der kommerziellen Verwertung durch die Informations-/Verlagswirtschaft geschützt im Vordergrund stehen, weniger der Nutzen für die einzelnen Menschen bzw. für Wirtschaft, Gesellschaft und Kultur. Groteskerweise wird auch für das Resultat der kommerziellen Verwertung der Eigentumsbegriff ins Spiel gebracht, obgleich Verwerter ja keineswegs neues *Intellektuelles* geschaffen haben und entsprechend nach dem Gesetz auch über keine Verwertungsrechte verfügen, sondern nur über Nutzungsrechte, die sie per Vertrag von den für das *Intellektuelle* zuständigen UrheberInnen erworben haben. *Geistiges Eigentum* ist daher tatsächlich eher ein ideologischer *Kampfbegriff* (Hoeren)[9] geworden, durch den heute faktisch weniger die Autorenrechte behauptet werden, sondern die ihrer Verleger.

Es fragt sich also, ob nicht ein umfassender Wandel für die Regulierung von Wissen und Information erforderlich ist. Reichten für die Wahrnehmung der Rechte der UrheberInnen nicht deren Persönlichkeitsrechte aus? Und muss die Verwertung überhaupt über das Urheberrecht geregelt werden? Sollte das bisherige, durch den Dreistufentest festgeschriebene Dogma nicht auf den Kopf gestellt werden, so dass nicht mehr die kommerzielle Verwertung der Default-Wert und die Einschränkung der exklusiven Verwertungs-/Nutzungsrechte nur die stark zu begründenden Ausnahmen sind, sondern genau umgekehrt: die freizügige Nutzung der Regelfall im Interesse individueller, kultureller und gesellschaftlicher Entwicklung, und die kommerzielle Nutzung der besonders zu begründende Ausnahmefall?

Das weitere Basteln an einzelnen Regelungen im Urheberrecht macht kaum noch Sinn – das zeigen deutlich die kaum verständlichen, kaum nutzbaren und nicht nützlichen Schrankenregelungen, die an sich den NutzerInnen zugute kommen sollten.

Das, was für geistiges Eigentum gilt, trifft auch für Wissenschaftsfreiheit zu. Niemand kann und wird diese absolut in Frage stellen, schon gar nicht die Anerkennung der Urheberschaft, aber ist für Wissenschaftsfreiheit die absolute Verfügung über die erstellten Werke zwingend? Der Bundesgerichtshof, anlässlich der Abschaffung des Hochschullehrerprivilegs 2002 durch Änderung des Arbeitnehmererfindergesetzes, hat deutlich gemacht, dass die „Freiheit von Forschung und Lehre … es allerdings nicht [gebietet], dass der Hochschullehrer auch Inhaber der Verwertungsrechte an seinen Forschungsergebnissen zu sein oder zu bleiben hat". „Die wirtschaftliche Zuordnung von geistigen Leistungen des Hochschullehrers fällt in den Normbereich des Art. 14 Abs. 1 Satz 1 GG, nicht des Art. 5 Abs. 3 GG"[10]:

„Das Grundrecht der freien wissenschaftlichen Betätigung [müsse] soweit unangetastet [bleiben], wie das unter Berücksichtigung der anderen legitimen Aufgaben der Wissenschaftseinrichtungen und der Grundrechte der verschiedenen Beteiligten möglich ist". Zu diesen Aufgaben, für deren Einhaltung der Staat auch zu sorgen habe, gehört auch die „Mittelaufbringung der Hochschule". „Der Funktionsfähigkeit der Institutionen des Wissenschaftsbetriebs [komme auch] Verfassungsrang zu". „Die grundrechtlich garantierte Freiheit von Forschung und Lehre erfordert nicht, dass den Forschern an Hochschulen die unbeschränkte Rechtsinhaberschaft an ihren dienstlich gemachten Forschungsergebnissen eingeräumt werden müsste …"[11].

Wissenschaftsfreundliches Urheberrecht

Zurück zum Urheberrecht: 2005 schien sich so etwas wie ein Wissenschaftsurheberrecht anzudeuten: Im Koalitionsvertrag der Regierungsparteien vom 11.11.2005 fand sich der Satz: „Wir wollen ein bildungs- und wissenschaftsfreundliches Urheberrecht." Was sich aber durch die *Reformen* im Ersten Korb (wirksam 2003) und dann im Zweiten Korb (wirksam 2008) über Paragraphen wie 52a (Bildungs- und Wissenschaftsschranke), 52b (eLeseplätze in Bibliotheken), 53 (Nutzung zum eigenen Gebrauch), 53a (Kopienversand auf Bestellung), 31a (Unbekannte Nutzungsarten), 38 (unverändert seit 1965: Zweitverwertungsrecht) sowie 95a und b (Einsatz technischer Schutzmaßnahmen – DRM) im Gesetz „zugunsten" Bildung und Wissenschaft wiederfand, ist, um es vorsichtig zu sagen, unzulänglich, verwirrend und nicht fair. Oder in den Worten der jetzigen Bundesjustiz-

ministerin Leutheusser-Schnarrenberger: „So haben die letzten gesetzlichen Änderungen zwischen 1998 und 2009 zu erheblichen Verkomplizierungen am Text des Urheberrechtsgesetzes und deutlichen Akzeptanzproblemen geführt.“[12]

So ähnlich hatte es allerdings auch schon der Bundestag 2007 bei der Verabschiedung des Zweiten Korbs gesehen und hatte einen Dritten Korb angemahnt, der nach dem Willen von Bundestag und Bundesrat ein Wissenschaftskorb werden sollte. Diesen hat es jedoch bis Ende 2012 nicht gegeben. Die Bundesjustizministerin hat ihn jüngst in dem eben zitierten Artikel sozusagen offiziell verabschiedet: „Es wird nicht einen 3. Korb geben, der alle Probleme umfassend regeln kann.“, und „die Verschränkung der Akteure erlaubt im Moment keinen großen Wurf und kein Superreformgesetz, das alle Interessenkonflikte der digitalen Welt auf einmal lösen könnte“. Dabei hatte die Bundesregierung unter Kanzlerin Merkel acht Jahre Zeit für ein wissenschaftsfreundliches Urheberrecht gehabt. Was derzeit noch sozusagen in der Gesetzgebungs-Pipeline ist, ist eventuell (aber wohl kaum mehr in dieser Legislaturperiode) eine Anpassung der Regelungen für die Nutzung verwaister Werke nach der Verabschiedung der entsprechenden Richtlinie der EU[13], Korrekturen bezüglich der Abmahnungspraxis und, überflüssig genug, ein Leistungsschutzrecht für Presseverleger. Vielleicht ist der dringend nötige Neuansatz, der vorsichtig ja auch von Parteien der Grünen, der Linken, mit etwas Abstand auch von der SPD und radikaler von den Piraten gefordert ist, nur in einer veränderten politischen Landschaft und vor allem in einem veränderten breiteren gesellschaftlichem Umfeld mit normativen Vorstellungen möglich, die dem Umgang mit Wissen und Information in elektronischen Umgebungen angemessen sind.

In Richtung einer allgemeinen Bildungs- und Wissenschaftsklausel

Woran liegt es, dass das wissenschaftsfreundliche Urheberrecht nicht vorankommt? Antrieb dafür wurde seit Jahren vom *Aktionsbündnis Urheberrecht für Bildung und Wissenschaft* (BuW) gegeben, das seit 2004 eine Doppelstrategie betrieben hat: Sich einerseits um eine Verbesserung der bestehenden Schrankenregelungen für BuW zu bemühen, und andererseits, wegen der Besonderheiten des Umgangs mit Wissen und Information in BuW, Vorschläge für ein Wissenschaftsurheberrecht als speziellen Teil des Urheberrechts zu entwickeln. Im Zentrum des Wissenschaftsurheberrechts stand und steht weiter die Forderung nach einer umfassenden Bildungs- und Wissenschaftsklausel (BuW-Privileg), durch welche die jetzigen unzureichenden Schranken weitgehend überflüssig werden könnten. Dem Vorschlag des Aktionsbündnisses von 2010 für einen neuen Paragraphen 45b im UrhR haben sich (mit leichten Modifikationen) dann auch die Allianz der Wissenschaftsorganisationen und die Kultusministerkonferenz (KMK) angeschlossen.

1. Mit dieser Wissenschaftsklausel sollen die anderen, auf Bildung und Wissenschaft bezogenen Schrankenregelungen im UrhG ersetzt werden, insbesondere die §§ 52a, 52b, und 53a und die Bildung und Wissenschaft betreffenden Teile von § 53 (eventuell auch andere Normen im Gesetz, ganz oder teilweise).

2. Durch diese Wissenschaftsklausel soll der volle Umfang der Nutzung wissenschaftlicher Literatur ohne weitere kleinteilige Einschränkungen (wie jetzt in § 52a UrhG) genehmigungsfrei (nicht in jedem Fall zwangsläufig vergütungsfrei) für den eigenen wissenschaftlichen Gebrauch und für nicht gewerbliche Bildungszwecke sowie für Vermittlungsleistungen der Kultureinrichtungen wie Bibliotheken zugestanden werden.

3. Die dadurch mögliche Verschlankung des Urheberrechts soll auch zu einer größeren Rechtssicherheit für den Umgang mit publiziertem Wissen in Bildung und Wissenschaft beitragen, nicht zuletzt auch für die Gerichte selber, die bislang verschiedentlich die jetzigen Regelungen widersprüchlich ausgelegt haben und mit für lange Phasen schwebenden Verfahren für weitere Unsicherheit gesorgt haben bzw. haben sorgen müssen.

4. Die in dieser Wissenschaftsklausel formulierten Nutzungsprivilegien sollen nicht auf die Vermittlungseinrichtungen wie Bibliotheken beschränkt sein (auch wenn diese natürlich in die Regelungen der allgemeinen Wissenschaftsschranke einbezogen werden; vgl. (3) in dieser Liste), sondern sollen in erster Linie einen unverzichtbaren Nutzungsfreiraum für die in Bildung und Wissenschaft Tätigen selbst schaffen.

5. Für Zwecke der Dokumentation und Bestandssicherung der Kultureinrichtungen ist eine genehmigungs- und vergütungsfreie Nutzung vorzusehen.

6. Die Öffentliche Zugänglichmachung (entsprechend § 19a UrhG) ist nur für geschlossene Benutzergruppen in der Forschung und der Ausbildung vorgesehen.

7. Durch diese umfassende Wissenschaftsschranke sollte es aus Sicht von Bildung und Wissenschaft nicht erforderlich sein, spezielle Regelungen für den Umgang mit verwaisten Werken zu treffen. Auch diese sollen entsprechend Abs. 1 des Vorschlags genehmigungsfrei sowohl für Bildung und Wissenschaft als auch für die Vermittlungseinrichtungen zu nutzen sein.

8. Mit der Einführung einer umfassenden Wissenschaftsschranke sollen auch bestehende Unsicherheiten bezüglich des Einsatzes von *Data-Mining*-Techniken beseitigt werden. Diese werden in der Wissenschaft immer wichtiger, setzen aber ein (temporäres) erlaubtes Herunterladen großer Datenmengen voraus, welches ja nach dem jetzigen Urheberrechtsverständnis eine Form der Vervielfältigung (als Recht der Rechteinhaber) ist.

9. Für den Fall, dass Vergütungen anfallen, sollen diese über Pauschalierungen durch die Träger von Bildungs-, Wissenschafts- und Kultureinrichtungen geregelt werden.

Das Aktionsbündnis sieht die hier vorgeschlagene Wissenschaftsschranke rechtlich voll im Einklang mit einer zeitgemäßen Interpretation der Urheberrechtsrichtlinie der EU von 2001, insbesondere von Art. 5, 3, a: “use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author‘s name, is indicated, unless this turns out

to be impossible and to the extent justified by the non-commercial purpose to be achieved", zusammen mit Erwägungsgrund (42) der Richtlinie: „Bei Anwendung der Ausnahme oder Beschränkung für nicht kommerzielle Unterrichtszwecke und nicht kommerzielle wissenschaftliche Forschungszwecke einschließlich Fernunterricht sollte die nicht kommerzielle Art der betreffenden Tätigkeit durch diese Tätigkeit als solche bestimmt sein. Die organisatorische Struktur und die Finanzierung der betreffenden Einrichtung sind in dieser Hinsicht keine maßgeblichen Faktoren."

Das Bundesjustizministerium weigert sich bislang

- die Kritik an den unzulänglichen, BuW betreffenden Schrankenregelungen des UrhG konstruktiv aufzugreifen,
- der Besonderheit eines Urheberrechts für BuW Rechnung zu tragen,
- eine öffentliche Debatte um ein Wissenschaftsurheberrecht und eine umfassende Wissenschaftsschranke zu eröffnen bzw. zu befördern,
- juristisch überprüfen zu lassen, ob eine umfassende Wissenschaftsschranke kompatibel mit EU-Vorhaben ist (oder nicht),
- Initiativen gegenüber der EU ergreifen, die Hindernisse der obsolet gewordenen Urheberrechtsrichtlinie von 2001 (!) zu beseitigen und
- sich mit anderen Ländern abzustimmen, um ein konzertiertes Vorgehen in Sachen einer umfassenden Wissenschaftsschranke zu erreichen.

Bei den im Bundestag vertreten Parteien (bis vielleicht auf die FDP) sieht es inzwischen aber anders aus:

- Die SPD-Bundestagsfraktion setzt sich mit ihren *Zwölf Thesen für ein faires und zeitgemäßes Urheberrecht* für eine „Überprüfung der Bildungs- und Wissenschaftsschranken" ein.
- DIE LINKE, in ihrem Papier *Die Chancen der Digitalisierung erschließen – Urheberrecht umfassend modernisieren*, fordert, „die bestehenden Schrankenprivilegierungen für Wissenschaft und Forschung in einer bereichsspezifischen Wissenschaftsschranke zusammenzufassen".
- Die Enquete-Kommission *Internet und digitale Gesellschaft* (auch im Einvernehmen mit der Politik der Grünen) will überprüft sehen, „ob im Urheberrecht eine allgemeine Bildungs- und Wissenschaftsschranke verankert werden soll, die die bestehenden Schrankenprivilegierungen für Wissenschaft und Forschung zusammenfasst, um eine breitere Nutzung und Verbreitung von wissenschaftlichen Erkenntnissen zu ermöglichen."
- Und auch im Diskussionspapier der CDU/CSU-Bundestagsfraktion zum Urheberrecht in der digitalen Gesellschaft vom 12. Juni 2012 findet sich ein Abschnitt *6. Wissenschaftsfreundliches Urheberrecht*: „Aufgrund der voranschreitenden Digitalisierung sind viele dieser Regelungen nicht mehr passgenau und teilweise technisch überholt. Außerdem könnten sich einige Regelungen vor Gericht als nicht praktikabel herausstellen. Auf der Grundlage einer umfassenden Evaluierung möchte die CDU/CSU-Bundestagsfraktion daher eine Überarbeitung dieser Regelungen und die Zusammenführung zu einer einheitlichen Wissenschaftsschranke erreichen."

Perspektiven

Sicherlich wäre mit der Einführung einer umfassenden Wissenschaftsklausel keineswegs allen Anforderungen eines Wissenschaftsurheberrechts Genüge geleistet.

- Ergänzt werden muss diese Wissenschaftsklausel durch eine Verbesserung der Urheber-/Autorenrechte an ihren publizierten Werken, in erster Linie durch eine Einführung eines unabdingbaren Zweitveröffentlichungsrechts. Dies müsste durch Veränderungen im Urhebervertragsrecht erreicht werden, vermutlich über § 38 UrhG, eventuell auch durch Änderungen in § 31 UrhG.
- Da das Zweitverwertungsrecht als Recht der AutorInnen mit Open Access zunächst nichts zu tun hat, ist dringend eine öffentliche und rechtliche Debatte darüber zu führen, in welcher Form eine Mandatierung der Zweitverwertung zugunsten Open Access eingeführt werden kann – vermutlich analog zur Abschaffung des Hochschullehrer-Patentierungsrechts im Jahr 2002, damals durch eine einfache Reform des Arbeitnehmererfindungsgesetzes.
- Mit einer allgemeinen Wissenschaftsklausel müssten auch Bestimmungen von § 95b UrhG angepasst werden, durch die bislang in bestimmten Fällen technischen Schutzmaßnahmen Priorität gegenüber einer genehmigungsfreien Nutzung in Bildung und Wissenschaft gegeben wurde.
- Im Urhebervertragsrecht sollte auch geregelt werden, dass der Urheber (Autor) seine Verwertungsrechte als Nutzungsrechte Dritter nur so weit übertragen kann, wie

Rainer Kuhlen

Rainer Kuhlen ist Professor für Informationswissenschaft an der Universität Konstanz und Sprecher des Aktionsbündnisses *Urheberrecht für Bildung und Wissenschaft*.

es zur Veröffentlichung des gesamten Werkes durch den Verwerter erforderlich ist. Damit sollten die Rechte an einzelnen Elementen seines Werkes (z. B. Abbildungen, Tabellen) nicht automatisch mit abgetreten werden.

Wie könnte es weitergehen? Drei Perspektiven sind erkennbar:

- Perspektive 1:
  Je restriktiver das Urheberrecht ist und bleibt, desto eher wird Open Access der offene, freie Standard wissenschaftlicher Publikation.

- Perspektive 2:
  Angesichts der offensichtlichen Unzulänglichkeit der Schrankenregelungen (für BuW) wächst die Bereitschaft, sich mittelfristig auf eine umfassende Bildungs- und Wissenschaftsschranke und langfristig auf ein Wissenschaftsurheberrecht zu verständigen.

- Perspektive 3:
  Je mehr den Verwertern (Verlagen) die WissenschaftlerInnen als AutorInnen abhandenkommen, desto mehr werden sie neue Geschäftsmodelle unter Anerkennung von Wissen und Information als frei verfügbare Gemeingüter (Commons) entwickeln, so dass sie auch als kommerzielle Anbieter auf den Informationsmärkten für BuW bleiben können. Bei solchen Geschäftsmodellen sind die Informationsobjekte selbst für jedermann frei nutzbar (kostenfrei und ohne weitere Einschränkungen) – verdient werden kann über die Bereitstellung informationeller Mehrwertleistungen, wie mediale Aufbereitung, Hypertextifizierung, Dossiers, Summaries, Übersetzungen, Retrieval- und Mining-Angebote, innovative Reviewmodelle, personelle und institutionelle Hintergrundinformation (vgl. Abbildung 1).

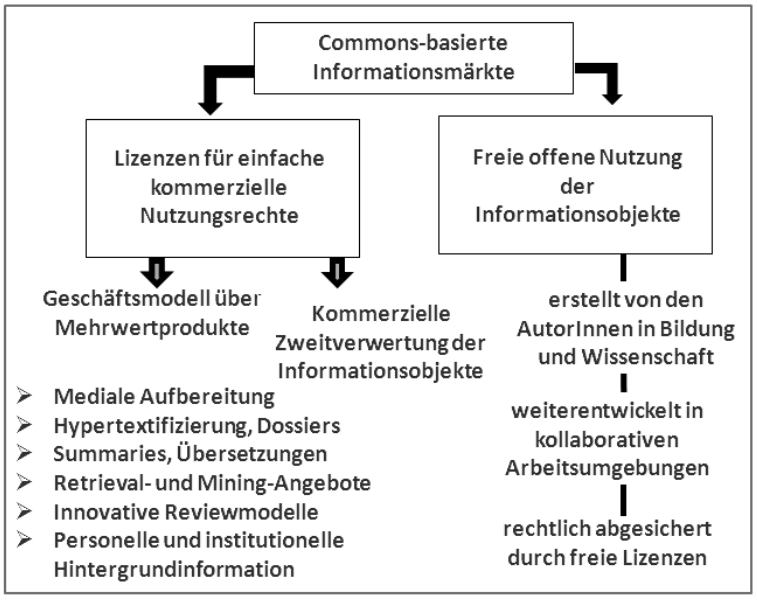


Abbildung 1: Modell einer zukünftigen commons-based information economy/society

Fazit: Das Urheberrecht muss sich nicht an geistiges Eigentum und Wissenschaftsfreiheit rückbinden

Um auf den Ausgang der Überlegungen in diesem Beitrag zurückzukommen: Die Regelungen für den Umgang mit Wissen und Information, zumindest in Bildung und Wissenschaft, brauchen, soweit dafür das Urheberrecht zuständig sein soll, keine Rückbindung an ein ohnehin problematisches Konzept des geistigen Eigentums und auch nicht an das Prinzip der Wissenschaftsfreiheit.

Die Interessen in Bildung und Wissenschaft sind kaum die nach Vergütung durch kommerzielle Verwertung, sondern richten sich in erster Linie auf Sichtbarkeit und Nutzung ihrer Werke, was bei positiver Wertschätzung zur Erhöhung der Reputation führt und dann im Gefolge durchaus auch zur Verbesserung der materiellen Situation wissenschaftlicher AutorInnen beitragen kann. Urheberrechtlich reichen dafür die im europäischen Urheberrecht ohnehin starken Persönlichkeitsrechte aus, also die Anerkennung der Urheberschaft, das Recht darüber zu entscheiden, ob, wann und wie ein erstelltes Werk zu publizieren ist, und das Recht, gegen vandalisierende Verfälschung der Werke geschützt zu sein. Von Eigentum, primär verstanden als das Recht, andere von der Nutzung auszuschließen, braucht dafür keine Rede zu sein.

Auch Wissenschaftsfreiheit – in erster Linie wohl doch zu verstehen als das Recht, frei, auch in der Wahl der Themen, forschen zu dürfen, ergänzt um das Recht, die Forschung durch ungehinderte Nutzung publizierten Wissens informationell absichern zu können – muss in der rechtlichen Sicherung des Umgangs mit Wissen und Information keine Rolle spielen. Die Debatte darüber hat zuweilen leicht absurde Züge angenommen. So wurde und wird auch weiter gegen ein Zweitveröffentlichungsrecht und erst recht gegen eine Zweitveröffentlichungsverpflichtung zugunsten eines institutionellen Mandats (also der Institutionen der AutorInnen) ins Spiel gebracht, dass Wissenschaftsfreiheit auch bedeuten müsse, alle Rechte an einen kommerziellen Verwerter abtreten zu dürfen und somit die Öffentlichkeit von der freien Nutzung auszuschließen.

Die Produktion von Wissen ist gewiss genuine und anzuerkennende Leistung von AutorInnen, zunehmend in Gruppen kollaborativ erstellt, beruht aber auf wesentlichen Vorleistungen des bestehenden Wissens und nicht minder entscheidend auf der Bereitstellung der personellen, materiellen, technischen und institutionellen Ressourcen der Gesellschaft. Zumindest in der durch öffentliche Gelder geförderten Wissenschaft sollte es eine Selbstverständlichkeit sein, dass die erstellten Werke nach Open-Access-Prinzipien freigestellt werden. Das schließt auch bei einem mandatierten institutionellen Zweitverwertungsrecht keineswegs die Möglichkeit aus, das erstellte Werk auch kommerziellen Verwertern anzubieten. Und bei einer Erstpublikation nach dem goldenen Open-Access-Modell (also in genuinen Open-Access-Organen) muss die Gesellschaft dafür sorgen, dass die für die Produktion und öffentliche Zugänglichmachung erforderlichen Ressourcen erbracht werden.

Freier Zugriff auf Wissen und Information ist das primäre Prinzip von Informationsgesellschaften – deren kommerzielle Verwertung erst das zu rechtfertigende sekundäre Ziel. Das solle auch das Prinzip eines Wissenschaftsurheberrechts sein.

Anmerkungen

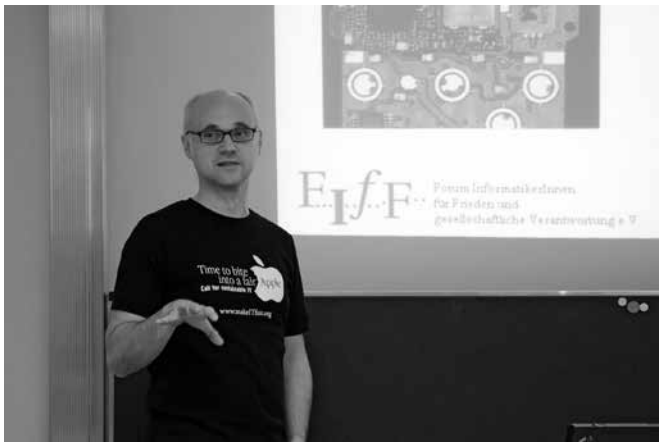
1 *Der Text beruht auf einem Vortrag auf der FIfF-Jahrestagung „Digitalisierte Gesellschaft – Wege und Irrwege“ 9.-11. November 2012 in Fulda.*
2 *U.S. Constitution, Article I, Section 8, Clause 8.*
3 *Thomas Jefferson, Letter to Isaac McPherson, 13 August 1813 – http://press pubs.uchicago.edu/founders/documents/a1_8_8s12.html*
4 *In der 8. Sitzung des Ausschusses für Grundsatzfragen vom 7.10.1948 – Der Parlamentarische Rat 1948-1949, Band 5/1, S. 198.*
5 *BVerfGE 31, 229, 240 – Kirchen-und Schulgebrauch.*
6 *BVerfGE 21, 73, 83; ähnlich BVerfG NJW 1999, 414.*
7 *Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights – http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:195:0016:0025:EN:PDF.*
8 *„Eigentümer des Originals eines Werkes der bildenden Künste“ (§ 44 UrhG); Eigentümer eines „Datenbankwerke“ (§ 55a, 87e UrhG); Eigentümer von „ Vervielfältigungsstücken“ (§ 69f, 98 UrhG).*
9 *Thomas Hoeren: Der Kampfbegriff Geistiges Eigentum ist falsch – http://www.elektrischer-reporter.de/rohstoff/video/143/.*
10 *Vgl. nur BVerfGE 36, 280, 291 = GRUR 1974, 142.*
11 *Vgl. BGH, Beschluss vom 18. 9. 2007 – X ZR 167/05 zur Regelung der „positiven Publikationsfreiheit“ des Hochschullehrers in § 42 Nr. 1 ArbEG.*
12 *http://www.bmj.de/SharedDocs/Namensartikel/20120531_Kein_Grund_zum_Kulturpessimismus.html.*
13 *Directive 2012/28/EU of 25 October 2012 on certain permitted uses of orphan works – http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:299:0005:0012:EN:PDF.*

Berichte aus den Arbeitsgruppen der Jahrestagung 2012

Sebastian Jekutsch

Arbeitsgruppe: „Sind faire Computer möglich?“

Nach dem kleinen aber feinen Workshop im Vorjahr wurde auch in Fulda eine Arbeitsgruppe zu Fairer IT angeboten.



Im Laufe meiner Recherchen habe ich viele interessante Quellen entdeckt und einige davon in der AG vorgestellt. Die „Arbeit“ der Gruppe bestand auch dieses Jahr darin, sich aus der Vielzahl von Informationen eine Meinung zu bilden, wie man die unschöne Situation bei der Herstellung von Hardware verbessern kann.

Der Ablauf wurde etwas gestrafft, hinzu kam ein Augenmerk auf aktuelle Entwicklungen:

- „Ist IT-Produktion unfair?“ mit Beispielen aus dem Rohstoffabbau, der Fertigung und der Entsorgung von Altgeräten, auf Basis öffentlich zugänglicher Recherchen diverser zivilgesellschaftlicher Initiativen.

- „Sind faire Computer möglich?“ mit einer Aufzählung der Probleme im Vergleich etwa mit fairem Kaffee oder Kleidung: viele Rohstoffe, viele Akteure, viele Länder und Industrieabhängigkeit.

- „Was können wir tun?“ mit einer Reihe von Gegenstrategien, die trotz scheinbar aussichtsloser Lage Hoffnung aufkommen lassen, die IT-Produktion doch zumindest an einigen Stellen fairer gestalten zu können, etwa durch Bau teilfairer Geräte, Ranking von Firmen, Siegel, Gesetzesinitiativen, öffentlichen Protest, Bildungsarbeit und so weiter.

Zu Gunsten von Nachfragen und Diskussion haben wir das eine oder andere weggelassen. Immer wieder kommt man an einen Punkt wo eine Abwägung der Argumente und Ziele schwierig ist. Hier eine Meinung bilden zu können ist die Stärke einer Arbeitsgruppe gegenüber etwa einem Vortrag. Eine Bestätigung aus dieser Runde: Das FIfF sollte weiterhin und vor allem das Thema unter die Leute bringen.

Schade allerdings, dass es nur vier Teilnehmer gab, und da sind der Organisator und der Fuldaer Hiwi schon eingerechnet.

Die Folien schicke ich auf Anfrage gerne zu. Wer bei dem Thema auf dem Laufenden bleiben möchte, kann sich unserer Mailingliste anschließen: *http://lists.fiff.de/mailman/listinfo/fiff-fairit*

Sebastian Jekutsch ist FIfF-Mitglied aus Hamburg.
Kontakt: sj@fiff.de.

Karin Kleinn, Britta Schinzel

Arbeitsgruppe: „Verantwortung in der Informatik“

(1) Brainstorming zu den Fragen

1. Welche durch Informatik (neu) geschaffenen Fakten sind gesellschaftlich ambivalent und problematisch und relevant für informatische Verantwortungsfragen? Was ist schädlich und wenn ja, warum?

2. Wie können InformatikerInnen diese Entwicklungen beeinflussen? Welche Aufgaben haben InformatikerInnen dabei? Wie können InformatikerInnen ihre Verantwortung wahrnehmen?

Beide Fragenkomplexe wurden bereits vermischt behandelt.

(2) Ergebnisse des 3-jährigen DFG-Projekts *Weltbilder in der Informatik* mit Bezug auf Verantwortung und Geschlecht

Karin Kleinn berichtete über das oben genannte Forschungsprojekt, in dem verschiedene Kategorien von auf die Informatik bezogenen Weltbildern von Informatik-Studierenden untersucht wurden, etwa Technikbilder, Berufsbilder, Menschenbilder, Entwickelnde und Benutzende, Realitätskonstruktion etc. Unter anderem lieferte das Projekt Ergebnisse zur Verantwortungsnahme und zu Geschlechterbildern. Dabei zeigte sich ein Einfluss des Studiums insofern, als Studierende zu Beginn des Studiums noch aus der Sicht der Nutzenden argumentieren und daher durchaus Verantwortung der Profession für informatische Produkte sehen, während Studierende im Hauptstudium die Seite gewechselt haben, ihre Verantwortung fast nur in der Erfüllung professioneller Anforderungen gegenüber Vorgesetzten und Auftraggebenden sehen, weitergehende moralische Anforderungen aber öfter auf Auftraggebende und Benutzende schieben. Sie argumentieren viel mit *dual use* für die Nutzungsverantwortung. Wenn die Rede auf militärische Anwendungen kommt, so erscheint ihnen dies eine einmalige binäre Entscheidung dagegen oder dafür. Mikroethische Fragen innerhalb der Software-Entwicklung sind nicht im Bewusstsein der Studierenden, ebenso wenig wie der Einfluss von Arbeitsklima und Arbeitshaltungen. Die Notwendigkeit, Nutzende zu integrieren, wird nur am Ende der Benutzungsschnittstelle gesehen.

(3) Zusammenbringen von (1) und (2), Diskussion dieser Ergebnisse und mögliche Maßnahmen

Die meisten Vorschläge bezogen sich auf die Lehre, ethische Grundbildung an der Schule, und ethische Fragen und IuG im Informatik-Unterricht.

- Lehrerausbildung: Vermittlungskompetenz entwickeln, zur Wiederverwendung Unterrichtsmaterialien entwickeln und in Berufsverbänden verbreiten, auf einheitliche Plattformen bringen, aber auch dezentrale Entwicklungen.

- Defiziten in der universitären Ausbildung begegnen.

Weiter wurde die Wichtigkeit von Öffentlichkeitsarbeit betont, den Kulturwandel in die öffentliche Wahrnehmung zu bringen, so wie dies zur technischen Überwachung teilweise bereits geschehen ist, Defizite dabei durchaus skandalisieren, um Rechtfertigungsdruck zu erzeugen.

Constanze Kurz, Britta Schinzel

Arbeitsgruppe: „Fallbeispiele zu Ethik und Verantwortung in der Informatik“

Im Rahmen der GI-Fachgruppe *Informatik und Ethik* wurden eine Reihe von Fallbeispielen entwickelt, welche an mehreren Hochschulen in Seminaren erprobt wurden. Einige davon sind in [1] veröffentlicht.

Die GI-Arbeitsgruppe veröffentlicht weiterhin regelmäßig im *Informatik Spektrum* Fallbeispiele unter der Rubrik *Gewissensbits*. Drei solcher Fallbeispielen wurden in dieser AG in drei Arbeitsgruppen durchgespielt, anschließend im Plenum der AG vorgestellt. Sie wurden besprochen und den Aspekten:

- Wer sind die Akteure?
- Welche ethischen Konflikte können auftreten?
- Was geschieht auf der Metaebene?

Dabei wurde auch jeweils an der Tafel eine Grafik zur Visualisierung der Beteiligten und ihrer Beziehungen untereinander angefertigt.

Das erste Fallbeispiele hieß: *Spyware*, dabei geht es um ein gutes Angebot zur Mitarbeit in einer Firma, die unter anderem Online-Werbung und Spyware herstellt; das zweite Fallbeispiel hieß *Kollateralschaden*. Hierbei geht es um die Veröffentlichung eines Urlaubsfotos aus der Famile in Facebook, ohne dass die Abgebildeten vorher gefragt wurden. Das dritte, Fallbeispiel, das aus Zeitgründen nicht mehr vorgeführt werden konnte, hieß *Anonymisierer*, wobei es um die (Nicht-)Erlaubnis geht, an einer Universität, *Tor*-Software zu benutzen und zu lehren.

Referenzen

[1] Debora Weber-Wulff, Christina Class, Wolfgang Coy, Constanze Kurz, David Zellhöfer: Gewissensbisse: Ethische Probleme der Informatik. [transcript]-Verlag 2009, Reihe Kultur und Medientheorie

Kai Nothdurft, Sylvia Johnigk

Arbeitsgruppe: „Cyberpeace“

In einem dreistündigen Workshop diskutierten insgesamt 15 Teilnehmende das Thema Cyberpeace. *Dabei wurden die bisher vom FIfF argumentierten Forderungen besprochen und auf dieser Basis das Thema* Cyberwarfare und friedenspolitische Antworten *weiter diskutiert und zusätzliche Forderungen entwickelt. Die Diksussion ist nicht abgeschlossen. Der momentane Stand wird im Folgenden wiedergegeben.*

Begriffsklärung

Zunächst wurde eine Abgrenzung der Begriffe *Cyberwar*, *Cyberwarfare*, *Cyberterror*, *Cybercrime*, *Cyber Espionage*, *Hacktivismus* vorgenommen. Einigkeit herrschte darüber, dass nicht alle Arten von Cyber-Angriffen als Kriegshandlungen eingestuft werden dürfen.

Unter *Cyberwarfare* wird von den Teilnehmenden des Arbeitskreises ein Angriff oder die Verteidigung gegen einen Angriff mittels IT auf ein IT-System verstanden, etwa in Form von Hacking-Attacken oder Malware. Um aber tatsächlich als *Cyberwar* zu gelten ist zusätzlich die Motivation und das Ausmaß des Schadens entscheidend. Man hat bisher nur von Krieg gesprochen, wenn es auch eine kinetische Wirkung einer Waffe gab. Für eine Kriegshandlung muss zudem mindestens eine der beteiligten Konfliktparteien ein Staat sein. Völkerrechtlich wird ein Konflikt erst bei einer vierstelligen Anzahl von Getöteten als Krieg eingestuft.

Medienhype?

Der Begriff *Cyberwar* erfuhr in den vergangenen Monaten in den Medien einen regelrechten Hype. Auf Sicherheitskonferenzen, Tagungen und in Regierungskreisen wird hektisch nach Lösungen gegen vermeintliche oder tatsächliche Bedrohungen gesucht. Das führt zu einer technischen und verbalen Aufrüstung, die eine gefährliche Rüstungsspirale in Gang gesetzt hat. Es wurde diskutiert, ob mit der Dauerpräsenz in den Medien bereits eine – möglicherweise sogar gewollte – Desensibilisierung der Öffentlichkeit und Gewöhnung an Cyberwarfare als legitime und normale Maßnahme staatlicher Sicherheitsstrategie einhergeht. Ein vergleichbarer Effekt ist bei der Informationsflut über Pannen in französischen Atomkraftwerken zu beobachten, wodurch kritische Störungen kaum noch auffallen.

Der AK diskutierte, inwieweit ein Cyberwar eine reale Bedrohung darstellt, ober ob es sich hier um Panikmache und Hysterie handelt. Es bestand der Eindruck, dass die Diskussion stark interessengetrieben von den Herstellern von IT-Sicherheitsprodukten und Sicherheitsbehörden geführt wird, und auf Seiten der Politik eine gewisse Ratlosigkeit über die richtige Strategie herrscht. Unabhängige Forschung zur Bedrohungslage, den militärischen Strategien oder dem Status von Cyberwaffen ist den Teilnehmenden weitgehend unbekannt oder technisch wenig fundiert. Eine Ausnahme bildet die Untersuchung des *Stuxnet*-Wurms. Da viele Informationen der militärischen Geheimhaltung unterliegen, ist die Recherche schwierig.

Der AK hält einen reinen Cyberwar für ein eher unrealistisches Szenario. Sehr viel wahrscheinlicher erscheint dagegen, dass Cyberwarfare vorbereitend oder als Unterstützungsmaßnahme

Eindrücke aus den Arbeitsgruppen, Fotos: FAI Fulda

begleitend zu einer allgemeinen kriegerischen Handlung eingesetzt wird.

Bemerkenswert ist, dass ausgerechnet die hoch entwickelten Industrieländer die verbale, strategische und technische Hochrüstung vorantreiben anstatt, zur Deeskalation beizutragen, obwohl gerade sie besonders anfällig für Cyberangriffe sind und dementsprechend besonders stark unter Cyberwarfare leiden würden.

Bestätigung und Erweiterung der FIfF Positionen

Der AK war sich einig, dass Deeskalation wichtig ist. Die bereits veröffentlichten Forderungen des FIfF[1] dazu erfuhren weitgehende Zustimmung.

Zur Rüstungskontrolle wurde vorgeschlagen, die Verbreitung von Exploits völkerrechtlich zu verbieten. Als wirksames Mittel wurde die Pflicht zur Offenlegung von Schwachstellen angesehen. Dadurch werden Cyberwaffen entschärft, die die Schwachstellen auszunutzen versuchen.

Das Attributierungsproblem

Im Konflikt um die georgische Provinz Südossetien wurde 2008 gezielt durch Cyberangriffe Kriegspropaganda und Irreführung betrieben, indem Kommunikationsstrukturen manipuliert und lahmgelegt wurden, u. a. durch Entstellung (*Defacement)* der Webseiten des Parlaments und des Außenministeriums von Georgien.

Nach einem Satz des Tragödiendichters Aischylos ist das erste Opfer des Krieges die Wahrheit. Dies gilt insbesondere für den Cyberwarfare. Da die Angriffe zunächst im virtuellen Raum stattfinden, sind ihre Wirkungen nur mittelbar wahrnehmbar. Dadurch sind Verdächtigungen und Behauptungen über angeb-

lich erfolgte Cyberangriffe nur schwer nachprüfbar. Von außen ist es schon schwierig festzustellen, ob überhaupt ein Angriff stattgefunden hat.

Das Problem verschärft sich dadurch, dass unter Umständen der Angreifer nicht eindeutig bestimmt werden kann. Selbst für die Angegriffenen, erst Recht aber für die Öffentlichkeit ist es schwierig nachzuvollziehen, wer den Angriff tatsächlich ausgeführt hat, also ihn einem konkreten Angreifer zuzuordnen. Aus der technischen Art eines Angriffs kann auch nicht immer auf die Motivation des Angreifers geschlossen werden, etwa ob es sich um eine Straftat oder einen kriegerischen Akt handelt. Dies erschwert eine angemessene politische Reaktion oder gar völkerrechtliche Sanktionierung.

Mit Forensik lassen sich zwar theoretisch Indizien und Spuren ermitteln, etwa durch Auswertung von Logdaten. Allerdings stehen viele durchaus vorhandene Daten kaum für eine Untersuchung zur Verfügung, wenn sie auf verschiedenen Systemen von verschiedenen Betreibern in unterschiedlichen Ländern gespeichert sind.

Um eine unabhängige, völkerrechtlich anerkannte Attributierung des Angriffs zum Aggressor vornehmen zu können, schlägt der AK vor, dass diese Daten über internationale Abkommen für transparente forensische Untersuchungen unter internationaler Aufsicht zugänglich gemacht werden, wenn behauptet wird, dass Cyberattacken stattgefunden haben und wenn der Angegriffene den Verdacht einer kriegerischen Motivation hegt und entsprechend politisch reagiert. Hier soll nicht einer weltumspannenden Vorratsdatenspeicherung das Wort geredet werden. Ein Aggressor wird ohnehin versuchen, soweit wie möglich seine Spuren zu verwischen und Daten zu löschen. Vielmehr sollen lediglich dann noch vorhandene Daten und Informationen ausschließlich für Vorfälle mit kriegsähnlichem Charakter völkerrechtlich legitimiert zusammengeführt und von unabhängigen Parteien idealerweise sogar öffentlich nachvollziehbar untersucht werden können.

Weiterführender Diskurs und Denkansätze im Arbeitskreis

Im Arbeitskreis wurden auch einige Aspekte diskutiert, zu denen die Teilnehmenden keine gemeinsame Sicht entwickeln konnten oder die nur angesprochen, aber nicht ausdiskutiert wurden, die aber eine wichtige Basis für die weitere Arbeit im FIfF bedeuten können:

1. Inwiefern sind durch Cyberwaffen zielgerichtete Angriffe (chirurgische Schläge) möglich, die damit in ihrer Wirkung eingrenzbar sind? Das Beispiel Stuxnet läßt an diesem Anspruch zweifeln. Der Stuxnet-Wurm wurde für ein sehr spezielles Ziel (die Urananreicherungsanlage in Natanz) entwickelt. Aufgrund eines Programmierfehlers ist er jedoch aus dem begrenzten Szenario ausgebrochen und wird inzwischen in modifizierter Form weiterverwendet.

2. Spielen beim Cyberwarfare nicht nur militärische Akteure mit? Cyberangriffe können nicht nur von militärischen Einheiten sondern auch von Cyberkriminellen, Wirtschaftsspionen, Terroristen, losen Hackergruppen, Scriptkiddies oder paramilitärischen Einheiten durchgeführt werden. Diese verschiedenen Kategorien von Angreifern verfügen über unterschiedliche Fertigkeiten und Schadpotenzial. Die Aktivitäten sind nicht unbedingt unter Cyberwarfare einzuordnen.

3. Entgrenzung: Ist ein Cyberkrieg unwahrscheinlich, weil der Angreifer sich auch selbst mit Cyberwaffen schädigt? Aufgrund der Globalisierung bestehen zwischen potenziellen Gegnern gegenseitige wirtschaftliche Abhängigkeiten.

4. Welche Kriegsszenarien mit welchen Gegnern sind möglich und wahrscheinlich? Im AK wurden verschiedenene Szenarien mit ihren Eintrittswahrscheinlichkeiten betrachtet: Wer greift wen an, beispielsweise die USA China, China die USA, Groß gegen Klein (wahrscheinlich?), Klein gegen Groß?

5. Die technische Machbarkeit von Angriffen und die Wahrscheinlichkeit der effektiven Ausnutzung wurden diskutiert am Beispiel eines Angriffs auf die Stromversorgung. Die grundsätzliche Anfälligkeit zeigte sich aktuell an den Auswirkungen des Wirbelsturms *Sandy*.

6. Besitzen die westlichen Industrienationen einen technologischen Vorteil, verfügt beispielsweise China über vergleichbare Fähigkeiten, einen Cyberwarfare zu führen, oder hat China den Westen bereits überholt?

7. Nordkorea verfügt laut eigenem Bekenntnis über eine Cyberwar-Einheit. Das Land ist de facto vom Internet abgeschnitten. Die wenigen offiziellen Seiten des Landes werden im Ausland gehostet. Lediglich die Nomenklatura hat wahrscheinlich Zugang zum Internet. Offizielle Stellen und wenige Personen verfügen über E-Mail-Adressen (in China), die laut Wikipedia streng reglementiert sind. Dennoch kam es angeblich bereits zu Angriffen des nordkoreanischen Geheimdienstes auf Südkorea, das Land mit nahezu der höchsten informationstechnischen Vernetzung weltweit. Nordkorea kann dort einen höheren Schaden anrichten, als Südkorea im umgekehrten Fall.[2]

8. Gibt es im Cyberwar Internet-Verbot für die Zivilbevölkerung? Wird das *Stay-Put*-Konzept der NATO, wonach die Zivilbevölkerung „in einer Krise und im Verteidigungsfall grundsätzlich zu Hause bleiben“ soll, damit die Kriegsführung „nicht durch umher vagabundierende, orientierungslos oder obdachlos gewordene Menschen behindert“[3] wird, auf den Cyberwar ausgeweitet? Denkbar wäre eine Einschränkung der Nutzung von Kommunikationsmitteln, wie das Internet für unabhängige Informationsbeschaffung, oder die Reservierung von Bandbreite für militärische Zwecke bei *Denial-of-Service*-Attacken auf Netzinfrastrukturen.

Ergebnisse des Arbeitskreises

Die bisherigen Forderungen des FIfF zu Cyberpeace wurden vom AK im Wesentlichen bestätigt. Als Ergebnis kamen aber zwei neue Forderungen hinzu, die das FIfF offiziell übernehmen soll. Der AK fordert:

- unabhängige Forschung zu Cyberwarfare zu intensivieren: Wichtige Aspekte sind dabei Empirie zum Status Quo der Cyberwarfare und die Erforschung politischer Wirkungen. Wir fordern eine Forschung, die unabhängig und frei ist von kommerziellen Interessen der Sicherheitsindustrie und des Militärs. Es muss eine kritische Auseinandersetzung mit der gesellschaftlichen und politischen Wirkung von Cyberwarfare stattfinden.

- die unabhängige und öffentliche Untersuchung von Cyberangriffen, um durch Transparenz dem Attributierungsproblem entgegenzuwirken. Damit soll vermieden werden, dass unter dem Vorwand eines Angriffs im Cyberspace ein konventioneller Krieg gegen beliebige Gegner politisch legitimiert werden kann, ohne das ein tragfähiger Nachweis erbracht wurde. Eine solche Behauptung in den Raum zu stellen, ist noch einfacher als die Behauptung, ein Gegner würde bereits über ein umfangreiches Waffenarsenal verfügen, das unschädlich gemacht werden muss. Die Behauptung ist jakaum widerlegbar ist.

Der AK schlägt folgende Gegenmaßnahmen zur Deeskalation und Abrüstung vor:

- Risikosenkung durch Dezentralisierung und Segregierung von IT-Systemen:
  Der Trend, immer mehr Systeme miteinander zu vernetzen und an das Internet anzubinden, erhöht deren Verletzlichkeit und damit das Gesamtrisiko von Cyberangriffen. Die Informationsgesellschaft wird somit als potenzielles Ziel immer attraktiver. Der Risikoeinsatz in diesem Poker gleicht einem *All-in.* Dezentralisierung und Segregierung können zur Deeskalation und Abrüstung beitragen.

- *Graceful Degradation* (Fehlertoleranz):
  IT-Systeme müssen robuster als bisher konzipiert und implementiert werden. Dadurch wird der potenzielle Schaden bei einer Cyberattacke gesenkt.

- Investition in defensive Technik und Maßnahmen:
  Wie können Frühwarnsysteme aussehen, wie kann man Angriffe erkennen, abwehren? Welchen Nutzen haben IPS, Netzwerkscanner, Analyse, SIEM-Systeme, und wie können diese Techniken allgemein zur Verfügung gestellt werden, etwa in Form von Open-Source-Produkten?

- Demystifizierung von Hacking:
  In der öffentlichen Wahrnehmung erscheint das Durchführen von Angriffen auf IT-Systeme als schwieriger als es tatsächlich ist. Die Sicherheit von Systemen wird überschätzt. Risiken werden nicht realistisch eingeschätzt und vielfach wird entsprechend unvorsichtig agiert. Bei IT-Projekten und der privaten Vorsorge wird der Sicherheit zu wenig Gewicht beigemessen. Durch Aufklärung kann ein besseres Risikobewusstsein erzielt werden, wodurch Vorsichtsmaßnahmen vermehrt umgesetzt und die Verletzlichkeit insgesamt gesenkt werden. Hacking zur Aufdeckung von Schwachstellen dient der Sicherheit.

- Dem Hype um Cyberwarfare entgegenwirken:
  Die Einschätzung der Bedrohungslage erfolgt fast immer mit einem *Worst-Case*-Szenario. Dies verschärft den Rüstungswettlauf und ebnet einer restriktiven und Demokratie-feindlichen Sicherheitsdoktrin den Weg, die die Bevölkerung als Sicherheitsrisiko betrachtet.

- Exportkontrolle für Überwachungstechnologie:
  Überwachungstechnologie lehnen wir generell ab. Zu einem Verbrechenswerkzeug wird sie, wenn sie in repressiven Gesellschaften zum Einsatz kommt. Deep-Packet Inspection Tools ermöglichen Zensur. Dadurch wird Propaganda ermöglicht und freie Kommunikation verhindert. Die Bevölkerung kann leichter manipuliert und aufgehetzt werden. Das folgende Beispiel zeigt, dass eine restriktive Durchsetzung eines Exportverbots notwendig ist: Oppositionelle in Bahrain wurden Opfer staatlicher Gewalt, da sie mittels deutscher Überwachungstechnologien ausgespäht werden. Der eigentliche Skandal ist, dass das Unternehmen *Gamma* behauptet, ihm sei die Technik auf einer Messe entwendet worden.[4] Das BKA erwägt das *Gamma*-Produkt *Finfisher* als Ersatz für den Bayerntrojaner zu kaufen.

Der Arbeitskreis hat gezeigt, dass die Diskussion noch längst nicht abgeschlossen ist. Das Thema wird das FIfF weiter beschäftigen: Es wurde eine Mailingliste eingerichtet[5], die zusammen mit dem Wiki[6] dafür genutzt werden kann. Interessierte sind herzlich eingeladen sich zu beteiligen.

Anmerkungen

1 *http://fiff.de/publikationen/fiff-kommunikation/fk-2012/fk-1-2012/fk-1-2012-cyberwarfare/view*
2 *http://www.zeit.de/digital/datenschutz/2011-08/cyberwar-korea*
3 *Zu Stay put siehe u. a.: http://www.spiegel.de/spiegel/print/d-13520723.html http://www.bildergalerie-diepholz.de/anlage_liebenau/html/das_szenario.html http://www.fritzstavenhagen.de/tl_files/pdf_word/alles_unter_kontrolle.pdf*
4 *http://www.heise.de/security/meldung/Trojaner-made-in-Germany-spioniert-in-Bahrain-1652460.html*
5 *CyberPeace@lists.fiff.de*
6 *http://wiki.fiff.de/Cyberwarfare*

Rainer Rehak

FIfF-Studienpreis 2012
1. Preis

Angezapft

Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung

– Eine Zusammenfassung –

Vielen herzlichen Dank noch einmal an das FIfF für die Auszeichnung meiner Diplomarbeit über die heimliche Online-Durchsuchung. Ich habe mich insbesondere darüber gefreut, weil das Thema nicht nur die Rolle der Informati(onstechni)k in einer digitalen Gesellschaft allgemein berührt, sondern speziell den Umgang staatlicher Stellen mit derartigen neuen Möglichkeiten. Doch warum ist gerade dieser Aspekt so interessant und wichtig?

Der freiheitliche Staat ist ein Mittel menschlich-gesellschaftlicher Selbstorganisation. Im Gegensatz zu anderen gesellschaftlichen Interaktions-, Aushandlungs- und Regelungsmechanismen sind das Staatskonstrukt und seine Prozesse stark strukturiert und formalisiert, was deren Betrachtung und Diskussion einerseits einfacher und andererseits schwieriger macht. Einfacher, weil dadurch eine gewisse Vorhersagbarkeit staatlicher Aktivität erzeugt wird, wofür die Strukturierung gedacht ist. Schwieriger, weil die Formalisierung viele Tücken (u. a. Mehrdeutigkeit, fehlerhafte Modellierung, usw.) birgt, wie gerade wir als Informatiker wissen.

Die Fragestellung der Arbeit nach der Analyse, Reglementierung und Folgen staatlicher Instrumente aus dem Werkzeugkasten der Informationstechnik berührt im Grunde nichts weniger, als die Frage nach den Bedingungen für die Freiheit des Menschen in einem digitalen Zeitalter. Eine Welt, in der vormals verborgene innere Vorgänge einer Person zunehmend nach außen in informationstechnische Systeme verlagert werden, und somit auch zunehmend zugreifbarer werden, gibt diese Vorgänge potentiell auch staatlichen Zugriffen preis. Um diese komplexen Sachverhalte zu erforschen, zu erklären und zu „modellieren" sind gerade Informatiker aus dem Bereich *Informatik und Gesellschaft* gefragt, von der Analyse technischer Methoden über die Erforschung der gesellschaftlichen Implikationen bis hin zur konstruktiven Teilnahme an der Diskussion über die Regulierung des Einsatzes solcher Methoden. Diese Partizipation der Informatik ist sehr wünschenswert, ja sogar verantwortungsvolle Pflicht, denn wie oben erwähnt handelt der Staat natürlich auch „im Auftrag" aller Informatiker.

Der explizite Verweis auf *Informatik und Gesellschaft* soll hervorheben, dass diese Art Vorhaben weder von reinen Informatikern noch von reinen Geistes- und Rechtswissenschaftlern sinnvoll durchgeführt werden kann, denn nur technische Sachkenntnis, also ein Verständnis der Möglichkeiten und Grenzen informationstechnischer Methoden, gepaart mit dem Verständnis gesellschaftlich-rechtlicher Sachverhalte, lassen tatsächliche gesellschaftlich-rechtliche Analysen technischer Belange gelingen. Auch wegen dieses fächerübergreifenden Ansatzes sind besonders in den informatikfremden Bereichen der Arbeit detaillierte Belege vollzogen worden.

Wenn Menschen in einer Gesellschaft leben wollen, die sich in großem Maße auf Computertechnologie verlässt und ihr einen zentralen Stellenwert im gesellschaftlichen Miteinander einräumt, ist die Erforschung dieser Aspekte unabdingbar. Die im folgenden zusammengefasste Arbeit hat das Ziel, die heimliche Online-Durchsuchung technisch fundiert, aber gut verständlich und mit explizitem gesellschaftlichen Bezug zu bearbeiten und so einen Beitrag zur Klärung diesbezüglicher Missverständnisse und auch -stände zu leisten.

Einleitung

Eine *heimliche Online-Durchsuchung* ist ein verdeckter staatlicher Zugriff auf persönlich genutzte informationstechnische Systeme. Im gesellschaftlichen Diskurs haben sich für diese Maßnahme die Begriffe *Bundestrojaner* und *Staatstrojaner* durchgesetzt, wobei der Einsatz dieser Maßnahme nach wie vor hoch umstritten ist.[1]

Die ersten Online-Durchsuchungen wurden 2005 per geheimer Dienstanweisung durchgeführt, um verschlüsselten Inhalten auf entfernten Computern habhaft zu werden. Ab diesem Zeitpunkt wurde sie schon einige tausend mal von Geheimdiensten und mindestens 100-mal von anderen staatlichen Stellen eingesetzt.[2] Bislang ist sie nur für einige Behörden und Polizeien zur Gefahrenabwehr geregelt.

	Bundesebene	Länderebene
Gefahrenabwehr	Bundeskriminalamt (BKA), Verfassungsschutz, Militärischer Abschirmdienst (MAD), Bundesnachrichtendienst (BND)	Bayerische Polizei, Bayerischer Verfassungsschutz, Rheinland-Pfälzische Polizei
Strafverfolgung	keine Gesetzesgrundlage (laut BGH-Urteil)	keine Gesetzesgrundlage

Abbildung 1: Ermächtigungsmatrix Online-Durchsuchung 2013

Methodik

Die Methodik der Arbeit besteht in der Analyse und Gegenüberstellung dessen, wozu diese Art von Maßnahme technisch in der Lage ist und wozu sie rechtlich gesehen nur in der Lage sein sollte. Aus dem in der Arbeit herausgearbeiteten Unterschied, dass die heimliche Online-Durchsuchung prinzipiell technisch

viel mehr kann, als sie rechtlich darf und der in der Arbeit aufgestellten und belegten These, dass ihre technischen Möglichkeiten auch nicht sinnvoll beschränkt werden können, werden gesellschaftlich-rechtliche Bedeutung und Folgen des trotzdem stattfindenden Einsatzes abgeleitet.

Zunächst werden anhand der Aussagen von verantwortlichen Politikern, Staatsorganen, anderen an der Diskussion beteiligten Personen und insgesamt des rechtlichen, technischen und gesellschaftlichen Kontextes der Situation konzeptionelle Anforderungen an eine heimlichen Online-Durchsuchung formuliert. Diese beschreiben bestimmte Eigenschaften, Funktionen und „Verhaltensweisen", die notwendig oder zumindest sehr wünschenswert für eine sinnvolle Anwendbarkeit der Online-Durchsuchung sind. Dies umfasst auch negative Anforderungen, also Folgen, Umstände und Aktivitäten des technischen Aspekts der Maßnahme, die auf jeden Fall vermieden werden müssen oder deren Auftreten zumindest sehr unwahrscheinlich sein muss.

Aus dieser konzeptionellen Beschreibung können konkrete technische Eigenschaften abgeleitet werden. Dies ist möglich, weil die beschriebenen Konzepte und Fähigkeiten in einer gegebenen Computersystemarchitektur nicht beliebig implementierbar sind. Oder anders ausgedrückt: Die aktuelle Computersystemarchitektur definiert funktionale Abhängigkeiten, in denen bestimmte Funktionen nur auf bestimmte Weise realisiert werden können.[3]

Die so abgeleiteten technischen Eigenschaften einer idealen heimlichen Online-Durchsuchungs-Software werden dann einer Analyse unterzogen, wobei das Augenmerk auf unbeabsichtigte Eigenschaften, technische Grenzen und ungewollte Nebeneffekte gerichtet ist, was insofern keine Unausgewogenheit darstellt, als dass die beabsichtigten Funktionen und Eigenschaften einer heimlichen Online-Durchsuchung den Ausgangspunkt der Betrachtung bilden.

Im Anschluss erfolgt in der Arbeit eine Zusammenfassung des Urteils des Bundesverfassungsgerichtes zu heimlichen Online-Durchsuchungen mit spezieller Analyse und Bewertung der Entscheidung aus technischer Sicht. Das Gericht hatte neben der Aufhebung der damaligen Regelung für den heimlichen Zugriff auf informationstechnische Systeme auch hohe Schranken für eine erneute Schaffung derartiger gesetzlicher Grundlagen formuliert, die den informationsgesellschaftlichen Folgen, Möglichkeiten und Risiken einer solchen Maßnahme Rechnung tragen sollen.[4]

Mit dieser zweifachen Herangehensweise ist es möglich, das vorher entwickelte Bild der beabsichtigten und unbeabsichtigten Konsequenzen und Eigenschaften einer heimlichen Online-Durchsuchung mit der Kritik und den Anforderungen des Bundesverfassungsgerichtes in Deckung zu bringen. Dies macht es möglich, konkrete Aussagen für den Einsatz verfassungsmäßiger heimlicher Online-Durchsuchungen zu erarbeiten, die die technischen Möglichkeiten und Grenzen dieser Maßnahme mit einbeziehen. Technikabhängige Implikationen des Urteils können somit aufgelöst werden.

Resultat sind die Sichtbarmachung des vom Gericht vorgegebenen verfassungsmäßigen Rahmens für derartige rechtlich-technische Regelungen und die dadurch mögliche Kritik der aktuellen Rechts- und Anwendungspraxis sowie eine Kritik des Urteils selbst und konkrete Forderungen für die Neubewertung der Maßnahme.[5]

Gesellschaftliche Einbettung

Eine Analyse der technisch-konzeptionellen und gesellschaftlichen Folgen der Online-Durchsuchung verlangt zunächst die Anerkennung, dass informationstechnische Systeme in vielen Bereichen des menschlichen Lebens Einzug gehalten haben, was Lebenswelt und Alltag immer mehr zu Prozessen informationstechnischer Verarbeitung werden lässt.[6]

Dies gilt auch für die Erledigung von Staatsaufgaben, z. B. die Ausübung von Exekutivbefugnissen. Da die Befugnisse rechtlich geregelt sind, muss sich die Beschränkung staatlicher Macht auch in ihren informationstechnischen Werkzeugen wiederfinden.[7]

Die Konvergenz verschiedener individueller und sozialer Lebensbereiche der Menschen im Computer nimmt ein immer größeres Ausmaß an, ohne dass das Verständnis des Computers und seiner Funktionsweise vergleichbar mitwüchse. Dies ergibt eine Abhängigkeit des Einzelnen von komplexen Systemen, die er nicht mehr überblickt.[8] Fremde Eingriffe können daher vom durchschnittlichen Nutzer weder wahrgenommen noch technisch verhindert werden.[9]

Beispiele dieser Komplexität sind unabsichtlich erzeugte Daten, die im Hintergrund Verhalten und Persönlichkeit des einzelnen Nutzers zeitlich festhalten, oder auch die zentrale Anhäufung von Telekommunikationsdaten vieler Personen in derartigen Systemen. All dies erreicht eine neue Qualität in der Ausweitung des Kernbereichs privater Lebensgestaltung ins Digitale. Ein geheimer Eingriff bedeutet den vollständigen Kontrollverlust über diesen Kernbereich; dort setzt die Online-Durchsuchung an.

Die Analyse der Online-Durchsuchung

Eine Online-Durchsuchung wird mittels einer Online-Durchsuchungs-Software (ODS) durchgeführt. Diese muss jeweils für den Einzelfall zusammengestellt werden[10] und kann daher nicht getestet werden. Die Aufbringung auf das zu durchsuchende System ist zudem mit hohen Fehlerrisiken verbunden[11], insbesondere wenn die Infiltration über das Internet erfolgen soll. Um effektiv und effizient heimlich[12] im zu infiltrierenden System suchen und insgesamt agieren zu können, muss die ODS nicht nur mit Benutzerrechten, sondern mit Betriebssystemrechten bzw. im Kernelmode laufen. Nur so kann sie sich z. B. aus Prozesslisten löschen oder Antivirenprogramme täuschen. Um Passwörter direkt aus dem Arbeitsspeicher auszulesen[13], Tastatureingaben abzufangen oder anderweitig Geräte abzufragen ist der Kernelmode zwingend nötig. Somit erlangt die ODS allumfassende Kontrollmöglichkeiten auf dem System.

Die Informationssuche selbst kann bei klassischen, textbasierten Dokumenten ausschließlich anhand syntaktischer Kriterien realisiert werden und ist somit sehr ungenau. Bei vielen Datenquellen aber müssen alle Daten gespeichert werden, da eine Auswertung (teilweise noch) nicht automatisiert erfolgen kann. Das Durchsuchen selbst hinterlässt Datenspuren im System (Datei-

system, Metadaten), die die ODS nach ihrer Aktivität wieder entfernen/zurücksetzen muss. Die gesammelten Daten werden auf dem System vorgehalten und wenn möglich zur entsprechenden staatlichen Stelle übermittelt oder später vor Ort abgeholt, auch dafür muss die ODS schreibend auf das System zugreifen.[14]

Da die ODS auf einem fremden System operiert, ist es nicht möglich, zuverlässige Kryptographie zu betreiben[15], weil auch die ODS weder ihre Integrität noch ihre Vertraulichkeit sicherstellen kann. Dadurch sind folglich weder die Funktionen noch die Aktivitäten der ODS verlässlich belegbar oder rekonstruierbar, was insbesondere wegen der notwendigen Updatefähigkeit der ODS, aber auch wegen der forensischen Bewertung der Funde höchst kritisch zu sehen ist.

Aktuell konzentriert sich die politische Diskussion auf die vermeintlich weniger eingriffsintensive Quellen-Telekommunikationsüberwachung (Quellen-TKÜ), die ausschließlich Daten aktuell laufender Kommunikation ableiten soll. Die Unterscheidung zwischen Online-Durchsuchung und Quellen-Telekommunikationsüberwachung ist aus zwei Gründen jedoch technisch nicht leistbar:

1. Die Quellen-TKÜ-Software wird für das Abfangen zuvor verschlüsselter Daten (Inhalteverschlüsselung, z. B. via pgp) verwendet. Der Versand von Klardaten durch verschlüsselte Verbindungen (Kanalverschlüsselung, z. B. via https) ist in diesem Kontext nicht relevant. Technisch ist jedoch nicht ermittelbar, ob inhalteverschlüsselte Daten überhaupt verschickt werden sollen oder einfach auf dem System verbleiben.

2. Es sind umfassende Informationen über das System nötig, um festzustellen, ob bestimmte Daten z. B. der Bildschirminhalt oder der Inhalt eines Ordners aktuell übertragen wird und somit Gegenstand eines Kommunikationsvorganges ist oder nicht. Diese Informationen darf eine Quellen-TKÜ nicht sammeln.

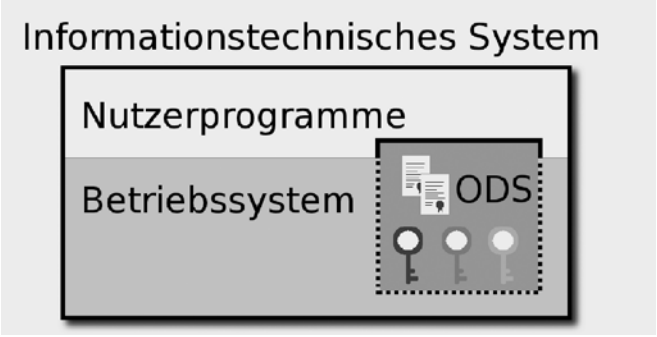


Abbildung 2: Informationstechnisches System

Online-Durchsuchungs-Software und Quellen-Telekommunikationsüberwachungs-Software sind folglich funktionsidentisch. Eine Unterscheidung der Eingriffstiefe der Maßnahmen ist nicht begründbar.

Auch eine Erkennung des Kernbereichs einer Person ist technisch nicht realisierbar[16], weil sie sich den gleichen Problemen gegenübersieht, wie die oben angesprochene Informationssuche. Bei den durchführenden Behörden wird daher eine Anhäufung privater und privatester Daten stattfinden. Daraus ergibt sich, welche Eingriffstiefe eine Maßnahme wie die Online-Durchsuchung für den Betroffenen haben kann und regelmäßig haben wird.

Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und ihre Abwägung

Das Bundesverfassungsgericht erkannte im Jahre 2008 die Abhängigkeit der Bürger von informationstechnischen Systemen und die damit in einem freiheitlichen Rechtsstaat verbundenen berechtigten Erwartungen an Vertraulichkeit und Integrität. Es formulierte nicht nur ein Recht auf diese beiden Eigenschaften, sondern ein Grundrecht auf deren Gewährleistung, auch gegenüber Dritten.[17] Damit beschreibt es einen von der konkreten Sicherheit eines Systems unabhängigen Schutz der Vertraulichkeits- und Integritätserwartung des Einzelnen an das System. Mit dieser Gewährleistung müssen alle Eingriffe in informationstechnische Systeme abgewogen werden.

Zu den oben bereits zusammengetragenen technischen Konsequenzen der Online-Durchsuchung kommen noch andere, weiterreichende Folgen hinzu. Dazu zählt das vergleichsweise hohe Missbrauchspotential[18], u. a. erzeugt durch die einfache Kopierbarkeit digitaler Daten, die geringe Größe heutiger Datenträger und die hohe Komplexität behördeninterner Verarbeitungsabläufe gepaart mit unklaren Handhabungsregeln. Aber auch die Gefährdung Dritter durch die große Streubreite der Maßnahme – auf Computern liegen im Allgemeinen nicht nur Daten des Besitzers – und die hohen gesellschaftlichen Kosten müssen bedacht werden. Ansehen und Glaubwürdigkeit in Sachen IT-Sicherheit, eGovernment usw. sind für einen „hackenden Staat", der durch seine Handlungen auch den Sicherheitslückenschwarzmarkt florieren lässt, selbst optimistisch nur als fragil zu bezeichnen.

Auf den konkreten Nutzen der durch eine Online-Durchsuchung erlangten Informationen bezogen ergibt sich, dass die Funde einer ODS keinesfalls forensischen Standards genügen. Datenmanipulation ist prinzipiell nicht erkennbar und die Echtheit von Funden technisch nicht belegbar.[19] Dennoch sind die Funde laut Bundesverfassungsgericht nicht ohne Informationswert.

Neben diesem nach wie vor laufenden gesellschaftlichen Abwägungsprozess gibt es noch die oben entwickelten, direkt greifbaren Konsequenzen und Erkenntnisse, die aus den technischen Gegebenheiten folgen und nicht Gegenstand, sondern Voraussetzung für eine Diskussion über die Online-Durchsuchung sein sollten.

Zusammenfassung der Ergebnisse

- Eine Funktionsbeschränkung der Software kann **weder sichergestellt noch belegt** werden, daher muss immer die maximale Eingriffshürde zur Anwendung kommen.

- Erlangte Daten haben grundsätzlich **keinen Beweiswert**, sofern sie keinen eigenen intrinsischen Personenbezug aufweisen (z. B. Bilder, die Personen zeigen).

- Die **Trennung** von Telekommunikations- und Nichttelekommunikationsdaten ist insbesondere bei verschlüsselten Daten **technisch nicht lösbar**, daher muss immer – auch für eine Quellen-TKÜ – die maximale Eingriffshürde zur Anwendung kommen.

- Der Kernbereich privater Lebensgestaltung ist praktisch immer betroffen, technischer **Kernbereichsschutz ist prinzipiell nicht möglich**.

Die Beachtung dieser Erkenntnisse ist in der nach wie vor nötigen Diskussion um Einsatz und Verhältnismäßigkeit der Online-Durchsuchung sowie der Interpretation des diesbezüglichen Bundesverfassungsgerichtsurteils dringend notwendig. Darüber hinaus widersprechen die Ergebnisse der aktuellen politischen Praxis und implizieren, dass Exekutive und Legislative ihr Verständnis der Online-Durchsuchung konsequent korrigieren müssen.

Die Folien eines Vortrages zur Online-Durchsuchung an der FAU-Erlangen sind unter folgender URL frei (CC-BY) herunterladbar: *https://od.laryllian.de/downloads/2013.1.7_Online-Durchsuchung.pdf*

Die Arbeit ist unter folgender URL frei (CC-BY) herunterladbar: *https://netzpolitik.org/wp-upload/Rehak-Angezapft.pdf*

Referenzen

Ross Anderson. Security Engineering. Wiley, Indianapolis, 2. Auflage, 2008.

Ulf Buermeyer und Matthias Bäcker. Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO. Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht (HRRS), (10):S eiten 433-441, 2009.

Andreas Bogk (Chaos Computer Club). Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07. 23.9.2007.

Frank Braun. 0zapftis – (Un)Zulässigkeit von "Staatstrojanern". Kommunikation & Recht, (11): Seiten 681-686, 2011. Passau.

Bundesministerium des Innern. Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien. Berlin, 22.8.2007.

Bundesregierung der 16. Wahlperiode. Drucksache 16/4997. 10.4.2007.

Bundesregierung der 17. Wahlperiode. Drucksache 17/11598. 21.11.2012 .

Bundesverfassungsgericht. Bundesverfassungsgerichtsurteil zur Online-Durchsuchung. 27.2.2008.

Bundesamt für Sicherheit in der Informationstechnik. „Leitfaden IT-Forensik". Bonn, Version 1.0.1, März 2011.

Alexander Geschonneck. Computer-Forensik. dpunkt.verlag, Heidelberg, 5. Auflage, 2011.

Kristian Köhntopp und Marit Köhntopp. Why Internet Content Rating and Selection does not work, 1999.

Constanze Kurz. Kernbereichsschutz. transcript-verlag, März 2009.

Henry Krasemann und Jörg Ziercke. Interview u. a. zur Online-Durchsuchung. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, MARITIM Hotel Bellevue, Kiel, 2007.

Bodo Pieroth und Bernhard Schlink. Grundrechte. C.F. Müller, Heidelberg, 26. Auflage, 2010.

Bruce Schneier. Secrets and Lies. Wiley, Indianapolis, 2004.

Holger Stark. Digitale Spionage. Der Spiegel, (11): 32-34, 2009.

Andrew S. Tanenbaum. Modern operating systems. Pearson Prentice-Hall, 3. Auflage, 2008.

Anmerkungen

1 *Buermeyer und Bäcker, „Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO", Seite 9, 2009, Braun, „0zapftis – (Un)Zulässigkeit von ‚Staatstrojanern'", Seite 686, 2011 oder der Generalbundesanwalt, siehe Bundesregierung der 17. Wahlperiode. Drucksache 17/11598. Antwort zu Frage 5, 2012.*

2 *Stark, „Digitale Spionage", 2009.*

3 *Z. B. das Rechtekonzept bei Tanenbaum, Modern operating systems, Seite 2 oder das Datei-/Metadatenkonzept, a. a. O., Seite 257, 2008.*

4 *Bundesverfassungsgericht, Bundesverfassungsgerichtsurteil zur Online-Durchsuchung, Absatz 190, 2008.*

5 *Buermeyer und Bäcker, „Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO", 2009.*

6 *Kurz, Kernbereichsschutz, 2009.*

7 *Pieroth und Schlink, Grundrechte, Seite 66 ff, 2010.*

8 *Schneier, Secrets and Lies, Seite 6 ff, 2004.*

9 *Bundesverfassungsgericht, Bundesverfassungsgerichtsurteil zur Online-Durchsuchung, Absatz 180, 2009.*

10 *Krasemann und Ziercke, Interview u. a. zur Online-Durchsuchung, Minute 2:35, 2007.*

11 *Bogk (Chaos Computer Club), Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07, Seite 16, 2007.*

12 *Bundesregierung der 16. Wahlperiode, Drucksache 16/4997, Antwort zu Frage 5, 2007.*

13 *a.a.O., Antwort zu Frage 13.*

14 *Bundesministerium des Innern, Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien, Antwort auf Frage 39, 2007.*

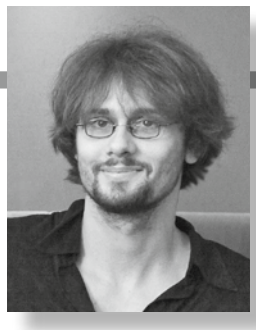
15 *Anderson, Security Engineering, Seite 147 ff., 2008.*

16 *Siehe dazu Köhntopp und Köhntopp, Why Internet Content Rating and Selection does not work, 1999.*

17 *Bundesverfassungsgericht, Bundesverfassungsgerichtsurteil zur Online-Durchsuchung, Absätze 181, 169, 204 und 206, 2007.*

18 *Stark, „Digitale Spionage", 2009.*

19 *Vergleiche Geschonneck, Computer-Forensik, Seite 91 ff, 2011 und Bundesamt für Sicherheit in der Informationstechnik, Leitfaden „IT-Forensik", Seite 89 ff, 2011.*



Rainer Rehak

Rainer Rehak ist Diplom Informatiker (HU-Berlin) und schrieb seine Diplomarbeit zum Thema „Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung". Er studierte von 2002-2012 Informatik und Philosophie in Berlin und Hong Kong und war zwischenzeitlich studentischer Mitarbeiter am Lehrstuhl von Wolfgang Coy. 2012 erhielt er den FIfF-Studienpreis für seine Diplomarbeit. Er ist Mitglied der GI, des CCC und des FIfF.

Göde Both

FIfF-Studienpreis 2012
2. Preis

Von Zwischenwesen und Nicht-Menschen

Ein Beitrag zur Geschlechterforschung in der Informatik

Nach der Abgabe meiner Diplomarbeit (Both 2011) überkamen mich Zweifel. Hatte ich mich ein ¾ Jahr mit einer vaporware *beschäftigt, welche nie zu einer breiten Anwendung kommen würde? Sollte ich ironischerweise dem Hype zum Opfer gefallen sein, den ich in meiner Arbeit kritisiere? Glücklicherweise – zumindest für die Nachhaltigkeit meiner Diplomarbeit – wurde* Siri *wenige Monate später als Bestandteil des Apple iPhone 4S mit großer medialer Aufmerksamkeit vorgestellt. Das* virtual personal assistant Siri *ist nicht nur Bestandteil der Popkultur geworden (vgl. Cendrowski 2012), sondern hat in vielen Ländern seinen/ihren Weg in den Alltag gefunden. In diesem Artikel trage ich die wichtigsten Thesen und Ergebnisse meiner Diplomarbeit zusammen und erläutere dabei, auf welche Weise informatische Artefakte wie* Siri *im Kontext der Geschlechterforschung in der Informatik analysiert werden können.*

„Siri. Dein Wunsch ist ihm Befehl“[1]

Die Verheißungen verständiger Maschinen, welche unser aller Leben leichter machen sollen, manifestieren sich im Interaktionsparadigma der Delegation. In der Vergangenheit haben prominente InformatikerInnen wie Brenda Laurel (1990) und Nicolas Negroponte (1997) dieses Paradigma als richtungweisend für die Zukunft der Mensch-Computer-Interaktion erklärt. Aktuell wird es von *virtual personal assistants* (VPAs) als einer neuen Generation von Schnittstellen-AgentInnen aufgegriffen und mit der mobilen und freihändigen Sprachsteuerung von Webservices, zum Beispiel beim Joggen oder Autofahren, beworben. Bei VPAs handelt es sich um Software-basierte (*virtual*), personalisierte (*personal*) AssistentInnnen (*assistants*). Das zentrale Versprechen der VPAs lautet Arbeitserleichterung und Zeitersparnis durch die Delegation von Routine-Aufgaben. Die fast schon kanonischen Anwendungsbeispiele heißen Reservierungen von Restaurants, Bestellungen von Veranstaltungskarten, Flugstatus abrufen und Versenden von Nachrichten (per mail, SMS, Twitter und Facebook). Ich beziehe mich bei meiner Definition von VPAs auf Adam Cheyer und Tom Gruber (2010). Ihnen zu Folge besteht das VPA-Paradigma aus drei Komponenten: Im Zentrum steht die (1) Aufgabenerledigung durch (2) Intentionserkennung unter Ausnutzung von Kontexten (Zeit, Ort, Aufgabe, Dialog) und der Anpassung an die NutzerInnen durch das (3) Erlernen persönlicher Informationen. Konkurrenz-Begriffe zu VPA, wie in etwa *(Intelligenter) Software Assistent* oder *(Intelligenter) Persönlicher Assistent*, bezeichnen in der Regel ähnliche Dienste.

Die Figur des VPA untergräbt die scheinbar eindeutige Grenze zwischen Mensch und Maschine. VPAs sind Zwischenwesen, denen sowohl traditionell menschliche als auch maschinelle Eigenschaften zugeschrieben werden. Um die Mensch-Maschine-Verhältnisse in Bezug auf VPAs zu analysieren, bietet sich insbesondere die feministische Theoriebildung[2] an, weil kulturhistorisch die Frau lange Zeit das andere des euro-amerikanischen Mensch-Mannes verkörpert hat. Die Frau hatte so den Status als Zwischenwesen, zum Beispiel bei der Unterscheidung von Mensch und Tier. Prägend für meine Analyse ist das Werk der feministischen Technikanthropologin und Gründungsmitglied der *Computer Professionals for Social Responsibility (CPSR)* Lucy Suchman. Ihre Auffassung von Konfigurationen geht über die Zusammenstellung von technischen Komponenten oder der Anpassung von Software hinaus. Suchman begreift Konfigurationen als materiell-semiotische, wechselseitige Prozesse, welche definieren, inszenieren, beschränken und kontrollieren, was Menschen und Maschinen auszeichnen und voneinander unterscheiden.

Die spezifischen Mensch/Maschine-Konfigurationen von VPAs und ihren NutzerInnen werden in der Diplomarbeit hinsichtlich der Kategorien *agency* und Geschlecht analysiert. Daraus ergeben sich zwei Forschungsfragen: Erstens, welche Form von *agency* wird VPAs in den informatischen Forschungen zur Künstlichen Intelligenz (KI) und Mensch-Computer-Interaktion (MCI) zugeschrieben und wie kann *agency* aus der Perspektive der feministischen Technikforschung alternativ konzipiert werden? Zweitens, wie werden VPAs vergeschlechtlicht, das heißt, wie werden sie durch die Geschlechterordnung strukturiert und wie reproduzieren die VPAs die Kategorie Geschlecht? Die Arbeit untersucht nicht die geschlechtsspezifischen Nutzungs- und Gestaltungsweisen, sondern die wechselseitige Materialisierung von Geschlecht und Technik. Ausgangspunkt sind daher nicht vergeschlechtlichte Körper (z. B. Männer) sondern wie Geschlechter-Stereotype, Geschlechter-Konnotationen (Mitbedeutungen) und die geschlechtskonstituierende Arbeitsteilung mit Technik artikuliert, stabilisiert und destabilisiert werden.

Diese Arbeit ist ein Beispiel dafür, welche Gestalt Geschlechterforschung in der Informatik[3] annehmen kann. Sie knüpft insbesondere an Corinna Baths Programm (2013) zur (Ent-)Vergeschlechtlichung informatischer Artefakte an, aber auch an die Forderung des FIfF und der ehemaligen Arbeitsgruppe *Theorie der Informatik* der Gesellschaft für Informatik, die Grundlagen der Informatik im breiteren Sinne zu reflektieren (vgl. Coy 1992). In diesem Sinne soll die Diplomarbeit einen Beitrag zur Diskussion um die Vorannahmen der Technikgestaltung und ihren soziotechnischen Effekten leisten. Die Thematisierung von Ein- und Ausschlüssen strebt so dem Ziel einer inklusiven und damit geschlechtssensiblen Informatik entgegen.

Das Repertoire der Geschlechterforschung in der Informatik erweitere ich in der Arbeit um die Akteur-Netzwerk-Theorie (ANT) aus der Wissenschafts- und Technikforschung. Gemäß ihres Anspruchs ist die ANT eine Methodologie, welche die mannigfaltigen Verbindungen von Menschen und Maschinen beschreiben kann, ohne den Verkürzungen des Sozial- und des Technikdeterminismus zu verfallen. Als technikdeterministisch wird eine Theorie bezeichnet, nach der eine Gesellschaft durch ihre technologische Entwicklung bestimmt wird. Sozialdeterministische Ansätze nehmen spiegelbildlich an, dass Technik das Resultat der sozialen Verhältnisse ist. Beide theoretische Spielarten arbeiten mit einer groben Vereinfachung auf Basis des Ursache-Wir-

kung-Prinzips und setzen eine strikte Trennung von Gesellschaft und Technik voraus. Die ANT beansprucht für sich, diese Defizite zu überwinden. Zu Beginn der 1980er war es ihre Strategie, die fehlende Masse (vgl. Latour 1992) der Sozialwissenschaften zu bestimmen. Gesellschaft bestehe nicht nur aus sozialen Beziehungen zwischen Menschen, so ihre damalige These, sondern werde durch Assoziationen von Menschen und Nicht-Menschen zusammengehalten. Nicht-Menschen sind für sie beispielsweise der Satz des Pythagoras, das Ozonloch oder eben auch Informationstechnik. Nur wenn den Nicht-Menschen *agency* zugestanden werde, könnten die Sozialwissenschaften zu einer adäquaten Beschreibung heutiger Gesellschaften gelangen. Der theoretische Kniff, Nicht-Menschen den Status von Aktanten zu eröffnen, macht die ANT zu einem geeigneten Werkzeug zur Beschreibung und Analyse von Mensch/Maschine-Konfigurationen.

„Siri versteht, was du sagst. Und weiß, was du meinst."

Als Einstiegspunkt für die Analyse habe ich die Leitvision *Knowledge Navigator* aus dem gleichnamigen Video (Dubberly und Mitch 1987) ausgewählt, auf das sich ForscherInnen, DesignerInnen und JournalistInnen im Zusammenhang mit VPAs immer wieder beziehen. Das Video suggeriert, dass VPAs eine Arbeitserleichterung darstellen, problemlos seine NutzerInnen verstehen und weitgehend unbeaufsichtigt nicht-standardisierte Aufgaben erledigen können. Als Komponente eines Tablets wird der *Knowledge Navigator* als Software-Agent mit Dialogsystem inszeniert. Der vernetzte Zugriff auf Informationssysteme und die Fähigkeit, wissenschaftliche Dokumente zu interpretieren, konfiguriert den *Knowledge Navigator* als einen Assistenten für das wissenschaftliches Arbeiten. Er verkörpert die Erfordernisse des lebenslangen Lernens der sozialen Mittelschicht, die in wissensintensiven Bereichen beruflich tätig ist. So visionär auch heute noch das Szenario gelten mag, ist das Video zugleich reaktionär, indem es (neo-)koloniale und sexistische Erzählungen aufgreift.

Im nächsten Schritt habe ich exemplarisch analysiert, welche kulturspezifischen Annahmen in den theoretischen Konzeptionen von VPAs einfließen. Das Paradigma der Delegation in der KI- und MCI-Forschung aktualisiert das euro-amerikanische Konzept vom rationalen, autonomen Individuum. Nicht nur in der feministischen Theoriebildung steht dieses Menschen-Bild in der Kritik. Die vorgeblich universelle Bestimmung des Menschen ist historisch nur den weißen, wohlhabenden Männern zugestanden worden. Dieses vorherrschende euro-amerikanische Konzept begreift das menschliche Individuum als Quelle von *agency* und ist daher nicht für eine adäquate Analyse von Mensch/Maschine-Konfigurationen geeignet. Vielmehr muss in Anschluss an Suchman (2007) *agency* als Effekt bzw. Ergebnis von Konfigurationen gefasst werden.

Neben der Auswertung von theoretischen Beschreibungen von VPAs und der Analyse des visionären Videos *Knowledge Navigator*, wird ein aktueller VPA empirisch untersucht. Die Wahl fiel auf *Siri*, weil es den aktuellen Stand der Technik verkörpert. Die Firma *Siri, Inc.*, welche den VPA vor dem Aufkauf durch den Apple-Konzern entwickelt und vertrieben hat, ist ein spin-off von Forschern aus dem DARPA-Projekt *Cognitive Assistant that learns and organizes* (2003-08, $150 Millionen). Das DARPA-Projekt verfolgte die Unterstützung von Befehlsstäben durch VPAs. Teile des Gesamtprojekts sind seit Sommer 2010 im *Command Post of the Future* bei der U.S. Army im Einsatz (Myers u. a. 2011). *Siri* setzt Maßstäbe für die weitere Entwicklung von VPAs. Die Konkurrenz-Dienste, wie beispielsweise *AIVC* und *iris.*, ähneln *Siri* sehr im Funktionsumfang und Bedienkonzept. Der Konkurrenzdienst *Skyvi* wird direkt als *Siri*-Alternative beworben.

„Hilft dir bei allem, was du so machst"

Für den empirischen Teil der Diplomarbeit habe ich *Siri* in der Version vom August 2010 untersucht. Der Funktionsumfang, was insbesondere die Delegation von Aufgaben angeht, unterscheidet sich nur geringfügig von der im aktuellen iOS6 integrierten Version (Stand: Dezember 2012). Der VPA, welcher nicht nur eine Internet-Verbindung voraussetzt, ist außerdem von einer Reihe von Webdiensten abhängig, die je nach Land und Stadt unterschiedlich verfügbar sind. Zum Beispiel kann *Siri* in New York City problemlos einen Tisch in einem Restaurant reservieren, wohingegen es für Hamburg lediglich Empfehlungen anzeigt.

Die sprecherInnen-unabhängige Spracherkennung und die Sprachausgabe suggerieren, *Siri* sei *wie* ein menschlicher Assistent. In meiner empirischen Untersuchung gehe ich in Anschluss an Suchman (2007) von der Prämisse aus, dass Mensch-Maschine-Schnittstellen keine statischen Objekte sind, sondern Prozesse in denen die Identitäten von NutzerInnen und VPAs ausgehandelt werden. Ich komme zu dem Ergebnis, dass *Siri* in der Interaktion sowohl anthropomorphisiert als auch maschinisiert wird, was seinen Status als Zwischenwesen bestätigt. Mit der Anthropomorphisierung wird *Siri* weiblich vergeschlechtlicht. Der VPA verkörpert das Ideal einer perfekten Servicekraft,

Göde Both

Göde Both berichtete in der FIfF-Kommunikation 3/2011 über die 6. Europäische Gender & ICT-Konferenz. Der Diplom-Informatiker arbeitet an der Schnittstelle von Geschlechterforschung in der Informatik und sozialwissenschaftlicher Wissenschafts- und Technikforschung. Seit April 2012 ist er Wissenschaftlicher Mitarbeiter bei Prof.'in Jutta Weber im Arbeitsschwerpunkt Mediensoziologie an der Universität Paderborn. In seinem Dissertationsprojekt untersucht er die Verschränkung von Technik, Kultur und Gesellschaft in der Entwicklung selbststeuernder Autos.

welche stets freundlich und hilfsbereit ist. *Siri* macht jedoch bestimmte Vorgaben an die NutzerInnen: Neben den ökonomischen Ressourcen, einer dialektfreien Aussprache und für die Benutzung notwendiger Medienkompetenz, müssen die AnwenderInnen lernen, *wie* sie ihre Wünsche zu formulieren haben, um *Siri* zur gewünschten Aktion zu bringen. Das beinhaltet u. a. für die NutzerInnen, die in *Siri* eingeschriebene Sichtweise der Welt zu akzeptieren. Die *agency* der Anwenderin erschöpft sich in der Wahl zwischen den durch *Siri* vorgegebenen Aufgaben und bietet kaum Raum für eine kreative Aneignung. Die Arbeit kommt zu dem Ergebnis, dass der Nutzer als ein hochmobiler, wohlhabender Konsument konfiguriert wird, der relativ autonom seine Zeit gestalten kann. Das eingeschriebene, eher männliche NutzerInnen-Bild geht von einer Person aus, die sich häufig auf Geschäftsreisen befindet.

VPAs als aktuelle Figurationen von Arbeitsersparnisgeräten beruhen auf dem Mythos vom *technological fix*, wonach die Probleme der Überarbeitung und der Zeitknappheit infolge von entgrenzter Erwerbsarbeit technisch gelöst werden können. Dass unter dem Strich technische Helferlein nicht notwendigerweise ein Zeitgewinn mit sich ziehen, weist Ruth Schwartz Cowans in ihrer historischen Studie (1985) zum Einsatz von Haushaltstechnologien nach. Die aufgewendete Arbeitszeit für den Haushalt konnte ihr zufolge trotz Automatisierung nicht signifikant reduziert werden. Dies legt nahe, dass die implizite Gleichsetzung von Fortschritt mit Verbesserung einerseits und Arbeitsersparnis mit Zeitgewinn anderseits auch im Zusammenhang von VPAs hinterfragt werden muss.

VPAs manifestieren die Phantasien und Begehren der Dienstleistungsökonomie. Die Vorstellung, dass es jemanden oder etwas gibt, der/die/das uns die Arbeit abnimmt und *unser* aller Leben leichter macht, setzt eine ungleiche Verteilung von Reichtum und Macht voraus. Es wirft die Frage auf, wer dieses *uns* verkörpert und wer die Dienstleistungen erbringt. Die Diplomarbeit problematisiert in den Figurationen der VPAs weniger die Auflösung der Grenze zwischen Mensch und Maschine, sondern das, was sie affirmieren: Die Annahme, dass eine Klasse von Dienstleistungswesen, menschlich und nicht-menschlich, wünschenswert ist, die für eine privilegierte Gruppe von Menschen Dienstleistungen erbringen. Die menschliche Arbeit verschwindet durch VPAs nicht, sie wird nur anders verteilt. In der Hardware für *Siri* steckt die Arbeitskraft von WanderarbeiterInnen in der Freihandelszone Shenzen, die in geschlechterhierarchischer Arbeitsteilung und unter z.T. menschenunwürdigen Arbeitsbedingungen die Geräte montieren. Aber auch die Delegation von Aufgaben, wie dem Taxiruf oder Restaurantreservierung setzt menschliche Servicekräfte voraus, welche für die NutzerInnen teils sichtbar, teils unsichtbar ihre Arbeit verrichten.

Fazit

Der in der vorliegenden Arbeit vorgestellte Ansatz zur Untersuchung von Mensch/Maschine-Konfigurationen ist nicht auf VPAs und andere Software-AgentInnen beschränkt. Mit den Analysekategorien Geschlecht und *agency* kann generell beschrieben werden, wie Handlungen zwischen Menschen und Informationstechnik hin und her verschoben werden und welche Implikationen sich für die symbolisch-strukturelle Geschlechterordnung ergeben. Darüber hinaus fokussiert der Ansatz darauf, wie die vergeschlechtlichten Identitäten der NutzerInnen produziert werden und welche Verhaltensweisen den NutzerInnen nahe gelegt werden, damit ein spezifisches informatisches Artefakt von ihnen genutzt werden kann. Die Analysekategorien Geschlecht und *agency* eignen sich insbesondere für die Untersuchung von Informationstechnologien, welche in der Dienstleistungsbranche, der Industrie, dem Handel und dem Gesundheitswesen zum Einsatz kommen.

Aus den Ergebnissen dieser Arbeit lassen sich Verbesserungspotentiale für VPAs im Allgemeinen und *Siri* im Besonderen ableiten: Die Einschränkung auf überwiegend männlich-konnotierte Bedürfnisse könnte zu Gunsten von inklusiveren NutzerInnen-Bildern aufgebrochen werden. Die Produktion der Hardware sollte unter menschenwürdigen Arbeitsbedingungen erfolgen. Eine kritische Reflexion von Geschlechter-Stereotypen müsste anstelle ihrer unreflektierten Wiederholung im Zusammenhang mit VPAs und anderen anthropomorphen Software-AgentInnen treten. Eine Ent-Vergeschlechtlichung von *Siri* hat jedoch ihre Grenzen. Das Verständnis von der Ko-Materialisierung von Geschlecht und Technik widerstrebt der groben Vereinfachung eines Ursache-Wirkung-Prinzips. Die spezifischen Mensch/Maschine-Konfigurationen und ihre Implikationen für die symbolisch-strukturelle Geschlechterordnung sind nur bedingt das Resultat einer ‚schlechten' oder ‚guten' Technikgestaltung. Die Einschreibungen von traditionellen Geschlechternormen und der geschlechtsspezifischen Arbeitsteilung weisen darauf hin, dass eine Verbesserung *Siris* nur im Zusammenhang mit weitreichenden gesellschaftlichen Veränderungen denkbar wäre.

Referenzen

Bath, Corinna. 2013. Informatik und Geschlecht: Grundlagen einer feministischen Technikgestaltung. Bielefeld: Transcript (im Erscheinen).

Bath, Corinna, Heidi Schelhowe, und Heike Wiesner. 2010. „Informatik: Geschlechteraspekte einer technischen Disziplin". In Handbuch Frauen- und Geschlechterforschung, hrsg. von Ruth Becker und Beate Kortendiek, 829–841. Wiesbaden: VS Verlag für Sozialwissenschaften.

Berszinski, S., R. Messmer, K. Nicoleyczik, B. Remmele, E. Ruiz Ben, B. Schinzel, S. Schmitz, B. Stingl, R. Swadosch, und S. Vossen. 2002. „Geschlecht (SexGender): Geschlechterforschung in der Informatik und an ihren Schnittstellen". FIfF-Kommunikation Jg. 2002 (3): 32–37.

Both, Göde. 2011. „Agency und Geschlecht in Mensch/Maschine-Konfigurationen am Beispiel von Virtual Personal Assistants". Humboldt-Universität zu Berlin. http://edoc.hu-berlin.de/master/both-goede-2011-07-19/PDF/both.pdf [letzter Zugriff: 29.12.12]

Cendrowski, Mark. 2012. „The Beta Test Initiation". TV-Serie. Big Bang Theory.

Cheyer, Adam, und Tom Gruber. 2010. „Siri: An Ontology-driven Application for the Masses" gehalten auf der Ontolog am 25. Februar 2010. http://ontolog.cim3.net/cgi-bin/wiki.pl?ConferenceCall_2010_02_25 [letzter Zugriff: 29.12.12].

Cowan, Ruth Schwartz. 1985. More work for mother: The ironies of household technology from the open hearth to the microwave. New York: Basic Books.

Coy, Wolfgang. 1992. „Für eine Theorie der Informatik!" In Sichtweisen der Informatik, hrsg. von Wolfgang Coy, Frieder Nake, Jörg-Martin Pflüger, Arno Rolf, Jürgen Seetzen, Dirk Siefkes, und Reinhard Stransfeld, 17–32. Braunschweig, Wiesbaden: Vieweg Verlagsgesellschaft.

Dubberly, Hugh, und Doris Mitch. 1987. The Knowledge Navigator, Apple Computer. http://vimeo.com/12143596 [letzter Zugriff: 29.12.12].

Latour, Bruno. 1992. „Where are the missing masses? The sociology of a few mundane objects". In Shaping Technology Building Society: Studies in Sociotechnical Change, hrsg. von Wiebe Bijker und John Law, 225–258. Cambridge, Massachusetts: MIT Press.

Laurel, Brenda. 1990. „Interface Agents. Metaphors with Character". In The art of human-computer interface design, hrsg. von Brenda Laurel, 355–365. New York: Addison-Wesley.

Myers, K., J. Kolojejchick, C. Angiolillo, T. Cummings, T. Garvey, M. Gervasio, W. Haines, C. Jones, J. Knittel, und D. Morley. 2011. „Learning by demonstration technology for military planning and decision making: A deployment story". In Proceedings of the 23rd Conference on Innovative Applications of Artificial Intelligence.

Negroponte, Nicholas. 1997. „Agents, From Direct Manipulation to Delegation". In Software agents, hrsg. von Bradshaw, Jeffrey M., 57–66. 2. Auflage. Menlo Park: AAAI Press.

Suchman, Lucy. 2007. Human-Machine Reconfigurations: Plans and Situated Actions. 2. erweiterte Auflage. Cambridge, New York, Melbourne: Cambridge University Press.

Anmerkungen

1 *Alle Zitate in den Zwischenüberschriften stammen von Apples deutschsprachiger Website (http://www.apple.com/de/ios/siri/ Letzer Zugriff: 27.12.12). Siri wird dort wie auf der englischsprachigen Website grammatisch im Neutrum behandelt.*

2 *Diese Einsicht verdanke ich Britta Schinzel.*

3 *Für eine Übersicht siehe (Berszinski u. a. 2002) und (Bath, Schelhowe, und Wiesner 2010).*

Stefanie Müller

FIfF-Studienpreis 2012
3. Preis

Informatik und Gesellschaft – ein zentraler Inhaltsbereich für den Informatikunterricht

Möglichkeiten und Grenzen allgegenwärtiger Datenverarbeitung schülerorientiert lehren

Ambient Intelligence is more than just a question of embedding technology into objects.
It involves human culture in its broadest sense – universal desires; complex social relationships;
different value systems; individual likes and dislikes; the sustainability of economic and natural ecosystems;
and codes of ethics, conduct and communication, both in civil society and in business.
Stefano Marzano 2001

Nie zuvor war ein Zeitalter einem so dynamischen Wandel hinsichtlich neuer Technologien unterworfen, wie das aktuelle. Während Medien wie die Zeitung oder technische Erfindungen wie die Schreibmaschine viele Jahre zur gesamtgesellschaftlichen Etablierung benötigten, wurden Innovationen der Informatik, wie das Internet oder mobile smarte Anwendungen, vergleichsweise rasend schnell zum Gegenstand des alltäglichen Gebrauchs. Diese hohe Dynamik der technischen, sozialen und kulturellen Umwelt ist ein Kennzeichen unserer modernen Gesellschaft. Eingesetzte Anwendungen allgegenwärtiger Informations- und Kommunikationstechnik führen zu vielfältigen positiven Effekten, erhöhen jedoch in vielen Lebensbereichen auch die Komplexität, Undurchschaubarkeit, und Durchlässigkeit. Sie beeinträchtigen außerdem deren Sicherheit und haben Auswirkungen auf Selbstbestimmung, Umweltbelastung sowie auf soziale Aspekte.

Laut Rutz gerät „angesichts von Technologien, die innerhalb von wenigen Jahren das soziale und ökonomische Leben verändern können […] die ‚normale' Ausbildung zu einer Farce." [Rutz 1999]

Gerade für den Informatikunterricht wird es zunehmend schwieriger, relevante fachliche Inhalte zu finden, die keinem ständigen Wandel unterworfen sind. Umso wichtiger wird die Ausbildung von Kompetenzen, die Jugendliche dazu befähigen, mit neuen Technologien verantwortungsbewusst und kritisch umzugehen, sich Inhalte selbstständig anzueignen, und somit lebenslanges Lernen zu gewährleisten.

Aufgrund der Zunahme des IT-Einflusses auf unser tägliches Leben und die immer stärker spürbaren Wechselwirkungen zwischen Informatik und Gesellschaft wird die Thematisierung von Inhalten aus dem Bereich *Informatik und Gesellschaft* und die hiermit erzielbaren Kompetenzen immer entscheidender. Leider findet die Behandlung des Inhaltsbereichs in der Praxis des Informatikunterrichts in vielen Schulen kaum oder nur am Rande statt und ist in den Rahmenlehrplänen einiger Bundesländer nach meiner Untersuchung schlichtweg nicht zu finden. Um einen kleinen Beitrag zur Behebung dieses Missverhältnisses zu leisten, setzt sich meine Staatsexamensarbeit mit *Informatik und Gesellschaft* im schulischen Kontext auseinander. Insbesondere die von mir erstellte Handreichung für Lehrkräfte soll eine schnelle und unkomplizierte Einarbeitung ins Thema gewährleisten und eine wertvolle Stütze im Unterricht sein.

Dieser Beitrag hat das Ziel, die Inhalte und Forschungsergebnisse meiner Abschlussarbeit kurz zu umreißen und will anhand der gewählten Thematik *Ubiquitous Computing* exemplarisch aufzeigen, wie Schüler zum reflektierten Umgang mit Informatiksystemen in ihrer täglichen Lebenswelt befähigt werden können.

Kompetenzgewinne im Lernbereich *Informatik und Gesellschaft*

Jugendliche wachsen ganz selbstverständlich mit neuen, im Alltag allgegenwärtigen Informations- und Kommunikationssys-

temen auf und nutzen diese für sich intensiv und regelmäßig. Aufgrund ihrer mangelnden Lebenserfahrung und Weitsicht reflektieren sie die Nutzung von allgegenwärtigen Informationstechnologien kaum, und können deren direkte und indirekte Folgen nur schwer abschätzen.

Als Ergebnis meiner Staatsexamensarbeit konnte ich unter anderem bestätigen, dass es möglich ist, an Unterrichtsthemen aus dem Inhaltsbereich *Informatik und Gesellschaft* gerade die Schlüsselqualifikationen auszubilden, die für einen verantwortungsvollen und kritischen Umgang mit Computersystemen wünschenswert sind [Müller 2011, S. 22]. Hierbei erfüllt der Lernbereich *Informatik und Gesellschaft* alle von Klieme [Klieme 2003, S. 79f.] angeführten Kriterien für einen erfolgreichen Kompetenzerwerb.

In *Informatik und Gesellschaft* wird an einem konkreten, gegenwärtigen gesellschaftlichen Gegenstand gearbeitet. Hierbei gilt es besonders, die Wechselwirkungen dieses Gegenstandes innerhalb unserer Gesellschaft zu analysieren, dessen Folgen abzuschätzen und daraufhin zu bewerten. Bei der Bemühung, Schüler bei der Ausbildung von allgemeinen Lern- und Denkstrategien (also metastrategischem Wissen) zu unterstützen, muss bedacht werden, dass diese Strategien „lernbar aber nicht direkt lehrbar" [Stern 2006, S. 47] sind. Die Kognitionsforschung hat belegt, dass diese nur in Bezug zu anspruchsvollen, authentischen Inhalten entwickelt werden können [Stern 2006, S. 46].

Da gerade im Bereich *Informatik und Gesellschaft* die Entwicklungen der Informatik mit ihren Wechselwirkungen auf und durch die Gesellschaft betrachtet werden, wird der kulturelle Kontext, innerhalb dessen Lernprozesse ablaufen, bedacht.

Wenn der Inhalt im Lernbereich *Informatik und Gesellschaft* Bezug zum aktuellen Geschehen hat und für die Schüler begreifbar ist – besser noch: sie direkt betrifft, machen sie innerhalb des gewählten Gegenstandsbereiches Lernerfahrungen, die für sie selbst relevant sind und bilden Eigen- und Sozialkompetenzen aus, die für ihre Entwicklung essentiell sind und heutzutage von so vielen Seiten der Berufswelt gerade auch für Informatiker gefordert werden.

Die nachfolgende Aufzählung enthält wesentliche Kriterien, welche bei der Wahl von Unterrichtsthemen erfüllt sein sollten. Themen, die sich aus meiner Sicht in besonderem Maße für den Einsatz im Unterricht eignen:

- sind möglichst aktuell,
- beziehen sich auf die Lebenswelt der Schüler,
- weisen eine Relevanz für die Gesamtgesellschaft auf,
- enthalten informatische Inhalte, die auf unterschiedlichen Niveaustufen vermittelbar sind,
- können von verschiedenen Perspektiven aus betrachtet werden und
- in einen bestimmten Rahmen eingegrenzt und hierdurch von anderen Themen abgegrenzt werden.

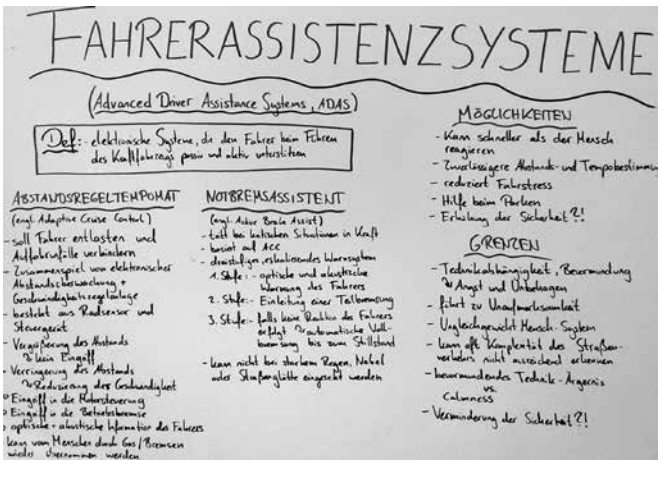
Im Weiteren seien beispielgebend einige Themen genannt, welche die aufgeführten Kriterien erfüllen und sich auch deshalb sehr gut für den Einsatz im Informatikunterricht eignen, da man an ihnen die rein technisch-informatischen Inhalte gemeinsam mit den Wechselwirkungen auf und durch die Gesellschaft thematisieren kann.

- Anhand der *elektronischen Kommunikation (von Jugendlichen)* lassen sich die verschiedenen Aus- und Wechselwirkungen dieser auf die Gesellschaft multiperspektivisch beleuchten. Da zu einzelnen Aspekten dieser Thematik bereits eine Fülle von Unterrichtsmaterial vorhanden ist, habe ich erste Vorschläge zur Umsetzung im Unterricht erarbeitet [Müller, 2010] und in einer Linksammlung festgehalten (online abrufbar unter: *http://www.informatikundgesellschaft.de/elekomm.html)*. Reichlich Potenzial bietet hierbei insbesondere die Behandlung von *Sozialen Netzwerken* als eigenständigen Schwerpunkt, welcher sich von der reinen Webanwendung bis hin zu deren weitreichenden sozialen Veränderungen betrachten lässt.

- Die Thematik *Informatik im Dienst des Militärs* bietet sich besonders für historische Betrachtungen in der Oberstufe und Sensibilisierung der Schüler für die Problematik des *Dual Use* an.

- Im Bereich der *Künstlichen Intelligenz* erscheint mir die Arbeit mit *Chatbots* sinnvoll, um bei den Schülern ein Grundverständnis für Vorgehensweise bei der Simulation von natürlicher Sprache anzubahnen. Am Thema *Robotik* und einer Vertiefung auf dem Gebiet der *humanoiden Roboter* werden ethische Konflikte für Entwickler und Anwender besonders deutlich, welche für Unterrichtsdiskussionen jeglicher Art (angefangen von Stimmungsabfragen und Meinungsbildern bis hin zu Pro-Kontra-Diskussionen und Amerikanischen Debatten) genutzt werden können.

- Elektronische Karten und deren Chips sind für eine Behandlung im Unterricht ebenfalls prädestiniert, da auch an diesem Thema mit den Schülern weitreichende Fragestellungen bearbeitet werden können: Welche „Vorteile" bieten Kunden- oder Mitgliedskarten, die Zutrittskontrolle und Leistungsabrechnung über elektronische Eintrittskarten, die eGK, ePass oder Coin Chip wirklich? Warum ist das Einkaufen und Bargeldversorgung mit der EC-Karte aus unserem Leben nicht mehr weg zu denken? Welche Informationen enthalten all diese Karten, wer hat Zugriff darauf und wie sicher sind meine persönlichen Daten?



- Wie *allgegenwärtig Informatiksysteme* in unserem Alltagsleben heute bereits sind und welche *Allmachtsfantasien, Auswirkungen und Abhängigkeiten* mit ihnen verknüpft werden, habe ich in meiner Staatsexamensarbeit untersucht. Als Zielsetzung der Unterrichtsreihe wurden folgende inhaltliche Kompetenzen für Schüler der Oberstufe zu Grunde gelegt: Schülerinnen und Schüler können Wechselwirkungen zwischen Informatiksystemen und ihrer gesellschaftlichen Einbettung benennen und beurteilen; kennen die weitreichende Bedeutung von humanistischen Werten in der Gesellschaft; wissen, dass diese durch unangemessenen Einsatz von Informatiksystemen bedroht werden können; und können angemessen auf Risiken bei der Nutzung von Informatiksystemen reagieren.

Datenverarbeitung ständig und überall – die Vision des *Ubiquitous Computing*

In diesem Abschnitt möchte ich die Vision des *Ubiquitous Computing* kurz umreißen, um danach die Auswahl der Inhalte in der von mir konzipierten Handreichung für Lehrkräfte zu begründen.

Im Rahmen seiner wissenschaftlichen Tätigkeit am Forschungszentrum PARC entwickelte der amerikanische Informatiker Dr. Mark Weiser die Vision des *Ubiquitous Computing* und publizierte sie erstmals 1991. In seiner Zukunftsprognose beschreibt er [Weiser, 1991] die Vision der allgegenwärtigen Datenverarbeitung, welche den (Personal)- Computer zu Gunsten von Alltagsgegenständen, die mit Computertechnik ausgestattet sind, verschwinden lässt.

Nach der Wortbedeutung von „Ubiquität" besitzen ubiquitäre Systeme zwei grundsätzliche Merkmale: Sie sind ständig präsent und nicht standortgebunden.

Für computergesteuerte Informationssysteme bedeutet dies idealtypisch: Daten und Datenverarbeitung sind zu jedem Zeitpunkt des Zugriffs verfügbar und an jedem beliebigen Standort abrufbar. Daraus folgt: Daten sind weder hinsichtlich ihrer Ansteuerung, Verarbeitung oder ihrem Nutzen an die Grenzen eines Standorts gebunden. Um dies zu verwirklichen, müssen Daten ständig erhoben, miteinander vernetzt, in Beziehung gesetzt und ausgegeben werden können.

Aus diesen Anforderungen heraus verschwindet der Computer in Form eines eigenständigen Gerätes. Stattdessen wird Mikroelektronik derart in Alltagsgegenstände eingebettet, dass der Nutzer weder die eingebaute Computertechnik, noch deren Vernetzung wahrnimmt.

Die Forschungsdisziplin *Ubiquitous Computing* befasst sich mit den Möglichkeiten dieser Vernetzung, Verarbeitung, der (mobilen) Abfrage und entwickelt Szenarios sowie Zukunftsvisionen zu deren Auswirkung auf Individuum, Gesellschaft und Umwelt.

Aufbau und Inhalt der Lehrerhandreichung zur allgegenwärtigen Datenverarbeitung

Die im Rahmen der Staatsexamensarbeit entwickelte Lehrerhandreichung ist prinzipiell zweigeteilt: Zu Beginn jedes Bereiches erleichtert eine Fachinformation die inhaltliche Einarbeitung für die Lehrkraft und bietet kurze Artikel mit Links und Materialhinweisen für vertiefende Informationen zu jedem Themenschwerpunkt. Danach folgen konkrete Vorschläge für Aufgabenstellungen und Anregungen zur Durchführung des Unterrichts. Diese wurden bewusst allgemein gehalten, um offenes und flexibles Arbeiten (beispielsweise in Projektform) zu gewährleisten.

Die Handreichung besteht insgesamt aus fünf inhaltlichen Modulen, deren Inhalt ich nun kurz beschreibe.

Mit dem Einstiegsmodul wird das Interesse der Schüler an der Thematik geweckt, sodass diese neugierig, motiviert und eigenverantwortlich die weiteren Module des Unterrichtsprojektes bestreiten. Hauptziel ist es, das Schülerinnen und Schüler Computertechnik, die ihren Alltag erleichtert und bereichert, bewusst wahrnehmen.

Im Modul „Smarte Anwendungsgebiete" wird der Einsatz von Computersystemen in verschiedenen Bereichen des täglichen Lebens untersucht. Überblicksartig werden Anwendungsgebiete vorgestellt, in denen Informations- und Kommunikationstechnik bereits heute nicht nur zusätzlich und unterstützend wirkt, sondern so weit eingebettet ist, dass die einzelnen Anwendungen und deren Tätigkeiten ohne Systemeinsatz nicht mehr adäquat ausgeübt werden können. Ziel der Betrachtung ist die Feststellung, dass schon heute Computersysteme in nahezu allen Lebensbereichen zur Anwendung kommen und in diesen durch Übernahme vielfältiger Aufgaben unverzichtbar geworden sind.

Das dritte Modul legt die technischen Grundlagen für eine detaillierte Analyse der Anwendungen in den weiteren Modulen.

Stefanie Müller

Stefanie Müller studierte nach ihrem Abitur Informatik und Geschichte an der Friedrich-Schiller-Universität Jena und ist lehrbefähigt für das Fach Medienkunde. Bei ihrer Mitarbeit am »Förderprogramm Demokratisch Handeln« in Jena entdeckte sie ihre Vorliebe für die projektbezogene Arbeit mit Schülerinnen und Schülern. Derzeit ist sie 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 auseinander zu setzten, weshalb sie diese Thematik auch für ihre Staatsexamensarbeit wählte, welche 2012 vom FIfF ausgezeichnet wurde. Sie ist Mitglied im FIfF und der GI.

Hierbei werden vier Schlüsseltechnologien allgegenwärtiger Datenverarbeitung betrachtet:

Es werden Sensornetzwerke als Voraussetzung für „intelligente“ Umgebungen, RFID-Systeme als Möglichkeit zur allgegenwärtigen Identifikation und Überwachung, Möglichkeiten zweidimensionaler Codierung sowie *Wearable Computing* als Technologie für tragbare Computersysteme am und im Körper thematisiert. Aufbau und grundlegende Funktionsweise der drei Technologien werden von den Schülern selbst erarbeitet.

Das Modul vier besteht aus sechs narrativ angelegten Szenarios welche dabei helfen, Chancen und Risiken der dargestellten Systeme an einem speziellen Anwendungsfall zu erkennen und zu diskutieren. Die gesammelten Erkenntnisse können danach in den Gesamtzusammenhang der Alltagswelt eingeordnet werden und wirken unterstützend, um allgemeingültige Aussagen über positive und negative Aspekte von Technologien zu treffen. Somit dienen die Szenarios aus Medizin und Gesundheitswesen bzw. Verkehrswesen dazu, subjektive Bewertungen und Abschätzungen von Technologiefolgen vorzunehmen.

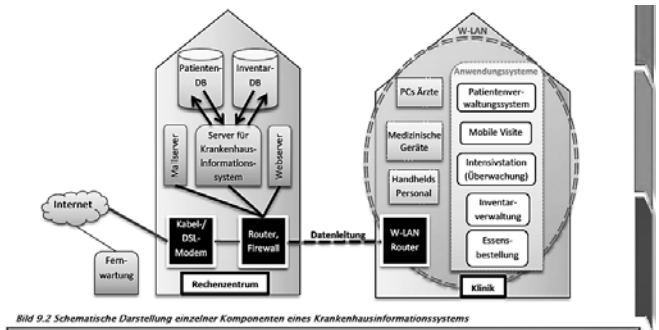


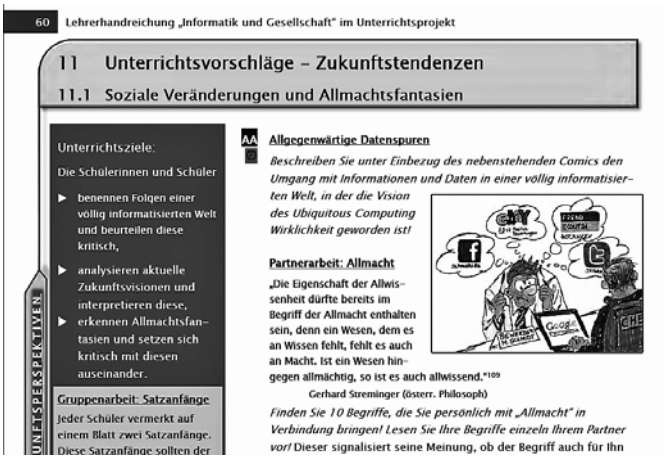
Bild 9.2 Schematische Darstellung einzelner Komponenten eines Krankenhausinformationssystems

IN KÜRZE: Der Einsatz von allgegenwärtigen Krankenhausinformationssystemen bedeutet für Kliniken ein hohes Einsparungspotenzial und eine Grundlage zur Qualitätsverbesserung, was zum Ausbau dieser Systeme führt. Die Sammlung aller behandlungs- und abrechnungsrelevanten Daten in elektronischer Form und deren Vernetzung bieten Ärzten neue Formen der Zusammenarbeit im gesamten Behandlungsprozess.

Mit dem letzten Modul „Ausblick“ können gesamtgesellschaftliche Folgen von ubiquitärer Computertechnik sowie Folgen für Natur und Umwelt im Unterricht betrachtet werden. Schwerpunkt der Analyse sind nicht nur derzeit bereits mess- und spürbare Auswirkungen, sondern auch Zukunftstendenzen. Hieran können aktuell populäre Zukunftsprognosen untersucht und historische Vorhersagen auf deren Eintreten überprüft werden. Anhand der dabei gewonnenen Erkenntnisse wird deutlich, dass eine detaillierte Vorhersage zukünftiger Technologien kaum möglich ist und somit Langzeitfolgen derzeitiger Entwicklungen nicht hinreichend abgeschätzt werden können. Hieraus lassen sich Maßnahmen für eine verantwortungsbewusste und sozialverträgliche Technikgestaltung ableiten.

Bisherige Erfahrungen und Erprobungen im Informatikunterricht

Erste positive Erfahrungen zur Gestaltung von Unterricht zur Thematik *Ubiquitous Computing* habe ich bereits mit meinen beiden Informatikkursen der Jahrgangsstufe 12 am Staatlichen Gymnasium in Schleiz sammeln können. Da es aus organisatorischen Gründen nicht möglich war, den Unterricht projektorientiert zu gestalten, habe ich diesen zur üblichen Unterrichtzeit


60 Lehrerhandreichung „Informatik und Gesellschaft“ im Unterrichtsprojekt

11 Unterrichtsvorschläge – Zukunftstendenzen

11.1 Soziale Veränderungen und Allmachtsfantasien

Unterrichtsziele:
Die Schülerinnen und Schüler
- benennen Folgen einer völlig informatisierten Welt und beurteilen diese kritisch,
- analysieren aktuelle Zukunftsvisionen und interpretieren diese,
- erkennen Allmachtsfantasien und setzen sich kritisch mit diesen auseinander.

Gruppenarbeit: Satzanfänge
Jeder Schüler vermerkt auf einem Blatt zwei Satzanfänge. Diese Satzanfänge sollten der

UNTERSPERSPEKTIVEN

Allgegenwärtige Datenspuren
Beschreiben Sie unter Einbezug des nebenstehenden Comics den Umgang mit Informationen und Daten in einer völlig informatisierten Welt, in der die Vision des Ubiquitous Computing Wirklichkeit geworden ist!

Partnerarbeit: Allmacht
„Die Eigenschaft der Allwissenheit dürfte bereits im Begriff der Allmacht enthalten sein, denn ein Wesen, dem es an Wissen fehlt, fehlt es auch an Macht. Ist ein Wesen hingegen allmächtig, so ist es auch allwissend.“[109]
Gerhard Streminger (österr. Philosoph)
Finden Sie 10 Begriffe, die Sie persönlich mit „Allmacht“ in Verbindung bringen! Lesen Sie Ihre Begriffe einzeln Ihrem Partner vor! Dieser signalisiert seine Meinung, ob der Begriff auch für Ihn

mit insgesamt 14 Unterrichtsstunden je Kurs durchgeführt. Erstaunlicherweise konnten die angestrebten Kompetenzen mit Hilfe der Materialien und mit ausgewählten Arbeitsaufträgen der Lehrerhandreichung auch in dieser sehr verkürzten Unterrichtzeit erreicht werden. Auch von Seiten des Staatlichen Studienseminars für Lehrerausbildung Gera (Außenstelle Jena) habe ich nach zweimaligen Unterrichtsbesuchen sehr positive Resonanzen erhalten.

Einen noch umfangreicheren Erfahrungsschatz konnte ich mit Eberhard Zehendner, dem Betreuer meiner Staatsexamensarbeit im Sommer 2012 bei der gemeinsamen Gestaltung eines zweiwöchigen Kurses für hochbegabte Jugendliche sammeln. Unter dem Motto „Allgegenwärtige Informatik – Überall sind Computer ... vielleicht sogar in mir?“ unterrichteten wir Jugendliche der siebten bis neunten Jahrgangsstufe im Rahmen der Juniorakademie im Bildungscamp Zella-Mehlis. Auch für die Juniorakademie 2013 ist ein gemeinsamer Kurs unter dem Motto „Allgegenwärtige Informatik – Plastikkarten, Codes und kluge Netze“ geplant.

Außerdem hoffe ich, dass mit der Herausgabe der Lehrerhandreichung durch das Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien Bad Berka *(http://www.thillm.de)* zahlreiche Lehrerinnen und Lehrer motiviert werden, Teile der Handreichung in ihrem Unterricht einzusetzen und durch ihre Rückmeldung helfen, diese weiterzuentwickeln.

Die Lehrerhandreichung ist in gedruckter Form (kurze Anfrage an *stefanie.mueller.3@uni-jena.de)* oder digital unter der Adresse *http://www.informatikundgesellschaft.de* erhältlich. Ich

freue mich sehr über Feedback zum Inhalt oder Aufbau der Handreichung und auf zahlreiche Unterrichtserfahrungen.

Ein herzliches Dankeschön an dieser Stelle dem gesamten FIfF für die Prämierung meiner Staatsexamensarbeit! Einen ganz besonderen Dank möchte ich an Phillip W. Brunst und Britta Schinzel für ihre Mühe und die bewegende Laudatio in Fulda richten!

Referenzen

[Klieme 2003] Klieme, Eckhard u. a.: Bildungsreform. Zur Entwicklung nationaler Bildungsstandards – Eine Expertise. 2. unveränderte Aufl./BMBF, (Hrsg.). Bonn, 2003, Bd. 1.

[Kündig 2008] Kündig, Albert. 2008. Selbständige Computer: Um was geht es? [Buchverf.] Albert Kündig und Danielle Bütschi. [Hrsg.] Albert Kündig und Danielle Bütschi. Die Verselbständigung des Computers. Zürich : vdf Hochschulverlag AG, 2008, S. 9-28.

[Müller 2010] Stefanie Müller: „Informatik und Gesellschaft" unterrichten – Betrachtung von Auswirkungen der Informationsgesellschaft anhand elektronischer Kommunikation von Jugendlichen. Projektarbeit Lehramt Informatik, Friedrich-Schiller-Universität Jena, 2010. Abrufbar über http://www.informatikundgesellschaft.de

[Müller 2011] Stefanie Müller: Das Thema „Informatik und Gesellschaft" als Unterrichtsprojekt – Erarbeitung einer Lehrerhandreichung zur Allgegenwärtigkeit, zu Allmachtsfantasien und Auswirkungen von Computersystemen in unserer heutigen Gesellschaft. Wissenschaftliche Hausarbeit im Fach Informatik zur Ersten Staatsprüfung für das Lehramt an Gymnasien, Friedrich-Schiller-Universität Jena, 2011. Erhältlich z. B. über das Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (Thillm) Bad Berka. http://www.thillm.de

[Rutz 1999] Rutz, Michael. 1999. Die Byte-Gesellschaft. Informationstechnologie verändert unser Leben. München: Olzog Verlag, 1999.

[Stern 2006] Stern, Elsbeth: »Lernen. Was wissen wir über erfolgreiches Lernen in der Schule?«. In: PÄDAGOGIK, Bd. 58, Nr. Sonderdruck, Serie: Bildungsforschung und Schule, S. 45-49, Jan. 2006.

[Weiser 1991] Weiser, Mark. 1991. The Computer for the 21st Century. [Online] September 1991. [Zitat vom: 14. April 2011] http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html.

Angel Tchorbadjiiski

FIfF-Studienpreis 2012 3. Preis

Liquid Democracy

Konzept zur kryptographischen Absicherung

Das Liquid-Democracy-Konzept ist in letzter Zeit durch verschiedene Institutionen (Enquête-Kommission, Munich Open Government Day) und auch durch den Einsatz bei der Piratenpartei Deutschland bekannt geworden. Die beiden meistverbreiteten Software-Implementierungen des Konzepts sind LiquidFeedback *und* Adhocracy*, welche ihren Nutzern verschiedene Diskussionsmöglichkeiten anbieten. Es können Vorschläge gemacht werden und über diese lässt sich abstimmen. Das Augenmerk beider Implementierungen liegt auf der Diskussion. Das führt zu verschiedenen Problemen bezüglich der Anonymität und Geheimhaltung der Abstimmungen und der Sicherheit der Systeme.*

Anforderungen an das System

Das Liquid-Democracy-Konzept bietet eine sehr aktuelle und interessante Grundlage. Aus diesem Grund habe ich es mir zum Ziel meiner Diplomarbeit gesetzt, ein Wahlsystem zu entwerfen, welches auf dem Konzept basiert und folgende Anforderungen erfüllt:

- **Wahl über das Internet** – Die Abstimmung kann über ein unsicheres Netzwerk durchgeführt werden.
- **Anonymität** – Die im System vorhandenen Informationen erlauben es nicht, Wähler zu identifizieren oder eine Korrelation zwischen Wählern und Stimmen herzustellen.
- **Geheimhaltung und Integrität** – Die übertragenen Daten sollten nicht von Dritten gelesen oder unbemerkt manipuliert werden können.
- **Öffentliche Wahlergebnisse** – Nach der Wahl sollen die Ergebnisse in einer Form vorliegen, die es den Wählern erlaubt, die eigene Stimme zu überprüfen.
- **Authentifizierung und Autorisierung** – Es soll sichergestellt werden, dass jede Stimme von einem gültigen Wähler abgegeben worden ist.
- **Wahlberechtigungen nur an gültige Wähler** – Das System darf nur bei aktiver Mitwirkung von gültigen Wählern Wahlberechtigungen erstellen können. Anderweitig erstellte Berechtigungen werden mit einer hohen Wahrscheinlichkeit aufgedeckt.
- **Delegation –** Im System ist es möglich, die eigene Stimme einfach oder mehrfach (priorisiert) zu delegieren. Zusätzlich ist jederzeit eine Überstimmung/Zurücknahme der eigenen Stimme wieder möglich. Eine Zeit- oder Bereichsdelegierung sollte auch möglich sein.
- **Nichtabstreitbarkeit** – Jede Entität (Wahlregister, Wahlcomputer, Wähler), die an einer Aktion teilgenommen hat, kann das nicht abstreiten, weil Daten vorhanden sind, die das belegen. Bei einer Manipulation soll dadurch feststellbar sein, welche der Entitäten genau daran beteiligt war.

Obwohl die gemeinsame Entscheidungsfindung sicherlich einen sehr wichtigen Punkt darstellt, fand ich es persönlich spannender, ein sicheres System zu entwickeln, dass anonyme und geheime Abstimmungen über das Internet ermöglicht. Es ist dabei sehr wichtig, dass die zwischen Wähler, Wahlregister *(Voting Register, VR)* und Wahlcomputer *(Voting Computer, VC)* ausgetauschten Daten für Dritte nicht einsehbar oder manipulier-

bar sind. Weiter sollte sicher gestellt werden, dass alle Benutzer des Systems wirklich dazu berechtigt sind, an einer Wahl teilzunehmen, und jeweils nur einmal abstimmen können. Die Wahlergebnisse sollten veröffentlicht werden, was es jedem Benutzer ermöglicht, zu überprüfen, ob die eigene, abgegebene Stimme der entspricht, die in der Datenbank des VCs gespeichert ist. Dafür sollte bei Stimmenabgabe eine Quittung vom VC generiert werden, die von den ausgetauschten Daten abhängt und nicht von Dritten erratbar ist. Zu guter Letzt, aber nicht minder wichtig, sollte das System auf dem Liquid-Democracy-Konzept aufsetzen, wobei aber nicht nur Einfach-, prioritätbasierte Mehrfachdelegierung und Rücknahme einer Delegierung möglich sind, sondern auch Weitergabe des Stimmrechtes basierend auf Zeit oder Themengebiet. Dies würde den Wählern eine größere Flexibilität ermöglichen.

Systemarchitektur

Das im Laufe meiner Diplomarbeit entstandene System ist in Abbildung 1 dargestellt.

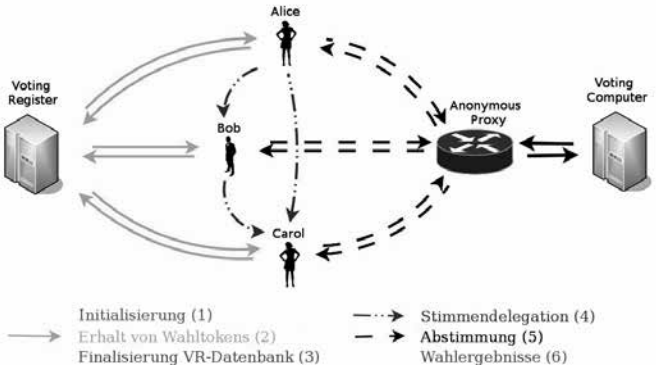


Abbildung 1: Systemarchitektur

Die VR-Instanz trägt Verantwortung für die Überprüfung der Wähleridentität, die Wahlberechtigung und die Vergabe von anonymen Wahltokens. Die Vergabe der Wahltokens ist physikalisch von der VR-Instanz getrennt, die anhand der Wahltokens entscheidet, ob ein Wähler zur Abstimmung berechtigt ist, die Stimmen speichert und die Wahlergebnisse öffentlich macht. Im Fall einer Manipulation ist es so möglich festzustellen, welche der Instanzen sich nicht an das Protokoll gehalten hat.

Der Abstimmungsprozess ist in sechs Phasen unterteilt (siehe Abbildung 1), wobei die folgenden Phasen eine Interaktion des Wählers erfordern:

Abstimmungsprozess

Phase 1 – Initialisierung

In dieser Phase werden die Datenbanken der Server (VR und VC) reinitialisiert und neue RSA-Schlüssel generiert. Dies entwertet explizit alle in der Vergangenheit vergebenen Wahltoken. Zusätzlich holt sich VR eine signierte aktuelle Liste der Wahlberechtigten (im weiteren WBL), die unter Anderem einen öffentlichen Schlüssel zu jeder der Personen enthalten muss. Diese werden in der nächsten Phase benötigt, um sicherzustellen, dass der VR nicht in der Lage ist, ohne Mitwirkung eines Wahlberechtigten gültige Wahltokens zu generieren.

Phase 2 – Erhalt von Wahltokens

Nachdem die Initialisierung abgeschlossen ist, kann jeder Wahlberechtigte mit dem VR in Verbindung treten und ein anonymes Wahltoken erhalten. Die Identität des Wählers wird mittels einer *Challenge-Response-Authentifizierung* bestimmt, basierend auf den in Phase 1 erwähnten öffentlichen RSA-Schlüssel. Die Response ist dabei mit dem privaten Schlüssel des Wählers signiert, sodass eine aktive Teilnahme nachgewiesen werden kann.

Um die Anonymität des Systems zu gewährleisten, muss jeder Wähler eine eigene *Hash-Kette* (wird anhand eines Beispiels in Phase 4 erklärt) generieren. Das letzte Element dieser Kette wird vom VR über blinde Signatur mit dem privaten RSA-Schlüssel des VR-Servers unterschrieben. Dies ist das Wahltoken, welches die Berechtigung für die spätere Abstimmung darstellt.

Phase 3 – Finalisieren der VR-Datenbank

Es muss sichergestellt werden, dass VR die Wählerliste nicht nachträglich verändern kann. Um dies zu gewährleisten, wird die Identität der Person, der dazugehörige öffentliche Schlüssel, die von VR gesendete Challenge (zum Beispiel Zeitstempel) und die vom Benutzer signierte Response veröffentlicht. So kann jede/r überprüfen, ob jede in der Liste aufgeführte Identität ein Token erhalten hat. Ist die Signatur der Response ungültig, hat eine Manipulation stattgefunden.

Phase 4 – Stimmendelegation

Will beispielsweise die Wählerin Alice ihre Stimme mit unterschiedlicher Priorität an die Personen Bob und Carol weitergeben, muss sie in Besitz einer Hash-Kette sein. Diese wird, wie in Abbildung 2 dargestellt, durch iteratives Anwenden einer kryptographischen Hash-Funktion $h()$ auf ein nur Alice bekanntes Element h_S generiert.

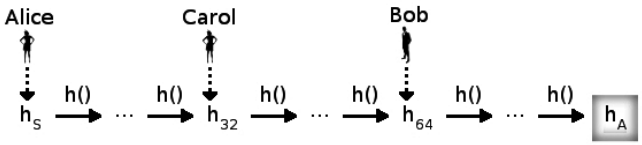


Abbildung 2: Verwendung von Hash-Ketten zur priorisierten Delegierung

Erhält Carol das Tupel (h_{32}, h_A) und Bob (h_{64}, h_A), so können sie beide anstelle von Alice abstimmen. Je weiter das erste Element des Tupels von dem Anker (letztes Element) entfernt ist, desto höher ist die Priorität. Da Alice in Besitz der Elemente h_S bis h_{31} ist, kann sie jederzeit mit einem dieser Tupel überstimmen, was als Rücknahme der delegierten Stimme anzusehen ist.

Um Zeit- oder Bereichsdelegierung zu ermöglichen, kann anstelle einer einfachen Hash-Kette auch ein Merke-Baum (Hash-Baum) verwendet werden. Dabei wird die Wurzel des Baumes, wie oben dargestellt, als Wahltoken verwendet, und die Blätter sind Hash-Ketten. Auf diese Weise kann zum Beispiel die eine Seite des Baumes verwendet werden, um verschiedene Delegierungsperioden zu definieren und die andere Seite, um Delegierungsbereiche vorzugeben.

Phase 5 – Abstimmung

Nach Abschluss der Delegierungsphase können alle Personen, die in Besitz einer gültigen Wahlberechtigung sind, beim VC eine Stimme abgeben.

Um die Identität des Wählers zu verschleiern, können anonyme Proxys eingesetzt werden. Dabei muss eine verschlüsselte Verbindung zwischen Wähler und VC hergestellt werden, die einerseits die Prüfung der Serveridentität ermöglicht, andererseits die Integrität und Geheimhaltung der übertragenen Daten gewährleistet.

Mit Hilfe des signierten Wahltokens kann VC feststellen, ob ein Wahlberechtigter vorliegt oder nicht. Mittels *Diffie-Hellmann-Key-Exchange* wird benötigtes Zufallsmaterial generiert, sodass sowohl VC als auch Wähler aktiv an diesem Prozess beteiligt sind.

Die eigentliche Stimmenabgabe erfordert ein kompliziertes kryptographisches Protokoll. Zuerst wird ein Commitment seitens des Wählers generiert, in dem die Zufallszahl und die Stimme enthalten sind. Diese werden mit einem Element der Hash-Kette verändert und dem VC zur blinden Unterschrift weitergegeben. Nachdem das Commitment unterschrieben worden ist, wird das verwendete Element dem VC verraten, damit die Stimme aufgenommen werden kann. Als letztes generiert der VC eine kryptographische Quittung, die von den ausgetauschten Daten und der vorherigen Server-Quittung abhängt. Diese kann bei einer erkannten Manipulation dazu verwendet werden, die Wahlergebnisse anzuzweifeln.

Phase 6 – Veröffentlichung der Wahlergebnisse

Der VC generiert zwei getrennte Listen. Die erste enthält die Wahltokens und die Elemente, die zum Maskieren der Wahl verwendet worden sind. So kann die Signatur des VRs und die Hash-Kette jedes einzelnen Wählers überprüft werden. Die zweite Liste enthält die Zufallszahl und die eigentliche Stimme. Da die Zufallszahl nur dem Wähler bekannt ist, kann kein anderer die Stimme mit der Identität des Wählers verbinden. Hat eine Manipulation stattgefunden, hängt die Wahrscheinlichkeit ihrer Entdeckung davon ab, wie viele Personen ihre Stimme überprüfen. Bei Wahlen mit mehr als einer Million Teilnehmern reicht etwa ein Prozent, um eine hundertprozentige Wahrscheinlichkeit einer Manipulationsentdeckung zu gewährleisten.

Nachteile

Wie bei jeder Wahl, die nicht in überwachten Wahllokalen stattfindet, ist es auch hier möglich, dass Stimmenkauf oder Erpressung von Wählern stattfinden. Da das System die Überprüfung der eigenen Stimme ermöglicht, kann das auch einem Käufer/Erpresser zu Gute kommen. Um dem entgegen zu wirken, können vertrauenswürdige Entitäten (trusted third parties) verwendet werden, die die Ergebnisse anstelle der Wähler überprüfen.

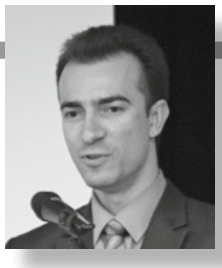
Ein weiterer Punkt betrifft die Sicherheit der Systeme, die von den Wählern verwendet werden. Ist das verwendete System unter der Kontrolle eines Angreifers, kann nicht sichergestellt werden, dass die abgegebene Stimme der gewollten Wahl entspricht. Um solche Angriffe zu verhindern, können Smartcards verwendet werden, die alle kryptographischen Operationen völlig autonom durchführen, sodass keine Manipulation auf der infizierten Maschine stattfinden kann. Weiter könnten Wähler eine CD mit einem bootfähigen Betriebssystem verwenden, das aktuell ist und mit sehr hoher Wahrscheinlichkeit nicht infiziert, um an einer Wahl teilzunehmen.

Um ein System zu erschaffen, das ein Augenmerk auf Sicherheit, Anonymität und Vertraulichkeit von Wahlen setzt und die oben aufgeführten Anforderungen erfüllt, habe ich verschiedene kryptographische Basisblöcke zu komplexen Protokollen kombiniert. Dadurch wirkt das System sehr undurchsichtig und erfordert Kenntnisse in Kryptographie, um den Abstimmungsprozess zu verstehen.

Fazit

Das während meiner Diplomarbeit entstandene System ermöglicht es, eine anonyme und geheime Wahl über das Internet durchzuführen. Ich habe mich mit Hilfe verschiedener kryptographischer Protokolle darum bemüht, die Sicherheit des Systems zu gewährleisten und jede Manipulation entdeckbar zu machen. Wegen der öffentlichen Wahlergebnisse ist jeder in der Lage, diese auf Korrektheit zu überprüfen, und falls eine Manipulation vorliegt, kann sichergestellt werden, welche Entität sich nicht an das Protokoll gehalten hat.

Angel Tchorbadjiiski



Angel Tchorbadjiiski hat an der Rheinisch-Westfälischen Technischen Hochschule (RWTH) Informatik auf Diplom studiert. Sein starkes Interesse an IT-Sicherheit wurde zum Studienschwerpunkt. Nebenbei nahm er mit einem Team von RWTH-Studenten regelmäßig an verschiedenen Capture-The-Flag-Wettbewerben wie Cipher *(http://www.cipher-ctf.org)*, iCTF *(http://ictf.cs.ucsb.edu/)* und RuCTFE *(http://ructf.org/e)* teil. Während und nach Abschluss seines Studiums arbeitete er als Penetrationstester.

Rainer Rehak, Constanze Kurz

Ohne besondere Sachkenntnis

Ein Kommentar zum dritten Platz des Studienpreises 2012

Der dritte Preis wurde an Angel Tchorbadjiiski für seine Diplomarbeit *Liquid Democracy* vergeben. In der Laudatio hieß es: „Sie [die Arbeit] stellt einen Bezug zu den Anforderungen des Wahlgesetzes her und zeigt auf, dass diese Anforderungen erfüllt werden können." Doch wird dieser Anspruch von der Arbeit erfüllt? Werfen wir einen kritischen Blick darauf.

Hätte sich die Arbeit allgemein mit der technischen Umsetzung von Abstimmungen und Wahlen durch Modifikation der bekanntesten Beteiligungsplattform *Adhocracy*[1] oder eines vergleichbaren technischen Partizipationswerkzeug beschäftigt, wäre sicher wenig an ihr zu kritisieren. Tchorbadjiiski betont jedoch mehrmals und explizit: "The system architecture [...] fulfills the [...] requirements and should satisfy the regulations in the German Constitution with respect to voting. It should therefore be usable for parliamentary elections." (S. 26, siehe auch S. 9, 25, 62 und 64). Die explizite Ausrichtung auf deutsche Wahlgesetze und rechtlich verbindliche demokratische Wahlen verlangt es zwingend, deren rechtlichen Rahmen in Deutschland zu betrachten. Und der ist keineswegs beschränkt auf das Bundeswahlgesetz (BWG).

Am 3. März 2009 verkündete der Zweite Senat des Bundesverfassungsgerichts ein Grundsatzurteil zum Einsatz von Wahlcomputern (2 BvC 3/07, 2 BvC 4/07). Der zweite Leitsatz daraus lautet:

> *„Beim Einsatz elektronischer Wahlgeräte müssen die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können."*

Ohne Zweifel ist dieser neue verfassungsrechtliche Grundsatz der Transparenz und Nachvollziehbarkeit des technischen Wahlverfahrens auf jegliche Form elektronischer Wahlen zu übertragen, sofern sie sich als demokratisch nach den Vorgaben der Verfassung verstehen.

Das von Angel Tchorbadjiiski in seiner Arbeit konstruierte Nutzungskonzept basiert auf einer Wahl von zu Hause aus, also mit dem eigenen Rechner über das Internet. Dafür hat sich der Begriff *Online-Wahl* durchgesetzt. Das in der Arbeit konstruierte Wahlsystem an sich funktioniert nur unter Nutzung anspruchsvoller kryptographischer Verfahren und Protokolle, die u. a. die gesicherte Verbindung des heimischen Computers mit einem entfernten Wahlserver, die Geheimheit der eigenen Abstimmung und die garantierte Zählung der eigenen Stimme sicherstellen sollen. Folglich erzeugen erst diese kryptographischen Verfahren die gewünschten Eigenschaften des Systems, dabei sind die kryptographischen Elemente nicht durch andere Mechanismen substituierbar. Gleichwohl entsprechen gerade diese Verfahren nicht dem verfassungsrechtlichen Gebot aus Karlsruhe.

Wie eine solche Architektur ohne besondere Expertise tatsächlich und unmittelbar bei einer Wahl durch den Bürger überprüft werden kann, ist nicht einsichtig. Selbst wenn das System die gewünschten Eigenschaften kryptographisch korrekt umsetzt, ist die Arbeitsweise des Systems nicht offensichtlich nachvollziehbar. „Zuverlässig und ohne besondere Sachkenntnis", wie es das höchste Gericht formuliert hat, kann für die große Mehrheit der Menschen das Innenleben ihrer Computer oder Telefone nicht mehr begriffen werden. Und nun soll der Single-point-of-failure einer Demokratie davon abhängen, dass die Wahlberechtigten hoch komplexe kryptographische Verfahren und deren computerbasierte Umsetzung verstehen? Ist es in diesem Fall nicht eher so, dass man das Vertrauen in das Wahlverfahren schlicht delegiert – die Experten werden es schon verstehen und richtig machen?

Es drängt sich die Vermutung auf, dass Angel Tchorbadjiiski die klare Entscheidung des Bundesverfassungsgerichts zu Wahlcomputern nicht wahrgenommen und daher in der Arbeit nicht beachtet hätte, doch er kommentiert das Urteil folgendermaßen: „The problem was that the voting machines used did not allow every citizen, taking part in the election, to verify the fundamental steps in the voting procedure." (S. 9) Ob der Autor das Urteil an sich überhaupt gelesen hat, darf bezweifelt werden, denn es findet sich bei der angegebenen Quelle (und auch sonst im Literaturverzeichnis) keinerlei Verweis auf den Urteilstext, sondern lediglich eine URL zur Pressemitteilung des Gerichts.

Mit Blick auf das Literaturverzeichnis sowie in Hinsicht auf die Prinzipien wissenschaftlichen Arbeitens stellen sich ohnehin Fragen bezüglich der Güte der Diplomarbeitsbetreuung durch Jó Ágila Bitsch, Dr. Tobias Heer, Prof. Dr.-Ing. Klaus Wehrle und Dr. Walter Unger.

In der Analyse der gesellschaftlichen Einbettung eines elektronischen Wahlsystems, die nur knapp eine halbe Seite umfasst, wiederholt Angel Tchorbadjiiski als Begründung für die Überlegenheit elektronischer Wahlsysteme eine lediglich von Wahlcomputerherstellern in die Welt gesetzte Aussage, deren empirischer oder sonstiger wissenschaftlicher Nachweis nach wie vor aussteht: "Compared to paper based ballots, its [e-voting's] advantages are the faster, flexible, cost effective and accessibility suitable ballot procedures." (S. 9) Einen Beleg bleibt auch er entsprechend schuldig. Die zurückliegenden US-Präsidentschaftswahlen haben

Constanze Kurz und Rainer Rehak

Constanze Kurz, Informatikerin, Sprecherin des Chaos Computer Club und Mitglied im Beirat des FIfF.
Rainer Rehak, Informatiker, Preisträger des FIfF-Studienpreises 2013 (siehe auch Seite 58-61).

das Gegenteil wieder eindrucksvoll bewiesen. Doch dass Schnelligkeit und Kosten bei parlamentarischen Wahlen nicht gleichrangig zu den Anforderungen an Allgemeinheit, Gleichheit, Freiheit, Geheimheit, Unmittelbarkeit und Nachvollziehbarkeit von Wahlen gesehen werden dürfen, steht ohnehin auf einem anderen Blatt und wurde von Tchorbadjiiski gekonnt ignoriert.

Mit der Auszeichnung dieser Arbeit hat sich das FIfF als Vereinigung kritischer Informatiker und Informatikerinnen in unseren Augen keinen Gefallen getan. Ganz im Gegenteil: Diese Auszeichnung ist ein fatales Zeichen eines Forums verantwortungsbewusster und politisch engagierter Techniker und Technikerinnen an die Gesellschaft, denn sie bestätigt: „Ja, unsere Technik kann das leisten, sie kann die verfassungsrechtlichen Vorgaben für demokratische Wahlen erfüllen." Doch das kann sie nach derzeitigem Stand der Forschung nicht, und gerade wir müssen das auch laut sagen.

Anmerkungen

1 https://adhocracy.de

Jury des FIfF-Studienpreises

Replik

zur Stellungnahme von Constanze Kurz und Rainer Rehak zu Vergabe des dritten Preises an die Arbeit Liquid Democracy von Angel Tchorbadjiiski

Rainer Rehak und Constanze Kurz kritisieren in ihrer Stellungnahme die Vergabe des FIfF-Studienpreises an die Arbeit *Liquid Democracy* von Angel Tchorbadjiiski. Wir, die Jury des Studienpreises, nehmen die Kritik zu Kenntnis und teilen die ihr zugrunde liegende Skepsis gegenüber technischen Wahlverfahren, nicht jedoch die Folgerungen für die durch uns ausgezeichnete Arbeit.

Entzündet hat sich die Kritik an einem Satz der Laudatio: „Sie [die Arbeit] stellt einen Bezug zu den Anforderungen des Wahlgesetzes her und zeigt auf, dass diese Anforderungen erfüllt werden können." Dieser Satz ist unglücklich formuliert, denn er könnte als Plädoyer für elektronische Wahlen jeglicher Art missverstanden werden. Das wäre in der Tat fatal und entspräche wohl kaum der mehrheitlichen Einstellung des FIfF zu diesem Thema. Uns sind selbstverständlich die Untersuchungen bekannt, in denen unter anderen der Chaos Computer Club auf die Problematik hingewiesen hat, und wir teilen deren Skepsis.

Die Diplomarbeit hat allerdings den Titel *Liquid Democracy* und beschäftigt sich auch primär mit den spezifischen Anforderungen bei der Bürgerbeteiligung am demokratischen Entscheidungsfindungsprozess, einschließlich der Delegation der Stimmabgabe. Der Hinweis auf das deutsche Wahlgesetz hat aus unserer Sicht hier eher begleitenden Charakter, da Angel Tchorbadjiiski aus dem Wahlgesetz einige Anforderungen für das Design seines Wahl- und Delegationssystems ableitet.

Der Autor selbst schreibt (2013): „Obwohl die gemeinsame Entscheidungsfindung sicherlich einen sehr wichtigen Punkt darstellt, fand ich es persönlich spannender, ein sicheres System zu entwickeln, dass anonyme und geheime Abstimmungen über das Internet ermöglicht." Der Wert der Arbeit ergibt sich daher aus Sicht der Jury vor allem aus der technischen Untersuchung, wie die abgeleiteten Anforderungen prinzipiell erfüllt werden könnten. Auch ohne den Bezug zum deutschen Wahlrecht ist die Diplomarbeit von Angel Tchorbadjiiski damit auszeichnungswürdig. Solche Untersuchungen sind auch die Voraussetzung für die mögliche Erkenntnis, dass als Ganzes die Anforderungen des deutschen Wahlgesetzes durch technische Verfahren eben nicht erfüllbar sind – auch wenn die Arbeit dies nicht explizit feststellt. Die Arbeit greift jedoch einen wichtigen Ausschnitt der Gesamtthematik auf.

Wie auch Constanze Kurz und Rainer Rehak in ihrem Kommentar feststellen, weist Angel Tchorbadjiiski durchaus auf die grundsätzliche Problematik hin. Sie lassen diesen Hinweis jedoch nicht gelten und stellen statt dessen Vermutungen über die Arbeitsweise des Autors und seiner Betreuer an. Daran möchten wir uns nicht beteiligen.

Die Jury war sich der grundsätzlichen Problematik des Vermischens von Liquid Democracy und Wahlrecht bewusst. Die Laudatio greift diese Probleme jedoch nicht explizit auf – was aber auch nicht ihre Aufgabe ist – sondern beschränkt sich auf sanfte Hinweise. Dies ist jedoch dem Preisträger nicht anzulasten.

Klar ist: Die Diskussion muss weitergehen. Vor allem die Piratenpartei setzt derzeit stark auf technische Verfahren der politischen Debatte und Entscheidungsfindung – einige Vertreter erhoffen sich dadurch einen grundsätzlichen Wandel der Demokratie, hin zu mehr Transparenz und Beteiligung. Dass technische Verfahren allein diese – politische – Fragestellung nicht lösen können, dürfte im FIfF weitgehend unbestritten sein. Um die Grundlage für diese Diskussion zu schaffen, sind aber Arbeiten wie die von Angel Tchorbadjiiski wichtig.

Vielleicht kann dies ja der Auftakt zu einer weiterführenden Debatte im FIfF sein – gerne auch in der FIfF-Kommunikation.

Referenzen

Stefan Hügel, Klaus Köhler (2012): Angel Tchorbadjiiski – Liquid Democracy. Laudatio für den 3. Preis. FIfF-Kommunikation 4/2012, 15-16.

Rainer Rehak, Constanze Kurz (2013): Ohne besondere Sachkenntnis – ein Kommentar zum dritten Platz des Studienpreises 2012. FIfF-Kommunikation 1/2013, 72-73.

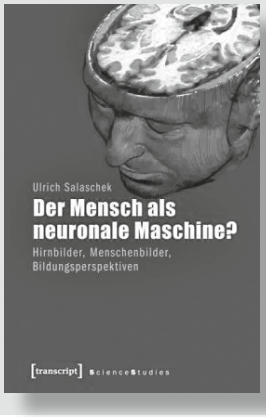
Angel Tchorbadjiiski (2012): Liquid Democracy. Diplomarbeit, Rheinisch-Westfälische Technische Hochschule Aachen.

Angel Tchorbadjiiski (2013): Liquid Democracy – Konzept zur kryptographischen Absicherung. FIfF-Kommunikation 1/2013, 69-71.

Britta Schinzel

Der Mensch als neuronale Maschine?

Zum Einfluss bildgebender Verfahren der Hirnforschung auf erziehungswissenschaftliche Diskurse



Salaschek, Ulrich (2012): Der Mensch als neuronale Maschine? Zum Einfluss bildgebender Verfahren der Hirnforschung auf erziehungswissenschaftliche Diskurse, Bielefeld: Transcript Science Studies, 221 S.

Der Band hält zwar nicht so ganz, was er im Untertitel verspricht, aber es ist ein in vielerlei Hinsicht äußerst kenntnisreiches, gut und verständlich geschriebenes Buch, auch dort, wo es keine leichte Kost bietet. Der Autor unternimmt es, die funktionelle Bildgebung mittels Magnetresonanztomographen, beginnend bei den physikalischen Grundlagen, in soweit ausreichender Annäherung an deren Komplexität darzustellen, dass bei Lesenden ein kritisches Verständnis für die Möglichkeiten und Grenzen ihrer Aussagekraft entstehen kann. Als Ziel des Buches bezeichnet er die Analyse der Frage, ob sich die BOLD-fMRT dazu eignet, den Menschen eindeutig als „neuronale Maschine" zu determinieren. Salaschek dekonstruiert diesen Anspruch indem er Kontingenzen der Bildgenese und Begründungslücken für diese These aufzeigt.

Er beginnt mit seiner Einschätzung der Erziehungswissenschaft als einer aus verschiedenen Gründen wenig selbstbewussten Disziplin, an die unerfüllbare Ansprüche an Gesellschaftsveränderung in kommenden Generationen gestellt würden, und die auch seit ihrem Bestehen inhaltlich und methodisch grenzenlos sei, was das dilettierende Eindringen aus anderen Wissensbereichen begünstige. Im Gegensatz dazu wird den Neurowissenschaften, sogar durch die OECD, Vorbildfunktion für die Erziehungswissenschaft zugebilligt, um den Traum vom Steuern des Lernens zu verwirklichen. Diese Erwartungen knüpfen sich an die ursprünglich nur metaphorisch gebrauchten, nun aber suggerierten Möglichkeiten der bildgebenden Verfahren, „Gedanken und unbewusste Verarbeitungsprozesse objektiv lesen" zu können, „das Bewusstsein entschlüsseln" oder „Schnappschüsse des Geistes" anfertigen zu können. Solche Zuschreibungen behaupten die Identität von geistigen und physikalisch-chemischen Zuständen des Gehirns und die pädagogischen Schlussfolgerungen landen bei *gehirngerechtem Lernen*, wobei Lernen mit dem Auf- und Abbau von neuronalen Verbindungen identifiziert wird, und bei *Bedienungsanleitung(en) für das menschliche Gehirn*, wonach es möglich (und erwünscht) wäre, die Neurochemie des Gehirns und damit Emotionen und Kognition aktiv und zielgerichtet verändern zu können.

Dazu analysiert er die Maschinenmetapher für den Geist. Er beginnt mit den historischen Menschenbildern, die Mensch und Automat identifizieren, und lotet die Möglichkeiten des medikamentösen *Neuroenhancement* aus, das im pädagogischen Bereich vor allem im Zusammenhang mit ADHS eingesetzt wird.

Danach wendet sich der Autor epistemologischen Fragen zu, einem in obigen Annahmen zum Vorschein kommenden reduktionistischen Materialismus sowie der Unterscheidung von Realismus und Nominalismus für die Interpretation der technisch hergestellten Bilder, bei denen es grundsätzlich unmöglich ist, gleichbleibende Rahmenbedingungen herzustellen. Das gilt besonders für Versuche, die unter Zwei-Personenperspektive in Wechselwirkung operieren, wie Gesa Lindemann es für diese Verfahren herausgearbeitet hat.

Es folgen eingehende Darstellungen technisch-instrumenteller Bilderzeugungsmethoden, der Mikroskopie (S. 75-110), und der strukturellen und später der funktionellen MRT, (S. 111-187). Wie bereits zu Beginn festgestellt, ist dem Autor der schwierige Balanceakt zwischen Verständlichkeit und hinreichender Genauigkeit der äußerst komplexen Verfahren hervorragend gelungen. Ich möchte die dortigen Erklärungen hier nicht nochmals wiederholen, das Buch sollte gelesen werden. Im Kapitel Bildgenese und Interpretation der fMRT werden weitere sich aus den kontingenten Rahmenbedingungen ergebende technische, mathematische und Versuchs-Anforderungen beschrieben. Am Beispiel des Haynes'schen *Gedankenlesens* dekonstruiert Salaschek anhand der vorher eingesammelten Kontingenzen, der engen Versuchsanordnung, der geschickt verdeckten Geringfügigkeit der statistischen Signifikanzen und der weit überschießenden Ergebnisinterpretation die durch den Titel insinuierte Behauptung.

Weitere konstruktive Anteile der statistischen Auswertung und der Bildgenerierung und -bearbeitung beschließen die Analyse der Kontingenzen der fMRT-Bildgenese.

Ein Schlusskapitel arbeitet die vorhergehenden Analysen der medizinischen Bildgebung noch einmal auf, im Hinblick auf ihren (eingeschränkten bis fragwürdigen) Wert für die Erziehungswissenschaften, und – so wäre hinzuzufügen –, auch für alle von medizinischen und MINT-Fächern entfernten Wissenschaftszweige mit dem Präfix Neuro-, wie Neuromarketing, Neurokriminologie, Neurotheologie oder Neuroästhetik.

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	**1.200 Stück**
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck
Schwerpunktredaktion	Werner Winzerling, Stefan Hügel
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@mtsf.de.* Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *http://www.fiff.de/regional*
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder
Titelbild	iStockphoto
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*)

19. Internationale DBU-Sommerakademie
9. bis 14. Juni in Ostritz
„Aktuelle Trends und Entwicklungen in der Umweltkommunikation"

Sigint 2013
5. bis 7. Juli in Köln
Konferenz für Hacker, Netzbewohner und Aktivisten

FIfF-Jahrestagung 2013
25. bis 27. Oktober in Siegen
„Cyberpeace"

FIfF-Beirats- und Vorstandsklausur
22. bis 24. März in Fulda

FIfF-Vorstandssitzungen
24. März, 09:00 – 12:00 Uhr in Fulda

FIfF-Kommunikation

2/2013 »Enquête-Kommission Internet und digitale Gesellschaft«
Stefan Hügel u. a.
Redaktionsschluss 3.5.2013

3/2013 »Informatik und Bildung«
Hans-Jörg Kreowski u. a.
Redaktionsschluss 2.8.2013

4/2013 »Fair IT«
Sebastian Jekutsch
Redaktionsschluss 1.11.2013

1/2014 »Cyberpeace«
Sylvia Johnigk, Kai Nothdurft, Stefan Hügel
Redaktionsschluss 1.2.2014

W&F – Wissenschaft & Frieden:
4/12 – Rüstung – Forschung und Industrie
1/13 – Geopolitik

DANA – Datenschutz-Nachrichten:
2/12 – Soziale Netzwerke
3/12 – Datenschutz bei Umfragen

Das FIfF-Büro

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

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

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

Schluss FIfF

Outsourcing für Jedermann

Das Auslagern von Tätigkeiten ist heute eine verbreitete und akzeptierte Form der Kosteneinsparung im Unternehmen. Ob nun Teile der Prozesskette *outgesourced* werden – im Rahmen des *Supply-Chain-Management* – oder ob durch *Offshoring* Entwicklungs- und Programmieraufgaben nach Osteuropa oder gleich nach Indien und China verlagert werden – stets erhoffen sich verantwortliche Manager und Shareholder verbesserte Renditen und einen höheren Bonus am Jahresende.

Da war es eigentlich nur noch eine Frage der Zeit, dass nach den Arbeitgebern auch Arbeitnehmer auf solche Ideen kommen. Mit den entsprechenden Management-Kompetenzen sollte es für jeden Mitarbeiter doch ein Leichtes sein, einen privaten Dienstleister in Fernost zu steuern. Die Honorare müssten angesichts der dort heute noch wesentlich geringeren Tagessätze doch leicht aus dem Gehalt zu finanzieren sein. So kann man den Tag mit Wichtigerem als seinem Job verbringen, und sich darauf beschränken, den Dienstleister zu koordinieren und dem eigenen Arbeitgeber die geforderten Berichte zu liefern.

Dies dachte sich offenbar ein Arbeitnehmer in einem amerikanischen Unternehmen. Bei einer Überprüfung seiner Logfiles stelle das Unternehmen fest, dass es eine aktive VPN-Verbindung nach China gab, die es so nicht hätte geben dürfen. Bei weiteren Untersuchungen durch die Sicherheitsfirma *Verizon* wurde festgestellt, dass diese Verbindung über Monate und dabei mehrere Stunden täglich offen war. Die Verbindung wurde dabei immer mit den gleichen Zugangsdaten eines im Unternehmen beschäftigten Softwareentwicklers geöffnet. Da das Unternehmen im Bereich kritischer Infrastrukturen tätig ist, schrillten natürlich sofort alle Alarmglocken. War man Opfer eines ausgefeilten Spionageangriffs geworden?

Doch die Untersuchung brachte Überraschendes zu Tage: Der Angestellte hatte seine Entwicklungsaufgaben einem chinesischen Dienstleister übertragen – für ein Fünftel seines eigenen Gehalts. So konnte er den Tag mit Facebook, eBay und Nahrungsaufnahme verbringen, und musste lediglich kurz vor Feierabend seinen Pflichten als Manager eines externen Dienstleisters nachkommen: Er erstellte den Tagesbericht für seine Vorgesetzten. Auch bei der Auswahl des Dienstleisters bewies er Kompetenz: Für „seinen“ Code bekam er stets beste Bewertungen. Den Zugang ermöglichte er seinem Auftragnehmer ganz klassisch – er schickte ihm seinen Token mit den Zugangsdaten per Post.

Sein Arbeitgeber war aber offenbar nicht bereit, diese Kompetenz im *Management* und im *Sourcing* von Dienstleistungen zu honorieren: Den Berichten zufolge ist der Mann mittlerweile entlassen. Was für ein Unternehmen legitim ist, ist es für seine Arbeitnehmer deswegen noch lange nicht.

Stefan Hügel

Referenzen

Case Study: Pro-active Log Review Might Be A Good Idea. Security Blog, Verizon Risk Team, Andrew Valentine, http://securityblog.verizonbusiness.com/2013/01/14/case-study-pro-active-log-review-might-be-a-good-idea/

Malware-Verdacht entpuppt sich als „privates Outsourcing“, heise online, http://www.heise.de/newsticker/meldung/Malware-Verdacht-entpuppt-sich-als-privates-Outsourcing-1785201.html

Manchmal steckt hinter einem fiesen chinesischen VPN-Zugriff auch bloß Telearbeit, Fefes Blog, http://blog.fefe.de/?ts=ae0b37b2

Security audit finds dev OUTSOURCED his JOB to China to goof off at work. The Register, Iain Thomson, http://www.theregister.co.uk/2013/01/16/developer_oursources_job_china/

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