H 7625

FIfF-Kommunikation

Zeitschrift für Informatik und Gesellschaft

34. Jahrgang 2017 Einzelpreis: 7 EUR 1/2017 – März 2017

FIfF-Konferenz 2016: *in.visible systems*

Versteckte Informationstechnik ist nicht diskutierbar

ISSN 0938-3476

• Virtual und Augmented Reality • Fortsetzung Zukunft der Arbeit •

FIfF-Kommunikation

Zeitschrift für Informatik und Gesellschaft

Titelbild: Videostill, Alexander Lehmann

inhalt

Inhalt

Ausgabe 1/2017

03 Editorial
- Stefan Hügel

Forum

04 *Der Brief:* Maßstäbe des Rechts
- Stefan Hügel

05 Wenn aus Spiel Wirklichkeit wird – Potenziale kollaborativer Augmented Reality
- Ute Bernhardt

Fortsetzung Schwerpunkt „Zukunft der Arbeit – Arbeit der Zukunft: Wer steuert wen?“

77 Das Ringen um Gute Arbeit in Zeiten *smarter* Technik – Die Gestaltung von Arbeit mit Software
- Nadine Müller

80 Gesundheit in Zeiten von Arbeit 4.0
- Eva von Buch

84 Besprechung der Stellungnahme von *Die Linke.* im Bundestag zum Grünbuch *Arbeiten 4.0*
- Michael Ahlmann

FIfF intern

90 Mitgliederversammlung des FIfF in Berlin
- Beschlussprotokoll

90 Ankündigung 33. FIfF-Konferenz
TRUST – Wem kann ich trauen im Netz und warum?

Rubriken

89 Lesen & Sehen

91 Impressum/Aktuelle Ankündigungen

92 SchlussFIfF

Schwerpunkt „FIfFKon 2016 – in.visible systems“

12 Editorial zum Schwerpunkt
- Benjamin Kees, Rainer Rehak, Stefan Hügel

14 2016: Kleine Geschichten verborgener Technik
- Stefan Ullrich

22 CYBER! Der Staat als Krimineller
- Zusammenfassung des Vortrags von Erich Möchel

26 Weitergehende Erkenntnisse aus den Verhandlungen zur EU-Datenschutzgrundverordnung
- Zusammenfassung des Vortrags von Jan Philipp Albrecht

29 Geheimdienste außer Kontrolle und warum die BND-Reform keine ist
- Zusammenfassung des Vortrags von Anna Biselli

33 Transparenz zwischen normativem Anspruch und kultivierter Unsichtbarkeit
- Zusammenfassung des Vortrags von Leon Hempel

37 Sozial gerechte Algorithmen? Problematiken, Konzepte und Perspektiven der Geschlechterforschung
- Zusammenfassung des Vortrags von Corinna Bath

40 Funktioniert Datenschutz im Unsichtbaren?
- Zusammenfassung des Vortrags von Marit Hansen

44 Die weitgehend verborgene Entwicklung autonomer Waffen
- Zusammenfassung des Vortrags von Hans-Jörg Kreowski

47 Die neue Globalisierung – wenn das Inland zum Ausland wird
- Zusammenfassung des Vortrags von Klaus Landefeld

50 Un.Sichtbare Datenpraktiken? Big Data in Wirtschaft, Wissenschaft & Politik
- Zusammenfassung des Vortrags von Judith Simon

54 An den Enden der Informatik
- Zusammenfassung des Vortrags von Wolfgang Coy

57 Sie haben den Nutzen der Technik noch nicht rational erkannt!
- Andrea Knaut

60 Informationen verstecken und Informationen herauskitzeln
- Zusammenfassung des Vortrags von Gaby Weber

61 We hate to say we told you so – IT-Sicherheit als Kriegshandwerk
- Sylvia Johnigk und Kai Nothdurft

66 Viel Licht und noch mehr Schatten: Plagiat in Dissertationen
- Zusammenfassung des Vortrags von Debora Weber-Wulff

68 10 Jahre Informationsfreiheitsgesetz – Ein Stück in 3 Akten
- Zusammenfassung des Vortrags von Arne Semsrott

73 Social Media in Südkorea: Staatliches Machtinstrument vs. „fünfte Gewalt“ in einer defekten Demokratie
- Zusammenfassung des Vortrags von Ok-Hee Jeong

Editorial

in.visible systems – Versteckte Informationstechnik ist nicht diskutierbar. Unter diesem Leitmotiv stand die *FIfF-Konferenz 2016*, die vom 25. bis zum 27. November 2016 in Berlin stattfand – und damit auch diese Ausgabe der *FIfF-Kommunikation*.

Der Schwerpunkt dokumentiert die Hauptvorträge der Konferenz, die von einem Team um die Schwerpunktredaktion zusammengefasst wurden. Ein eigenes Schwerpunkteditorial leitet den Schwerpunkt ab Seite 12 ein:

„Unsere digitale Umwelt ist frei von Öl, Staub und Müll. Wir erfahren und erleben sie durch glänzende Oberflächen, flüssige Animationen und ästhetische Bilderwelten. Wir werden mit sozialen Räumen und (freiem) Internet versorgt, unsere E-Mail-Boxen und Kalender werden für uns betrieben, unsere Daten bequem entfernt verwahrt, das Internet durchsuchbar gehalten, der Straßenverkehr optimiert und unser Zahlungsverkehr abgewickelt. Nun bleiben wir fit, können schneller Taxis finden und Zimmer vermieten. Gesundheitssysteme, der ÖPNV und auch andere staatliche Aufgaben werden digitalisiert. All dies geschieht mit Hilfe größtenteils unsichtbarer Systeme.

Zweck von Informationstechnik ist immer auch Komplexitätsreduktion und -verschleierung. Die Zusammenhänge bleiben nicht nur unsichtbar, sondern sie werden ganz gezielt versteckt. Dies geschieht einerseits zur sinnvollen Komplexitätsreduktion, andererseits aber auch, um verdeckte Zwecke zu verfolgen. Ein inzwischen durchdigitalisiertes Leben und die genutzte Infrastruktur mündig zu beurteilen oder gar zu gestalten, wird so zunehmend unmöglich gemacht."

Das Schwerpunkteditorial vermittelt den Überblick über die Beiträge der Konferenz und skizziert deren Inhalte. Weitere Einzelheiten des Schwerpunkts sind dort und in den ausgearbeiteten Beiträgen zu finden.

Immer noch ein wenig stolz sind wir auf unsere vorhergehende Ausgabe, die sich mit der Zukunft der Arbeit befasste, und die wir gemeinsam mit Kolleg.innen der Technologieberatungsstelle des DGB Nordrhein-Westfalen zusammengestellt haben. Leider haben nicht alle vorgesehenen Beiträge in der vorigen Ausgabe Platz gefunden, so dass wir in dieser Ausgabe eine Fortsetzung als zweiten, kleineren Schwerpunkt präsentieren können:

Das Ringen um Gute Arbeit in Zeiten smarter Technik behandelt *Nadine Müller*. „Unter dem Schlagwort Digitalisierung wird derzeit eine Reihe umfassender Veränderungen in der Arbeitswelt gefasst, die uns vor (teils) neue Herausforderungen für die Arbeitsgestaltung stellen. Diese als Digitalisierung oder auch als Computerisierung bezeichnete Entwicklung ergreift nahezu alle Arbeitsplätze, direkt oder indirekt", leitet sie ihren Beitrag ein, der die Gestaltung von Arbeit mit Software thematisiert. „Ein zentraler Punkt, um im Zeitalter *smarter* Technik Demokratisierung voranzutreiben, ist die Verbesserung der Beteiligung der Erwerbstätigen und der Mitbestimmungsrechte von Betriebs- und Personalräten in verschiedenen Feldern wie im Arbeits- und Gesundheitsschutz, bei Auftragsvergaben, Out- und Crowdsourcing und bei Wertschöpfungsprozessen in vernetzten *virtuellen* Strukturen", so ihr Fazit.

Eva von Buch thematisiert in ihrem Beitrag *Gesundheit in Zeiten von Arbeit 4.0*. „Mit der großflächigen Umsetzung von Industrie 4.0- und Digitalisierungsvorhaben verändern sich die Anforderungen an die Gestaltung von Arbeit. Damit stellen sich auch neue Fragen hinsichtlich der Gesundheit von Beschäftigten", so leitet sie ihren Beitrag ein. „In Zukunft wird es mehr innovative und nachhaltige Lösungen für gesunde *entgrenzte* Arbeitsplätze und Arbeitsbedingungen geben müssen. Diese Herausforderung gilt für alle Ebenen – Staat, Betrieb und Individuum. Die Form der Interventionen für gesunde Arbeitsbedingungen wird sich dabei vielleicht gar nicht so sehr verändern – eher die Frage der Zuständigkeit. Gelingt hier die Einbeziehung der Antonovsky-schen Theorie von den Ressourcen, ist den Beschäftigten schon viel geholfen!" – so schließt sie.

Als Abschluss des Schwerpunkts bespricht *Michael Ahlmann* die Stellungnahme der Fraktion *Die Linke.* zum Grünbuch des Bundesministeriums für Arbeit und Soziales.

Wenn aus Spiel Wirklichkeit wird. *Ute Bernhardt* stellt in ihrem Beitrag in der Rubrik *Forum* die Frage nach den Konsequenzen des Einsatzes von Datenbrillen wie *Google Glass* durch kriminelle Gruppen oder Terroristen für die zivile Sicherheit und den Folgerungen daraus für die Technikgestaltung: „Es ist Zeit für eine breite Debatte über die Implikationen eines kollaborativen Einsatzes von Datenbrillen und deren Missbrauch für unsere Gesellschaft, unsere Sicherheit und über mögliche Lösungsansätze – bevor uns die Wirklichkeit äußerst schmerzhafte Lektionen lehrt."

Regelmäßigen Leser.innen der *FIfF-Kommunikation* mag auffallen, dass das gewohnte *Log* weder in der aktuellen, noch in der vorigen Ausgabe enthalten war. Das ist den umfangreichen Schwerpunkten geschuldet, denen wir in beiden Fällen Priorität eingeräumt haben – in dieser Ausgabe kommen wir auf den beachtlichen Umfang von 92 Seiten. Wir werden das Log aber weiterführen und dabei verstärkt auf die Veröffentlichung in elektronischen Medien setzen.

Auch sonst planen wir, die *FIfF-Kommunikation* verstärkt in elektronischer Form zur Verfügung zu stellen. Dies umfasst die Veröffentlichung von Beiträgen in Blog-Form und die Intensivierung der Hinweise auf unsere Beiträge in sozialen Medien wie *Twitter*. Wir wollen die Reichweite der *FIfF-Kommunikation* erhöhen und sie als Publikation für *Informatik und Gesellschaft* im deutschsprachigen Raum verstärkt etablieren.

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

Stefan Hügel
für die Redaktion

Der Brief

Maßstäbe des Rechts

Liebe Leserinnen und Leser, liebe Mitglieder des FIfF,

man stelle sich diese beiden – fiktiven – Szenarien vor:

(1) Es entsteht zunehmend die Sorge, dass die Meinungsfreiheit immer stärker eingeschränkt wird. Maßnahmen wie Netzsperren werden von der Politik diskutiert, es wird auch ins Gespräch gebracht, Anbieter von Netzdiensten dazu zu verpflichten, „missliebige" Inhalte zu löschen. Tatsächlich werden soziale Medien auch missbräuchlich dafür genutzt, andere Menschen zu beschimpfen, *Hate Speech* und *Fake News* zu verbreiten, zu hetzen. Nicht immer ist klar, was genau gemeint ist: als *Hate Speech* werden häufig justiziable, beispielsweise beleidigende Inhalte bezeichnet, aber gelegentlich auch Meinungen, die lediglich nicht dem eigenen Weltbild entsprechen. Der Begriff ist nicht eindeutig definiert, er geht über heute strafbare Inhalte wie Beleidigungen etc. hinaus – viele als *Hate Speech* bezeichnete Veröffentlichungen in sozialen Netzen sind nach heutigem Recht eben *nicht* strafbar. Der Gesetzgeber reagiert besonnen. Er sieht die Meinungsfreiheit als ein hohes, schützenswertes Gut an. Deswegen sorgt er nicht nur dafür, dass sie nicht über das notwendige Maß hinaus eingeschränkt wird, er hebt sogar bestehende Gesetze auf, die sie bereits heute unnötig einschränken. Obwohl er das Risiko sieht, dadurch *Hate Speech* in Einzelfällen zu legalisieren, sieht er die Meinungs- und Pressefreiheit als so schützenswert an, dass er diese Nachteile in Kauf nimmt. Die bestehende Gesetzgebung muss ausreichen – wenn sie angemessen angewendet wird.

(2) Ein Untersuchungsausschuss des Deutschen Bundestags untersucht das Verhalten einzelner nachrichtendienstlicher Behörden und stellt dabei eine Reihe von rechtswidrigen Vorgängen fest – Verletzung des Datenschutzes, rechtswidrige Ausspähung von Menschen, Unterstützung rechtswidriger Praktiken von Nachrichtendiensten befreundeter Staaten bis hin zum Verdacht auf Industriespionage. Sofort werden Forderungen laut, dieses rechtswidrige Verhalten zu unterbinden und unter Strafe zu stellen. Bestehende Strafvorschriften werden verschärft, doch es gibt auch Vorgänge, die in der Öffentlichkeit „unerwünscht", aber bisher überhaupt nicht strafbar sind. Um solche Strafbarkeitslücken zu schließen, wird ein neuer Straftatbestand „Geheimdienstkriminalität" eingeführt. Kritik von Mitarbeitern der Behörde, die ihren Handlungsspielraum eingeschränkt sehen, verhallt ungehört. Eine rechtsstaatliche Ordnung kann ihre eigene Gefährdung durch rechtswidriges Verhalten ihrer eigenen Behörden nicht hinnehmen, so wird argumentiert.

Klingt absurd? Aber das passiert gerade in Deutschland – nur genau umgekehrt. Gerade wurde das BND-Gesetz reformiert und damit bisher rechtswidriges Verhalten des Bundesnachrichtendienstes weitgehend legalisiert.[1] Gleichzeitig gibt es eine Gesetzesinitiative, mit der sogenannte *Hate Speech* und sogenannte *Fake News* bekämpft werden sollen: Anbieter von Social Media müssen – bei erheblicher Strafandrohung – „offensichtlich rechtswidrige" Inhalte (was bedeutet das eigentlich, in einem Rechtsstaat?) binnen 24 Stunden vom Netz nehmen.[2]

„Aber wir müssen doch gegen *Hate Speech* und *Fake News* vorgehen!" Sicherlich. Macht sich dann auch der Bundesinnenminister strafbar, wenn er seine repressive Innenpolitik gegen geflüchtete Menschen mit falschen Statistiken begründet?[3] Machen sich die Verantwortlichen von Qualitätspresse und öffentlich-rechtlichem Rundfunk strafbar, wenn sie durch einseitige Darstellung einen falschen Eindruck von weltpolitischen Ereignissen erzeugen?

„Aber wir brauchen doch die Geheimdienste, um den Terrorismus zu bekämpfen!" Vielleicht auch das. Dass die deutschen Geheimdienste bei der Bekämpfung des rechtsgerichteten NSU-Terrors offenbar weitgehend versagt haben, ist eine Sache. Auch ihre Erfolge bei der Spionageabwehr werden gelegentlich in Zweifel gezogen.[4] Die wichtigere Frage ist aber, ob die Arbeit dieser Behörden und die Gesetze, auf deren Basis sie arbeiten, mit den Prinzipien unserer freiheitlichen Verfassung vereinbar sind.

Verallgemeinert aber heißt die Frage: Nach welchen Maßstäben wird unser Recht weiterentwickelt? Wenn sich der berechtigte Eindruck verbreitet, dass rechtsstaatliches Verhalten, je nach politischer Opportunität, mit zweierlei Maß gemessen wird, dann müssen wir wohl von einer Krise des Rechtsstaats sprechen.

Eine Frage der Maßstäbe sind auch die Kölner Ereignisse vom Silvesterabend 2016. Nach den Übergriffen des Vorjahres waren sich wohl alle einig: Das darf nicht wieder passieren! Es passierte auch nicht wieder – Beobachter hatten aber auch hier Zweifel an den Maßstäben, nach denen die Kölner Polizei die Übergriffe verhindert hat. Menschen, die aufgrund ihrer äußeren Erscheinung den Eindruck erweckten, dass sie aus nordafrikanischen Staaten stammen, wurde offenbar – unter der Bezeichnung *Nafri* – als potenziellen Tätern (sic!) besondere polizeiliche Aufmerksamkeit gewidmet. Man nennt so etwas *Racial Profiling*.

Kritik an diesem Vorgehen wurde – virtuell – niedergebrüllt. Um ein Beispiel herauszugreifen: Von Simone Peter, Sprecherin der *Grünen*, die es wagte, Fragen zum Vorgehen der Polizei zu stellen, distanzierten sich die meisten ihrer Kolleg.innen der Parteiprominenz.[5] Auffällig war das vor allem bei Cem Özdemir, der noch in den 1990er-Jahren selbst Opfer von *Racial Profiling* war.[6] Bei der Berichterstattung beispielsweise der *Bild*[7] zu dem Thema stellt sich dann wieder die Frage nach den Maßstäben: War das schon (künftig?) strafbare *Hate Speech*?[8] (Wo war übrigens der Ruf nach dem Strafrecht, als in der Vergangenheit eben dieser *Bild* die Verbreitung von *Fake News* – damals gab es diesen Begriff noch nicht – in mehreren Publikationen nachgewiesen wurde?[9])

Wir müssen zu einheitlichen Maßstäben in der rechtsstaatlichen Bewertung zurückkehren. Und wir dürfen das Recht nicht zum Spielball kurzfristiger parteipolitischer Erwägungen verkommen lassen. Gelingt uns das nicht, haben wir sie tatsächlich: Eine Krise des Rechtsstaats.

Mit FIfFigen Grüßen

Stefan Hügel

Anmerkungen

1 *Vgl. dazu beispielsweise die Zusammenfassungen der Vorträge von Anna Biselli und Klaus Landefeld auf der FIfFKon 2016 in diesem Heft.*

2 *Bundesministerium für Justiz und Verbraucherschutz: http://bmjv.de/fair-im-netz – kritsch dazu netzpolitik.org: https://netzpolitik.org/2017/analyse-so-gefaehrlich-ist-das-neue-hate-speech-gesetz-fuer-die-meinungsfreiheit/*

3 *https://youtu.be/rqGi64i9khY?t=1770*

4 *https://twitter.com/MdB_Stroebele/status/839399985137528832*

5 *http://www.spiegel.de/politik/deutschland/koeln-gruenen-chef-cem-oezdemir-distanziert-sich-von-ko-chefin-simone-peter-a-1128287.html*

6 *http://www.spiegel.de/spiegel/print/d-7547700.html*

7 *http://www.bild.de/politik/inland/die-gruenen/chefin-peter-und-die-nafri-debatte-49571068.bild.html*

8 *Man darf gespannt sein, welche strafrechtlichen Auswirkungen es auf die Chefredaktion von Bild online hat, wenn sie diesen Artikel nicht vor Inkrafttreten des o. g. Gesetzes gegen Hate Speech vom Netz nimmt.*

9 *Z. B. Günter Wallraff (1977): Der Aufmacher: Der Mann, der bei Bild Hans Esser war. Köln: Kiepenheuer & Witsch oder viele Beiträge bei http://www.bildblog.de/*

Ute Bernhardt

Wenn aus Spiel Wirklichkeit wird

Potenziale kollaborativer Augmented Reality

Virtuelle und „erweiterte Realität" – Virtual und Augmented Reality – mit Smartphones ist heute Alltag. Mit diversen Datenbrillen sollen neue Anwendungen auf dem Markt etabliert werden. Diese Entwicklung erfordert es, sich mit den Potenzialen ihres kollaborativen Einsatzes näher zu beschäftigen. Welche Konsequenzen hat ihr Einsatz durch kriminelle Gruppen oder Terroristen für die zivile Sicherheit und was folgt daraus für die Technikgestaltung?[1]

Augmented Reality auf dem Weg zum Massenmarkt

Die um digitale Informationen „erweiterte Realität" – Augmented Reality, kurz: AR – ist mittlerweile zu einem Massenmarkt mit Millionen Endkunden geworden. Mit *Pokémon Go* war 2016 ein Computerspiel erfolgreich, bei dem Smartphones als AR-Werkzeug dienen, um Spielfiguren in einer realen Umgebung aufzufinden. Bei derartigen AR-Spielen, perspektivisch aber vor allem für betriebliche Anwendungen, liefern Datenbrillen eine möglichst realistische Kombination von Umgebungsbild und virtuellen Daten und lassen die Hände frei für Bedienaufgaben. Für solche Datenbrillen gibt es bereits neben Einzel- auch AR-Gruppenspiele wie etwa *Life is Crime,* die daraus bestehen, in der eigenen realen Umgebung bei einer virtuellen kriminellen Gang aktiv mitzuwirken als – so die Werbung – Weg, um das „Leben eines Kriminellen zu führen, ohne dafür ins Gefängnis zu müssen"[2]. Die deutsche Innenministerkonferenz hat beschlossen, Datenbrillen zu evaluieren. Insgesamt wurden für Datenbrillen schon viele Anwendungsideen entwickelt, einige davon gehen deutlich über Computerspiele und Unterhaltung hinaus. So erprobt Volkswagen den Einsatz von Datenbrillen in der Logistik.[3]

Durch die Eigenschaften des ersten breit publizierten Produkts *Google Glass*, einer vernetzten Datenbrille, wurde bereits eine Datenschutzdebatte angestoßen. Wegen ihrer Ausstattung mit Videokamera, Mikrofon und der Möglichkeit sofortiger akustischer oder optischer Rückmeldungen, die in das Sehfeld projiziert werden, war die Debatte konzentriert auf die durch unbemerkte und allgegenwärtige Aufzeichnung und Übermittlung von Live-Videos der Umgebung des Brillenträgers geschaffenen Möglichkeiten zur individualisierten Videoüberwachung der vom Nutzer beobachteten Personen, den Verlust von Kontrolle und Vertraulichkeit und – durch die Speicherung und Analyse der Daten auf zentralen Servern zur weitergehenden Analyse der Daten – den damit drohenden Verlust von Autonomie und Reputation[4].

Diese Diskussion kreiste bisher darum, Datenbrillen als vernetzte Einzelsysteme[5] und das Verhältnis einzelner Nutzer zu ihren Gegenübern zu betrachten. Es fehlt jedoch bisher eine ähnlich umfassende Betrachtung von Datenbrillen als Kollaborations- und Gruppenunterstützungssystemen, den daraus folgenden Potenzialen und ihren Folgen. In diesem Beitrag sollen daher spezifische Möglichkeiten und Konsequenzen eines Einsatzes durch Gruppen von kollaborierenden Nutzern betrachtet werden. Ausgangspunkt der weiteren Betrachtung sollen nach einer kurzen Darstellung der Eigenschaften eine Beschreibung bereits dokumentierter Manipulationen der Systeme und die von den Herstellern nicht intendierten oder gar in Abrede gestellten Eigenschaften sein. Dies wird in Bezug gesetzt zu den Zielen bei der ursprünglichen Entwicklung von Datenbrillen und schließlich werden die möglichen Folgen dieser dokumentierten Eigenschaften betrachtet.

Datenbrillen und ihre Eigenschaften

Die zahlreichen Typen von angekündigten[6] oder erhältlichen[7] Datenbrillen machen es wenig sinnvoll, ein einzelnes spezifisches System als Basis einer Analyse auszuwählen. Um als Augmented-Reality-Werkzeug eingesetzt werden zu können, müssen alle Geräte Daten aus dem situativen Kontext des Benutzers in dessen Sichtlinie auf ein *head-mounted display* (HMD) projizieren. Üblich ist ein semi-transparentes Brillenglas, patentiert ist bereits eine Kontaktlinse[8]. Um die Umwelt zu erfassen, verfügen sie über eine Kamera, zumeist auch über Mikrofon und Kopfhörer. Die Videodaten werden mit Bildanalyse-Software auf spezifische optische Marker hin analysiert. Es gibt auch Bilderkennungs-Werkzeuge, die eine Gesichtserkennung leisten oder Personen anhand von spezifischen Zusatzmerkmalen erkennen.[9] Für all dies verfügen Datenbrillen über eine mehr oder minder ausreichende Rechenkapazität und Netzwerkanbindung.[10] Verschiedene Systeme sind darauf ausgelegt, zusätzliche Sensoren einzubinden und zu vernetzen, wofür Programmschnittstellen offengelegt werden, die es Entwicklern erlauben, die Datenbrille auf ihre eigene Weise zu nutzen.

Jeder Träger einer Datenbrille erstellt also in aller Regel Audio- und Videoaufnahmen der Umgebung, die der Kommunikation und Interaktion mit Back-end-Systemen oder Support-Fachleuten dienen und dazu in Echtzeit an eine Gegenstelle übermittelt werden, die die Bilder analysiert und zur Unterstützung oder Aufzeichnung nutzt. Wer die Bild- und Tonaufnahmen der Lebensumwelt des Trägers einer Datenbrille sieht, ist dessen Umgebung ebenso unklar wie die Dauer einer Aufzeichnung und die Art der darauf durchgeführten Datenanalyse.

Die Datenschutzprobleme dieser intensiven Umgebungsüberwachung sind unmittelbar einsichtig und bereits intensiv diskutiert. Aus Datenschutzsicht lassen sich dabei vor allem die auf Handhabungsaufgaben bezogenen Systeme in betrieblichen Anwendungen noch relativ gut fassen, wenn personenbezogene Daten zwar über die Handlungen der beteiligten Personen erhoben werden, selten aber über unbeteiligte Dritte[11].

Intendierte und nicht-intendierte Nutzung

Für viele der nachfolgend beschriebenen Möglichkeiten gibt es noch keine App zu kaufen. Nötig sind daher gewisse Fertigkeiten in der Programmierung von derartigen oder vergleichbaren Geräten. Einige der beschriebenen Funktionen wurden immerhin bereits in Forschungsprojekten realisiert. Bei der Bewertung des Anpassungsaufwands liefert *Google Glass* recht gute Vergleichsangaben.

Um offenbar erwartete, von Google nicht gewollte Anwendungen von *Google Glass* zu verhindern oder zumindest zu ahnden, sah Google in den Nutzungsbedingungen vor, dass das Unternehmen „sofern ein Google Gerät die Entwickler-Regelungen oder andere Übereinkünfte, Gesetze, Regularien oder Policies verletzt“, dieses „Glass-Gerät fernabschalten oder das Gerät aus seinen Servicesystemen entfernen kann".[12] Zu Kontrollzwecken und zur Umsetzung dieser Nutzungsbedingung hatte sich Google zudem das Recht vorbehalten, die Ortungsdaten des Nutzers sowie alle aufgenommenen Fotos, Videos und in das Display des Nutzers eingespielte Daten aufzuzeichnen und zu speichern.[13] Damit ist Google in der Position, auf Anforderung oder eigene Initiative alle Daten auf unzulässige Handlungen zu scannen. In Googles Version war *Google Glass* damit als die zivile Version eines mächtigen Kommando- und Kontroll-Systems angelegt.

Wie viele andere Datenbrillen arbeitet *Google Glass* mit dem Android-Betriebssystem und wurde mit Hilfe gängiger Werkzeuge schon wenige Tage nach Ausgabe der ersten Prototypen an Entwickler gehackt. Sie hatten danach vollen Zugang zu allen Komponenten des Systems.[14] Google selbst wollte keine Gesichtserkennungs-Software auf den Markt bringen. Dafür kamen Apps alternativer Anbieter in Umlauf, deren Installation teilweise das Hacken der Google-Datenbrille voraussetzte.[15] Googles Überwachungs-Werkzeuge ließen sich damit umgehen.

Solche Sicherheitsprobleme sind nicht spezifisch für *Google Glass*, da alle Datenbrillen nur eine begrenzte Rechenkapazität haben. Bislang hat kein System mit vergleichbaren Ressourcen gezielten Angriffen dauerhaft widerstehen können. Es ist daher davon auszugehen, dass jedes Datenbrillen-System nach überschaubarer Zeit kompromittiert wird und seine Technik nach Belieben manipuliert werden kann, sofern keine kostspieligen und am Markt kaum durchsetzbaren Sicherheitskomponenten eingebaut werden.

Kollaborative Datenbrillen-Systeme und ihre Urspünge

Über die bisher diskutierten Szenarien hinaus gehen Anwendungsfelder, bei denen es um die Interaktion mit Dritten geht, deren Verhalten mit Datenbrillen beobachtet wird[16]. Noch weiter gehen die Konsequenzen, wenn Datenbrillen als Mittel der Gruppenkoordination gegen unbeteiligte Dritte eingesetzt werden, wie es Google in seiner Werbung für *Google Glass* skizziert hat[17]. Extreme dieser Möglichkeiten sind ein Google-Glass-Egoshooter[18] und andere Ideen etwa von Microsoft. Sie repräsentieren zugleich eine Rückkehr der Datenbrillen zu den historischen Ursprüngen aller AR-Systeme mit HMD, auf die im Folgenden kurz eingegangen werden soll.

Die U.S. Army führte 1993 verschiedene Manöver mit Bodentruppen durch, um neu entwickelte Informations- und Kommunikationstechnik im Einsatz zu erproben. In der so genannten *Soldier Integrated Protective Ensemble (SIPE) Advanced Technology Demonstration (ATD)* überfiel eine sehr kleine Gruppe von Soldaten erfolgreich eine weit größere Einheit und eroberte und besetzte verschiedene Positionen im offenen Feld ebenso wie im Häuserkampf. Unter herkömmlichen Bedingungen und gleichwertiger Ausstattung wird davon ausgegangen, dass ein erfolgreicher Angriff die dreifache Personalstärke des Angreifers voraussetzt. Die Vorläufer von Datenbrillen stellten dieses Verhältnis auf den Kopf: Der unterlegene Verteidiger war dreimal stärker als der Angreifer.

Möglich machten dieses umgekehrte Kräfteverhältnis nicht Techniken wie die einzeln schon lange genutzten Laser- und Infrarot-Sensoren sowie Audio-Verstärkung und Richtmikrofone, sondern die Vernetzung von Soldaten und Sensoren in einem

kollaborativen AR-System. Die Angreifer konnten durch den Sensor-Datenaustausch die Gegner mit passiver Datenerhebung triangulieren und auf einer gemeinsamen Gefechtsfeldkarte markieren. Diese Karte wurde mit anderen Daten in die Displays eingespielt. Mit vernetzten Videokameras wurde unbemerkt um die Ecke gespäht und die Bilder an alle Gruppenmitglieder übertragen. Vor dem Überfall lieferten die Daten in den AR-Displays einen vollständigen Überblick über den Gegner und unterstützten einen hoch koordinierten Ablauf. Die gleichzeitige Datenübermittlung an einen zentralen Befehlshaber erlaubte es, die Aktion in Echtzeit zu verfolgen und mit zusätzlichen Informationen zu unterstützen.[19]

Die umfassende Vernetzung zwischen Soldaten und Kommandeuren erwies sich als äußerst wirksamer *Force Multiplier*. Aus den bis in die 1980er-Jahre zurückreichenden Ursprüngen[20] wurde ein technologisches Entwicklungs- und Einsatzziel verschiedener Armeen, allen voran der USA.[21] Sie bauten mit einem einheitlichen Kommunikationssystem einen Datenverbund auf[22], mit dem Audio- und Videodaten in Echtzeit zwischen Kampfeinheiten und Kommandozentralen ausgetauscht werden[23]. Die Bilder aus dem Lagezentrum in Weißen Haus bei der Erstürmung des Verstecks von Osama bin Laden in Pakistan zeigten den Einsatz vernetzter Spezialeinheiten und deren Steuerung.

Der Schritt zur alltäglichen militärischen Nutzung von Datenbrillen steht allerdings noch aus; die Systeme sind noch nicht leistungsfähig, robust und genau genug. Derzeit werden diverse Systeme von verschiedenen Armeen erprobt.[24] So ist die Bundeswehr von der Konzeptionsphase im Programm *Infanterist der Zukunft*[25] mittlerweile zur Kampferprobung übergegangen. Das *Gladius*-System für AR-Anwendungen mit einem HMD wurde 2013 an das Heer für den Einsatz in Afghanistan ausgeliefert.[26] Die Einsätze sind jedoch auf spezielle Aktionen von Spezialeinheiten oder Geheimdiensten beschränkt.[27] Trotz dieser Einschränkungen wurde der Markt für AR-Systeme in Kampfeinsätzen auf 8,2 Mrd. Dollar für 2016 geschätzt.[28]

Von der militärischen zur zivilen Nutzung

Nach der Einführung von *Google Glass* interessierten sich 2014 die Polizeibehörden New Yorks[29] und Dubais[30] für die Nutzungspotenziale. Berichte über Ergebnisse liegen nicht vor. In Deutschland beschäftigte sich die Innenministerkonferenz im Juni 2016 damit, „aus Streifenbeamten vernetzte Polizisten" zu machen und „Datenbrillen, um Fahndungsfotos oder Einsatzbefehle direkt an jeden einzelnen Polizisten zu verschicken, schon bald zur Standardausrüstung der Beamten" zu machen.[31]

Was ist nun zu erwarten, wenn Datenbrillen außerhalb von militärischen Kampfzonen im Zivilleben eingesetzt werden? Und – bisher kaum beachtet – was geschieht, wenn Datenbrillen bei kriminellen oder terroristischen Aktivitäten Verwendung finden? Drei einfache Beispiele mit anwachsendem Gefahrenpotenzial sollen dazu dienen, diese Möglichkeiten auszuloten.

Alle beschriebenen Eigenschaften von kollaborierenden Datenbrillen-Systemen sind zum Teil bereits im Rahmen heutiger Systeme verfügbar oder so in Reichweite, dass es nicht mehr als eines Jahres bedürfte, sie zu entwickeln. Noch sind solche Anwendungen aber nicht bekannt. Damit stellt sich im Anschluss die Frage, welche Bedingungen, Szenarien und Interessen für eine solche Nutzung ausschlaggebend sein könnten.

Überwachung und Verfolgung

Eine einfache kollaborative Anwendung ist die Navigation. Wenn eine Navigation per Karte nicht zum Ziel führt, wird ein Nutzer von einer anderen, ortskundigen Person anhand der Videoaufnahmen der Datenbrille zum Ziel gelenkt – entweder durch gesprochene Richtungsangaben oder durch eingespiegelte Richtungspfeile. Ersetzt man dabei ein geografisches Ziel durch eine Person, die im Sichtfeld der Datenbrille – möglicherweise automatisch – erkannt, *getaggt* und hervorgehoben wird, so ist unmittelbar ersichtlich, dass vernetzte Datenbrillen ein erhebliches Potenzial zur Erleichterung bei der Verfolgung von Personen auch in sehr belebter Umgebung haben.

Erweitert man im nächsten Schritt einen solchen einfachen Datenaustausch um die bereits in den 1990er-Jahren erprobten Mittel zur Distanzmessung und die passive Triangulation durch zwei und mehr kollaborierende Nutzer von AR-Systemen und ergänzt das durch die mit heutiger Technik mögliche automatische Erkennung und Markierung charakteristischer Features eines Verfolgten aus Videodaten, so sind erhebliche Erleichterungen bei der Verfolgung zu erzielen. Dass die Kommunikationsunterstützung bei Datenbrillen so unauffällig wie möglich gestaltet ist, vereinfacht die Koordination der Verfolger und verringert die Gefahr, dass Gruppen heimlicher Beobachter erkannt werden.

Mit einer solchen Sensorintegration lässt sich die Leistung eines AR-Systems weiter steigern. In Militärmanövern wurde schon gezeigt, dass sich beliebige Sensoren mit AR-Systemen koppeln lassen. Videokameras ließen sich ersetzen oder ergänzen durch Infrarot- und Nachtsicht-Systeme. Das ist eine attraktive Eigenschaft für diverse Outdoor-Spiele. Zugleich ließe sich aber auf

Ute Bernhardt

Ute Bernhardt ist Mitglied im wissenschaftlichen Beirat des FIfF e. V. sowie im Netzwerk Datenschutzexpertise.

diese Weise die von den Sicherheitsbehörden genannte Zahl von bis zu 35 Beamten für eine Observation[32] mit weit weniger Personal durchführen. Auf gleiche Weise könnten jedoch auch kriminelle oder terroristische Gruppen ein Opfer verfolgen.

Nach Terroranschlägen mit polizeilich bekannten Tätern wurde in Deutschland und in Frankreich darüber debattiert, dass eine Observation durch Sicherheitsbehörden so viele Ressourcen bindet, dass sie nur in ausgesuchten und dringenden Fällen infrage kommt. Der ausufernde Einsatz *stiller SMS* zur Ermittlung des Standorts von Verdächtigen[33] dokumentiert ein hohes Interesse am Einsatz technischer Hilfsmittel. Datenbrillen können den Aufwand für eine Observation eindeutig reduzieren. Noch einfacher wird es, wenn Umgebungsintelligenz in Form von Videokameras für die Personenerkennung oder mobiler IMSI-Catcher[34] erlaubt, Daten mit Observationsteams auszutauschen, die über Datenbrillen verfügen – wie schon in Manövern in den 1990er-Jahren beschrieben. Diverse Analysen von Personenflüssen bei Großveranstaltungen[35] auch anhand von Handy-Kennungen zeigen die enormen Potenziale: auch in großen Menschenmengen lässt sich zuverlässig observieren. Entsprechende AR-Technologie dürfte mit hoher Wahrscheinlichkeit in die Anforderungen an Entwicklung und Beschaffung von Technik für die Sicherheitsbehörden in den nächsten Jahren einfließen.

Wenn eine Observation von Einzelpersonen nicht länger einen derart hohen Personaleinsatz erforderlich macht, und da die Technologie heute bereits verfügbar ist, um eine begrenzte Zahl von Personen für unterschiedliche Bedarfe parallel in einer Umgebung zu verfolgen, können Observationstechniken von einer Einzelbeobachtung zu einem System der Zonen-Observation gegenüber definierten Personen umgebaut werden. Eine deutlich kleinere Zahl von Sicherheitskräften mit Datenbrillen und Sensoren könnte in einer Zone mehrere markierte Verdächtige gleichzeitig observieren, das über verschiedene Zonen hinweg durchführen und dabei aufgenommenes Videomaterial als Beweismittel nutzen.

Der polizeiliche Nutzen einer solchen Observation lässt sich bereits einfach erkennen an der Observation einer Gruppe von Taschendieben. Die Taschendiebe hätten allerdings denselben Nutzen, wenn sie gemeinsam mit AR-Hilfe auf Beutejagd gehen.

Diebstahl und Einbruch

Auf dieselbe Weise lassen sich Werkzeuge zum Orten und Anzeigen von WLAN-Emittern, Smartphones oder anderen funkgestützten Systemen einbinden, wofür je nach Emitter-Typ Modifikationen der heute in Smartphones vorhandenen Ortungswerkzeuge gegen Diebstahl ausreichen. Bisweilen können komplexere Zusatzinstallationen[36] erforderlich sein.

Mit derselben Kombination von Sensoren können auch Einbrecher WLAN-Emitter taggen und funkbasierte versteckte Sensoren und Einbruchserkennungstechnik finden und markieren. Anfällig sind hier insbesondere WLAN-Überwachungskameras, deren Standort sich peilen lässt. Mit einem kollaborativen AR-System können die ermittelten Daten für eine Internet-Recherche oder den Rat von Experten irgendwo auf der Welt genutzt werden, um sich Wege zur Umgehung dieser Systeme vorschlagen zu lassen – wenn die Kameras nicht ohnehin offen im Internet zu finden sind[37]. Mit Datenbrillen und solcher Hilfe lassen sich auch untrainierte Einbrecher aus der Ferne unterstützt auf sicherheitstechnisch gut geschützte Objekte ansetzen. Ein Experte könnte einer größeren Bande für einen gleichzeitig verübten großen Raubzug zur Verfügung stehen und wäre keinem Verhaftungsrisiko ausgesetzt.

Organisiertes Verbrechen und Terrorismus

Nicht nur in Hollywood-Filmen werden die Abläufe bei Raubüberfällen auf hochwertige Ziele geplant und geübt. Auch terroristische Anschläge werden detailliert und über längere Zeit geplant und vorbereitet.

Unaufdringliche Datenbrillen erleichtern und verbessern die Koordination von Überfällen – insbesondere bei komplexen Abläufen. Mit solchen AR-Werkzeugen lassen sich das Timing perfektionieren und Ablenkungsmanöver effektiver einsetzen. Datenbrillen werden als Werkzeuge explizit dazu entwickelt und genutzt, Handlungen an realen Orten virtuell durchzuspielen oder die Realität in einem Übungsgelände nachzubilden. Mit der Übung an *Originalschauplätzen* mit unauffälligen Datenbrillen lässt sich ein risikoreicher Raubüberfall besser planen und umsetzen.

Terrorüberfälle größerer Gruppen von Angreifern gab es auf Hotels, Shopping Center, Flughäfen und andere Orte wie in Mumbai, Nairobi[38], Paris, Brüssel und natürlich auf viele Ziele im Irak und in Afghanistan. Selbst beim Amoklauf eines Einzeltäters in München 2016 spielte dessen Chat-Kommunikation mit sich selbst eine Rolle bei seiner Selbstdarstellung und der Bewertung durch die Sicherheitsbehörden. Insbesondere die IS-Terrorgruppe experimentiert schon länger mit ferngesteuerten oder durch IT-Einsatz automatisierten Fahrzeugen, Kanonen und anderen Angriffswerkzeugen.[39] Anhaltspunkte wie diese belegen, dass Gewalttäter und insbesondere Terrorgruppen hinreichende IT-Kenntnisse auch für den Einsatz von AR-Werkzeugen haben.

Wie schon in Militärmanövern der 1990er-Jahre demonstriert, könnten koordiniert vorgehende Terrorgruppen mit Datenbrillen eine gemeinsame Lagekenntnis zu Lasten der angegriffenen Zivilbevölkerung ausspielen. Auch bei terroristischen Angriffen ließe sich die Abstimmung von Angriffsabläufen verbessern durch die gemeinsame Kenntnis über Standorte und das Vorgehen der Gruppenmitglieder anhand des visuellen und akustischen Austauschs in Echtzeit.

Eine Terrorgruppe könnte zu Beginn eines Angriffs die Sicherheitskontrollen an verschiedenen Stellen simultan und koordiniert angreifen, bevor Alarm ausgelöst wird. Als zweiten Schritt könnte eine solche Gruppe mehrere Ziele einnehmen und abriegeln, bevor Sicherheitskräfte mobilisiert werden können. Jeder kritische Zugangspunkt ließe sich unter kollaborativer Kontrolle halten – möglicherweise sogar unter Einbeziehung vorhandener Sensoren oder Kameras. Im dritten Schritt könnte eine solche Gruppe Geiseln im Gebäude oder Gelände ohne Kontrollverlust so verteilen, dass eine Geiselbefreiung durch Sicherheitskräfte wesentlich risikoreicher würde. Im Fall einer Befreiungsaktion würde die AR-Vernetzung einer Terrorgruppe den Überra-

schungseffekt verringern, weil selbst getötete Terroristen den Mitgliedern ihres Datennetzwerks weiterhin die Videoaufnahmen des ablaufenden Angriffsgeschehens übermitteln können. Zu allem Überfluss ließen sich die Videobilder der Datenbrillen vom Tatort auch noch zu Propagandazwecken verwenden.

Bewertung

Einen solchen Terrorüberfall mit Unterstützung durch Datenbrillen mag man sich nicht ansatzweise vorstellen. Schutz und Sicherheit setzen aber voraus, neue Szenarien durchzuspielen. Deswegen ist es durchaus erstaunlich, dass die einfache Übertragung der Erfahrungen aus militärischen Manövern in die Gegenwart von leicht verfügbarer, kollaborativer Datenbrillen-Technologie bisher nicht unter dem Blickwinkel der zivilen Sicherheit gesehen wurde. Mittlerweile ist die Beschaffung und Adaption der nötigen AR-Technik deutlich einfacher zu bewerkstelligen als die Beschaffung von Waffen, Sprengstoff und anderer Militärausrüstung. Es ist daher leider davon auszugehen, dass wir in den nächsten Jahren Szenarien erleben werden, in denen bewaffnete Täter zusätzlich mit Datenbrillen ausgestattet sind, durch die sich eine neue Art von *Datenbrillen-Überfällen* oder gar *Datenbrillen-Terrorismus* entwickeln kann. Wir sollten diese Möglichkeiten nicht ignorieren, sondern heute darüber nachdenken.

Die kollaborativen Einsatzpotenziale von Datenbrillen bergen große Risiken, für illegale Zwecke genutzt zu werden. Die Experimente verschiedener Strafverfolgungsbehörden haben bereits gezeigt, dass diese ihrerseits neue Einsatzszenarien sehen und die Möglichkeiten dieser Technik in der Praxis erproben wollen. Dabei ist in Erinnerung zu rufen, dass HMDs als nicht-zivile Versionen von Datenbrillen heute schon von Spezialeinheiten operativ genutzt werden, auch in der Bekämpfung ziviler Unruhen. Lediglich der Einsatz marktgängiger, unauffälliger Modelle zu Überwachungszwecken wäre eine wirkliche Neuerung. Einige der möglichen Konsequenzen sind unschwer abzusehen. Andere erfordern grundsätzlichere Überlegungen.

Sollte es dazu kommen, dass Datenbrillen mit ihrer Übermittlung von Videodaten in Echtzeit an zentrale Server zu einer breiteren Nutzung kommen, werden die Sicherheitsbehörden wohl versuchen, auf diese Daten Zugriff zu erlangen mit dem Argument, dass Nutzer der Datenbrillen unwissentlich Aufnahmen eines für die Behörden wichtigen Geschehens machen könnten. Die Durchsuchung des zentral gesammelten Videomaterials von Datenbrillen im Hinblick auf Daten zu einem Tatort oder Tathergang entweder ex post durch Beschlagnahme oder bei Verdacht in Echtzeit von allen dort vorhandenen Nutzern dürfte sich zu einer vergleichbar eingesetzten Methode entwickeln wie heute die Auswertung von Überwachungskameras bzw. Handy-Videos.

Verschiedene der zuvor beschriebenen illegalen Nutzungspotenziale dürften mit einer Manipulation insbesondere auch der gemeinsam genutzten Kommunikationsverbindungen einhergehen, um durch eigene Kommunikationskanäle die bei einigen Modellen vorgesehene zentrale Datensammlung zu umgehen. Für die Sicherheitsbehörden wird daraus die Forderung erwachsen, die lokale Kommunikation von Tätergruppen – etwa per WLAN – am Ort eines Geschehens analysieren, überwachen oder stören zu können. Nach IMSI-Catchern und anderem Gerät wird daher der Wunsch nach weiterer Überwachungstechnik laut werden.

Grundsätzlich anders fällt die Betrachtung aus, wenn es um die Frage geht, ob und wie Datenbrillen gegen eine Nutzung für illegale Aktivitäten gesichert werden können, die mit großen Gefahren für die Allgemeinheit, aber auch für die Sicherheitsbehörden verbunden sind. Hier fällt eine Antwort ziemlich ernüchternd aus. Schon heute ist zu viel Software im Umlauf, die für Einzelnutzer und Nutzergruppen die Grundlagen für eine Weiterentwicklung zur Realisierung der vorab beschriebenen kollaborativen AR-Anwendungen schafft. Diese Entwicklung ist nicht mehr einzudämmen.

Was das Verhindern der Anbindung externer Sensorik an Datenbrillen und das AR-typische Taggen von Elementen im Sichtfeld des Nutzers angeht, so ist auch das nur eine Frage der softwareseitigen Datenintegration. Da es regelmäßig um nur wenige Daten geht, ist der Aufwand überschaubar.

Datenbrillen, die mit einem gängigen Betriebssystem für den Massenmarkt angeboten werden, sind nicht wirksam gegen Manipulation und Missbrauch zu sichern. Die Hersteller müssten schon an verschiedenen Punkten ihrer Systeme Mechanismen vorsehen, die bei Manipulationen die Datenbrille zur Selbstzerstörung bringen oder eine Deaktivierung von außen erlauben. Wie leicht letzteres umgangen werden kann, hat schon *Google Glass* gezeigt. Auch hierbei lässt sich daher letztlich nur an der konkreten Implementierung ermessen, ob solche Maßnahmen ausreichen.

Fazit

Gegen die meisten und vor allem die extremsten der beschriebenen illegalen Nutzungsszenarien von Datenbrillen kommen nur sehr wenige technische Mittel infrage. Ideen zur unbegrenzten Datenerhebung wiederum würden massive Grundrechtseingriffe für die Allgemeinheit ohne erkennbaren Nutzen bedeuten.

Zur Prävention von erwartbarem Missbrauch notwendig wäre vielmehr ein *Code of Conduct* von Selbstbeschränkungsregeln der Anbieter und Software-Entwickler. Hardwareseitig sollte ernsthaft über Manipulationshemmnisse nachgedacht und entsprechende Erschwernisse eingebaut werden. Softwareseitig sollten solche kollaborativen Spiele und Anwendungen gar nicht erst auf den Markt gebracht werden, die sich ohne größere Veränderungen für illegale Einsatzszenarien nutzen lassen und so selbst Tätern ohne vorheriges Training die erheblichen Gefährdungsmöglichkeiten einer kollaborativen Datenbrillennutzung eröffnen. Es ist fraglich, ob für eine solche Bewertung die bisherigen Prüfverfahren der Altersfreigabe für Computerspiele ausreichend sind.

Datenbrillen weisen ein erhebliches Potenzial zur Überwachung des Alltags Unbeteiligter auf, das für die Sicherheitsbehörden von großem Interesse ist. Militärische HMDs werden bereits operativ genutzt und dürften zukünftig auch bei Sondereinheiten der Polizei Verwendung finden. Unauffällige zivile Daten-

brillen eröffnen den Sicherheitsbehörden erhebliche neue Perspektiven für die Observation und Überwachung. Das sind nur bedingt positive Aussichten, die aber prinzipiell regelbar und in bestimmten Konstellationen auch nutzbringend sind.

Nicht regelbar ist der Einsatz von Datenbrillen für kriminelle und terroristische Zwecke. Es ist daher umso erstaunlicher, dass diesen Fragen bisher so gut wie nirgendwo nachgegangen wurde und sie für Entwickler und Anbieter keine Rolle zu spielen scheinen.

Bevor wir die ersten Datenbrillen-Terroristen erleben müssen, wäre es dringend geboten, in der Informatik daran zu arbeiten, wie diese Technik eingegrenzt werden kann, oder die missbräuchlich nutzbare Arbeit an solchen Geräten aus ethischer Verantwortung heraus einzustellen. Sicherheitsbehörden und Gesetzgeber sind aufgefordert, sich unter operativen und regulatorischen Gesichtspunkten mit den Missbrauchspotenzialen von Datenbrillen auseinanderzusetzen. Die Hersteller schließlich sollten damit konfrontiert werden, dass sie erhebliche Risiken gedankenlos in Kauf nehmen.

Es ist Zeit für eine breite Debatte über die Implikationen eines kollaborativen Einsatzes von Datenbrillen und deren Missbrauch für unsere Gesellschaft, unsere Sicherheit und über mögliche Lösungsansätze – bevor uns die Wirklichkeit äußerst schmerzhafte Lektionen lehrt.

Anmerkungen

1 *Ausgangspunkt dieser Betrachtung ist der Beitrag von Ute Bernhardt: Google Glass: On the implications of an advanced military command and control system for civil society. In: International Review of Information Ethics (IRIE): Cyber warfare, Issue No 19, Vol. 20, December 2013, p. 16–27, http://www.i-r-i-e.net/inhalt/020/IRIE-Bernhardt.pdf*

2 *Werbung für Life is Crime auf: http://www.androidauthority.com/best-ar-apps-and-games-for-android-augmented-reality-584616/; das Spiel ist in Deutschland nicht verfügbar.*

3 *Wilfried Eckl-Dorna: Datenbrille als Logistik-Helfer. Neue Chance für Google Glass – in den Lagerhallen von VW, manager magazin, 9.3.2015, http://www.manager-magazin.de/unternehmen/autoindustrie/datenbrille-google-glass-soll-produktivitaet-von-vw-erhoehen-a-1022591.html*

4 *Mark Hurst: The Google Glass feature no one is talking about, 28.2.2013, http://creativegood.com/blog/the-google-glass-feature-no-one-is-talking-about/*

5 *"Even share what you see. Live", http://www.google.com/glass/start/what-it-does/; zur Throughglass App: http://glass-apps.org/throughglass-google-glass-app*

6 *So: Google Glass-Like Products Can Launch For As Low As $400, Forbes, 21.7.2013, http://www.forbes.com/sites/haydnshaughnessy/2013/07/21/google-glass-like-products-can-launch-as-low-as-400/. Zu dieser Zeit wurde bereits über vergleichbare Microsoft-Entwicklungen berichtet: Microsoft Tests Eyewear Similar to Rival Google Glass, Wall Street Journal Online, 22.10.2013, http://online.wsj.com/news/articles/SB10001424052702304402104579150952302814782. Samsung hatte derweil dazu seinerseits Patente angemeldet: Samsung files patent for Google Glass-like device, San Jose Mercury News, 25.10.2013, http://www.mercurynews.com/business/ci_24386791/samsung-files-patent-google-glass-like-device*

7 *Beispiele dafür sind Produkte wie Recon Jet HMD (http://reconinstruments.com/products/jet/), Epiphany Eyewear (https://en.wikipedia.org/wiki/Epiphany_Eyewear), GlassUp aus Italien (http://www.glassup.net/) und das Vuzix Smart Glasses Accessoire für Smartphones (http://www.vuzix.com/consumer/products_m100.html). Sogar Nissan präsentierte ein AR-Gerät auf der Tokyo Motor Show 2013 unter dem Produktnamen 3E: The 3E View of the Tokyo Motor Show, 19.11.2013, http://blog.nissan-global.com/EN/?p=11271*

8 *Doug Bolton: Samsung patents design for 'smart' augmented reality contact lenses, The Independent, 6.4.2016, http://www.independent.co.uk/life-style/gadgets-and-tech/news/samsung-smart-contact-lenses-patent-a6971766.html; unter Bezug auf: Samsung is working on smart contact lenses, patent filing reveals, http://www.sammobile.com/2016/04/05/samsung-is-working-on-smart-contact-lenses-patent-filing-reveals/. Die Konzepte dazu sind älter: Babak A. Parviz: Augmented Reality in a Contact Lens, IEEE Spectrum, 1.9.2009, http://spectrum.ieee.org/biomedical/bionics/augmented-reality-in-a-contact-lens*

9 *Die 2013 angebotene MedRec app referenziert Patientendatensätze aufgrund ihrer Bilder, http://glass-apps.org/medref-google-glass-app. Auf dem CCC-Kongress im Dezember 2013 kündigte Lambda Labs eine Gesichtserkennungs-App an, die nicht von Google unterstützt wurde: Google Glass Face Recognition App Coming This Month, Whether Google Likes It Or Not, Forbes Online, 18.12.2013, http://www.forbes.com/sites/andygreenberg/2013/12/18/google-glass-face-recognition-app-coming-this-month-whether-google-likes-it-or-not/*

10 *Siehe Beschreibung und Berichte bei: http://www.google.com/glass/start/*

11 *Die datenschutzrechtliche Betrachtung kann zurückgreifen auf Überlegungen zu Wearables bei Beschäftigten, siehe dazu auch Thilo Weichert: Wearables – Schnittstelle Mensch und Computer, CuA 10/2016, S. 8 ff.*

12 *Google Glass Terms of Sale and Use, Dezember 2013, http://www.google.com/glass/terms/*

13 *ebd.*

14 *Entwicklerversion der Google Glass per QR-Code gehackt, http://www.heise.de/security/meldung/Entwicklerversion-der-Google-Glass-per-QR-Code-gehackt-1919373.html; basierend auf: Lookout: Sicherheit für die vernetzte Welt: Ein Google Glass-Fallbeispiel, company blog, 17.7.2013, https://blog.lookout.com/de/2013/07/17/sicherheit-fur-die-vernetzte-welt-ein-google-glass-fallbeispiel/*

15 *Google Glass Face Recognition App Coming This Month, Whether Google Likes It Or Not, Forbes Online, 18.12.2013, http://www.forbes.com/sites/andygreenberg/2013/12/18/google-glass-face-recognition-app-coming-this-month-whether-google-likes-it-or-not/*

16 *Das gilt auch für gleichartige Produkte. Microsoft versuchte, sich eine Datenbrille für Multiplayer-Spiele patentieren zu lassen, so: Microsoft tries to patent AR glasses for multiplayer gaming, engadget, 2.8.2013, http://www.engadget.com/2013/08/02/microsoft-ar-glasses-for-multiplayer-gaming-patent/*

17 *Simon Parkin: ButtonMasher: First AR games for Google Glass emerge, New Scientist, 1.11.2013, http://www.newscientist.com/article/dn24505-buttonmasher-first-ar-games-for-google-glass-emerge.html*

18 *http://www.youtube.com/watch?v=QxG5xNktqw0*

19 *Victor Middleton, Ken Sutton, Bob Mclntyre, John O'Keefe IV: Soldier Integrated Protective Ensemble (SIPE) Advanced Technology Demonstration (ATD), Dayton, Oct. 2000, p. 22f., http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA384680*

20 *So die Präsentation des britischen Unternehmens Scicon Computer Systems bei der British Army Equipment Exhibition 1984. Diese prototypische Ausrüstung für Soldaten sollte volle AR-Funktionalität mit zusätzlicher Infrarot-Fähigkeit in einem integrierten HMD-Display*

bieten, so: Military Technology, No. 10, 1986, p. 166. Steven M. Shaker, Robert Finkelstein: The Bionic Soldier, in: National Defense, April 1987, S. 27–32. Head-mounted displays (HMDs) für AR-Anwendungen wurden zuerst publiziert als akademisches Paper von Thomas P. Caudell, David W. Mizell: Augmented reality: an application of heads-up display technology to manual manufacturing processes, in: Proceedings of the Twenty-Fifth Hawaii International Conference on System Sciences, 1992, Vol. 2, pp. 659–669.

21 U.S. Army: Force XXI Operations, A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century, TRADOC Pamphlet 525-5, Fort Monroe, Aug. 1994, p. 2–1ff.

22 U.S. Department of Defense, Office of the Assistant Secretary of the Army: Weapons Systems 2012, p. 108f.

23 *Im Warfighter Information Network-Tactical Increment 3 Programm, siehe: U.S. Department of Defense, Office of the Assistant Secretary of the Army: Weapons Systems Handbook 2013, p. 322f.*

24 *Michael M. Bayer, Clarence E. Rash, James H. Brindle: Introduction to Helmet Mounted Displays, p. 47–107, in: Clarence E. Rash, Michael B. Russo, Tomasz R. Letowski, Elmar T. Schmeisser: Helmet-Mounted Displays: Sensation, Perception and Cognition Issues, Fort Rucker, Alabama, 2009, http://www.usaarl.army.mil/publications/HMD_Book09/*

25 *Infanterist der Zukunft, http://www.deutschesheer.de/portal/a/heer/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9jNTUIr-2S1OSMvMxsvYLUouKC1Gy9zLy0xLySVP2CbEdFAPnFG_s!/*

26 *Drittes Auge für deutsche Soldaten, Spiegel Online, 20.2.2013, http://www.spiegel.de/wissenschaft/technik/militaertechnologie-bundeswehr-will-gladius-system-einfuehren-a-884238.html; siehe auch die Pressemitteilung von Rheinmetall, https://www.rheinmetall-defence.com/de/rheinmetall_defence/public_relations/news/archiv/archive_2015/index~1_3264.php*

27 *So: Samuel Liles: Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency, Conference on Cyber Conflict, NATO CCD COE Publications, 2010, p. 47–57.*

28 *Mind Commerce: Augmented Reality in the Battlefield 2012–2016, ADS Report, Amsterdam, Juli 2012, https://www.asdreports.com/shopexd.asp?id=32490*

29 *Matthew Sparks: New York Police Testing Google Glass, The Telegraph, 7.2.2014, http://www.telegraph.co.uk/technology/google/10623753/New-York-police-testing-Google-Glass.html*

30 *Polizei in Dubai geht mit Google-Datenbrille auf Verbrecherjagd, in: Reuters, 2.10.2014, http://de.reuters.com/article/dubai-google-datenbrille-polizei-idDEKCN0HR19T20141002*

31 *Peter Welchering: Was die Polizei von morgen über uns weiß, www.heute.de, 15.6.2016, http://www.heute.de/polizeiausruestung-thema-bei-innenministerkonferenz-was-die-polizei-von-morgen-ueber-uns-weiss-43944016.html*

32 *Terrorismusbekämpfung: Zu wenig Ermittler? ARD Hauptstadtstudio-Blog, 15.10.2016, http://blog.ard-hauptstadtstudio.de/terrorismusbekaempfung-zu-wenig-ermittler/*

33 *In den ersten sechs Monaten 2016 wurden von den deutschen Sicherheitsbehörden über 210.000 Stille SMS zur Ortung von Handys verschickt, vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Abg. Hunko u. a.: Einsätze von sogenannten stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im ersten Halbjahr 2016, vom 9.8.2016, Bt.-Drs. 18/9366, Frage 4.*

34 *Sie gaukeln eine Basisstation vor Ort vor und ermitteln so die Telekommunikationskennungen der Mobilgeräte von unbekannten observierten Personen.*

35 *Marco Dettweiler, Tillmann Neuscheler: Computersimulierte Menschenströme: Eine Viertelstunde in die Zukunft schauen, in: FAZ, 17.10.2016, http://www.faz.net/aktuell/gesellschaft/ende-der-loveparade/computersimulierte-menschenstroeme-eine-viertelstunde-in-die-zukunft-schauen-11008870.html; siehe auch: Crowd Management: Smartphone soll Massenpanik verhindern, http://www.golem.de/news/crowd-management-smartphone-soll-massenpanik-verhindern-1209-94331.html*

36 *So verfügen Landes- und Bundespolizeibehörden neben IMSI-Catchern, die eine Funk-Basisstation vorgaukeln, über Beweissicherungs- und Dokumentationskraftwagen, die Handy-Besitzer metergenau lokalisieren können sollen, siehe Detlef Borchers: Bessere Handy-Ortung für die deutsche Polizei, heise online, 9.8.2014, http://www.heise.de/newsticker/meldung/Bessere-Handy-Ortung-fuer-die-deutsche-Polizei-2289542.html; siehe auch die Antwort der Bundesregierung auf die Kleine Anfrage der Abg. Hunko u. a.: Neue digitale Überwachungsmethoden, Frage 17 ff.*

37 *Ronald Eikenberg: IP-Kameras von Aldi als Sicherheits-GAU, heise Security, 15.01.2016, https://www.heise.de/security/meldung/IP-Kameras-von-Aldi-als-Sicherheits-GAU-3069735.html*

38 *Drama in Einkaufszentrum: Präsident meldet Sieg über Geiselnehmer in Nairobi, http://www.spiegel.de/politik/ausland/praesident-meldet-sieg-ueber-geiselnehmer-in-nairobi-a-924322.html; zu Pakistan und Indien: Hasnain Kazim: Angriff in Lahore: Taliban richten Blutbad in Moscheen an, Spiegel Online, 28.5.2010, http://www.spiegel.de/politik/ausland/angriff-in-lahore-taliban-richten-blutbad-in-moscheen-an-a-697393.html*

39 *Thomas Gibbons-Neff: Why the Army is worried about insurgents turning to remote-controlled weapons, The Washington Post, 30.8.2016, https://www.washingtonpost.com/news/checkpoint/wp/2016/08/30/insurgent-groups-such-as-isis-are-increasingly-turning-to-remote-controlled-weaponry-army-report-says/; siehe auch: Robert J. Bunker, Alam Keshavarz: Terrorist and Insurgent Teleoperated Sniper Rifles and Machine Guns, Foreign Military Studies Office, Kansas, August 2016, http://fmso.leavenworth.army.mil/documents/20160822_BUNKER%20and%20KESHAVARZ_Teleoperated%20Sniper%20Rifles%20article.pdf*

VR4two – A new universe of opportunities with "VR4two"
Foto: sndrv, CC BY 2.0

Editorial zum Schwerpunkt

In einer digitalisierten Gesellschaft untergraben unsichtbare Systeme die individuelle Selbstbestimmung und die demokratische Mitbestimmung. Doch nicht nur das, die Manipulation des Denkens und Handelns ist zur treibenden Kraft der IT-Entwicklung geworden. Dies wurde vom 25. bis zum 27. November 2016 in Berlin auf der FIfF-Konferenz 2016 deutlich.

Unsere digitale Umwelt ist frei von Öl, Staub und Müll. Wir erfahren und erleben sie durch glänzende Oberflächen, flüssige Animationen und ästhetische Bilderwelten. Wir werden mit sozialen Räumen und (freiem) Internet versorgt, unsere E-Mail-Boxen und Kalender werden für uns betrieben, unsere Daten bequem entfernt verwahrt, das Internet durchsuchbar gehalten, der Straßenverkehr optimiert und unser Zahlungsverkehr abgewickelt. Nun bleiben wir fit, können schneller Taxis finden und Zimmer vermieten. Gesundheitssysteme, der ÖPNV und auch andere staatliche Aufgaben werden digitalisiert. All dies geschieht mit Hilfe größtenteils unsichtbarer Systeme.

Zweck von Informationstechnik ist immer auch Komplexitätsreduktion und -verschleierung. Die Zusammenhänge bleiben nicht nur unsichtbar, sondern sie werden ganz gezielt versteckt. Dies geschieht einerseits zur sinnvollen Komplexitätsreduktion, andererseits aber auch, um verdeckte Zwecke zu verfolgen. Die Möglichkeit, ein inzwischen durchdigitalisiertes Leben und die genutzte Infrastruktur mündig zu beurteilen oder gar zu gestalten, wird so zunehmend unmöglich gemacht.

Kriegführung im Cyberspace steht im Widerspruch zur IT-Sicherheit und macht sich doch deren Methoden zunutze. Um den Cyberkrieg führen zu können, werden Schwachstellen in IT-Systemen geheim gehalten oder im Verborgenen erzeugt. Autonome Waffen werden im Geheimen entwickelt, und ihre Algorithmen und Verfahren entscheiden eigenständig und für den Menschen unsichtbar über Leben und Tod.

Die Überwachung der Menschen durch Geheimdienste, Sicherheitsbehörden und private Akteure schreitet dabei fort: Durch weltweite Kommunikationsüberwachung, durch Videoüberwachung des öffentlichen und privaten Raums und durch biometrische Verfahren zur weiteren Automatisierung und Erkennung. Technologien wie *Big Data* erweitern das Instrumentarium der Überwachung – auch hier sind die automatisierten Entscheidungen und Ergebnisse für die Nutzer.innen oft nicht mehr nachvollziehbar. Effektiver Datenschutz muss juristisch und technisch durchgesetzt und sichergestellt werden.

Themen der Konferenz waren Geheimdienste und die Defizite ihrer (parlamentarischen) Kontrolle; Informationsfreiheit, ihre Verhinderung durch Amtsträger.innen und der Versuch, sie wieder durchzusetzen; Techniknutzung und Algorithmen in sozialen Kontexten; Ethik in Informatik und Wissenschaft; Theorien der Transparenz; kultivierte Unsichtbarkeit; das technisch Unbewusste. Mehrere Workshops ergänzten das Programm zu Themen wie Malware, globalen Friedensinitiativen, Menschenrechten, politischer Informatik und nachhaltiger Mobilität.

Die Vorträge der Konferenz sind in dieser Ausgabe der *FIfF-Kommunikation* dokumentiert:

Stefan Ullrich führte in die Tagung ein. *Kleine Geschichten verborgener Technik* war der Titel seines Vortrags, in dem er Beispiele aus der Geschichte benannte und den Bogen zur FIfF-Konferenz 2014 an gleicher Stelle schlug: „Im Gegensatz zur FIfF-Jahres-Konferenz 2014, die angesichts des offenkundigen Grundrechtsbruchs durch Geheimdienste ein Ausrufezeichen setzen wollte, möchten wir diesmal große Fragezeichen hinter Themen setzen, die unsere heutige von Technik durchdrungene Welt uns auf dem gebürsteten Alutablett serviert. … Eine Leitfrage der Konferenz ist daher auch ‚Wieviel Transparenz ist nötig und wieviel Transparenz ist (ohne Funktionseinbußen) möglich?'"

Der massive Einsatz hochentwickelter Schadsoftware durch NSA und GCHQ war Thema des Beitrags von *Ernst Möchel*: *CYBER! Der Staat als Krimineller*. *Jan Philipp Albrecht* saß als Berichterstatter im Europäischen Parlament an der Schaltstelle für die neu verabschiedete *EU-Datenschutz-Grundverordnung*. Er berichtete von *weitergehenden Erkenntnissen aus den Verhandlungen* – Grundannahmen der Unternehmen und staatlichen Akteure und den Folgerungen daraus. *Anna Biselli* berichtete aus dem NSA-Untersuchungsausschuss des Bundestages, dessen Sitzungen sie verfolgt und für *netzpolitik.org* gebloggt hat, und fragte, ob und wie Geheimdienste kontrollierbar sind und ob derartige Institutionen in eine demokratische Gesellschaft passen: *Geheimdienste außer Kontrolle und warum die BND-Reform keine ist*.

Transparenz zwischen normativem Anspruch und kultivierter Unsichtbarkeit, so der Beitrag von *Leon Hempel*. Beobachtung erfolgt in sozialen Situationen. Sie verlangt Kooperation zwischen den Akteuren, der beobachtenden Instanz und den Beobachteten – und dies in Kontexten von Überwachung und Kontrolle als Zwang. Der Beitrag diskutiert das Problem der Transparenz in einem Raum kooperativen Zwangs. Mit der *sozialen Gerechtigkeit von Algorithmen* setzte sich danach *Corinna Bath* auseinander. Im Fokus ihres Vortrags standen Verzerrungen, die als sexistisch, rassistisch oder anderweitig ungerecht bezeichnet werden können. Ihr Ziel war es, Möglichkeiten der Analyse ungerechter und der Gestaltung sozial gerechterer Algorithmen zu eröffnen. *Marit Hansen*, Landesbeauftragte für den Datenschutz in Schleswig-Holstein, fragte in ihrem Vortrag, ob *Datenschutz im Unsichtbaren funktioniert*, und thematisierte *Datenschutzgarantien, Transparenz und Intervenierbarkeit in versteckter Informationstechnik*. Welche Herausforderungen bestehen angesichts einer für die Betroffenen (und sogar für so manchen Datenverarbeiter) unsichtbaren Funktionalität?

Die weitgehend verborgene Entwicklung autonomer Waffen war das Thema von *Hans-Jörg Kreowski*. In den Waffenschmieden und Denkfabriken der NATO und sicher auch darüber hinaus findet seit einigen Jahren eine weitgehend vor der Öffentlichkeit verborgene Entwicklung autonomer Waffen statt. Er diskutierte in seinem Vortrag den Stand der Technik, die technischen Herausforderungen autonomer Systeme und die Perversität des autonomen Tötens. Danach ging es um den Frankfurter Internetknoten DE-CIX und *Die neue Globalisierung – wenn das Inland zum Ausland wird*: *Klaus Landefeld* beantwortete die Frage, was die Klage gegen den BND wegen Überwachung an DE-CIX mit der BND-Reform nach dem Beschluss zur Ausland-Ausland-Fernmeldeaufklärung zu tun hat. Sehr viel, wie sich herausstellt.

Judith Simon referierte über *Un.Sichtbare Datenpraktiken? Big Data in Wirtschaft, Wissenschaft und Politik*. Die Proliferation von Big-Data-Praktiken ist ein relativ neues und komplexes Thema. Ein wesentlicher Teil ihrer Governance seien neben den rechtlichen Regelungen auch die transparenzförderliche Gestaltung der IT-Systeme. *An den Enden der Informatik* bewegte sich *Wolfgang Coy*: „So wie die Physik vom Subatomaren bis zum Kosmischen forscht, spannt sich die Informatik von den beliebig unterteilten Dingen des *Internet of Things* bis zu den weltumspannenden Netzen, die im letzten Jahrzehnt riesige Data Center als Knoten ausgebildet haben. Wir bewegen uns im digitalen Nebel der Clouds und im Dunstkreis unserer Wearables in immer engmaschigeren Datengeweben."

„Wird Biometrie inzwischen breiter akzeptiert, weil die Nutzer.innen sie besser verstehen?" Das fragt *Andrea Knaut* in ihrem Originalbeitrag: *Sie haben den Nutzen der Technik noch nicht rational erkannt! – Biometrie verstehen und akzeptieren.* Sie diskutiert darin die Bedeutung der Offenlegung der Fehler und Funktionsweisen von biometrischer Überwachungstechnik für ihre bessere Akzeptanz im Alltag.

Informationen verstecken und Informationen herauskitzeln: Von ihren Versuchen, als Bürgerin Zugriff auf staatliche Informationen für ihre journalistische Arbeit zu bekommen, berichtet *Gaby Weber*. Sie diskutiert dabei auch die zweifelhafte Praxis von Amtsträger.innen, sensible Akten einfach „mit nach Hause" zu nehmen und damit dem Zugriff der Öffentlichkeit zu entziehen – tolerierter Diebstahl in ihren Augen.

Den Widerspruch zwischen IT-Sicherheit und Cyberwar diskutieren *Kai Nothdurft* und *Sylvia Johnigk* in ihrem Originalbeitrag: *We hate to say we told you so – IT-Sicherheit als Kriegshandwerk*. Sie untersuchen dabei, welche Voraussagen der letzten Jahre zur IT-Sicherheit – genauer: zu deren Schwächung – inzwischen tatsächlich eingetreten sind.

Der Fall des damaligen Verteidigungsministers Karl-Theodor zu Guttenberg schlug hohe Wellen – seither sind noch einige weitere spektakuläre Fälle von Plagiaten in wissenschaftlichen Arbeiten an die Öffentlichkeit gelangt: 175 Fälle sind derzeit im dafür genutzten Wiki *VroniPlag* – benannt nach Veronika Saß, der Tochter von Edmund Stoiber, deren Dissertation als Erste damit untersucht wurde – dokumentiert. *Viel Licht und noch mehr Schatten*, so das Fazit von *Debora Weber-Wulff* zum Thema *Plagiat in Dissertationen*.

Rückschau auf 10 Jahre Informationsfreiheitsgesetz hielt *Arne Semsrott*: *Wie wir den Staat zu mehr Transparenz zwingen*. Obwohl der Zugang zu staatlichen Informationen längst als Teil der Menschenrechtskonvention und der Jahrhundertziele der Vereinten Nationen anerkannt sei, bleibe das Thema in Deutschland aufgrund mangelnden Engagements und schlechter Gesetze aber meist unter dem Radar. „Wie können wir das ändern? Und welche Mittel haben wir?" – so die Fragen, auf die er in seinem Beitrag Antworten suchte. Einen Blick auf die Situation in Südkorea bot uns zum Abschluss der Tagung die Journalistin *Ok-Hee Jeong*: *Social Media in Südkorea: Staatliches Machtinstrument vs. „fünfte Gewalt" in einer defekten Demokratie*. Wie der Staat mithilfe der Social Media die Bürger manipuliert und lenkt, aber gleichzeitig wie unentbehrlich die Rolle der Social Media als „fünfte Gewalt" in dieser defekten Demokratie ist, beleuchtete sie in diesem Beitrag anhand einiger Beispiele.

Kooperationspartner des FIfF bei der Tagung waren das *Zentrum für Technik und Gesellschaft* (ZTG) der TU Berlin, die Fachgruppe *Informatik und Ethik* der Gesellschaft für Informatik (GI), der Chaos Computer Club (CCC), Alexander Lehmann, das VOC für die Videos und Streams und d1zz1 für die Lichtinstallationen. Die Web-Seite mit weiteren Informationen ist unter *https://2016.fiffkon.de* zu finden. Von dort sind auch die Videoaufzeichnungen der Vorträge verlinkt, die unter *https://media.ccc.de/c/fiffkon16* abgerufen werden können. Für die Unterstützung der Konferenz bedanken wir uns herzlich.

Die Texte auf den folgenden Seiten sind – soweit die Autor.innen nicht ausdrücklich als solche genannt sind – nicht-autorisierte Zusammenfassungen der Vorträge auf der Tagung, die gleichwohl mit größtmöglicher Sorgfalt zusammengestellt wurden. Großartige Arbeit für diesen Schwerpunkt leisteten Juliane Krüger und Kai Lücke. Herzlichen Dank.

Zuletzt: Es gilt das gesprochene Wort! Sollten sich bei der Verschriftlichung Fehler eingeschlichen haben, gehen diese selbstverständlich zu Lasten der Redaktion.

Benjamin Kees, Rainer Rehak, Stefan Hügel
für die Schwerpunktredaktion

Stefan Ullrich

2016: Kleine Geschichten verborgener Technik

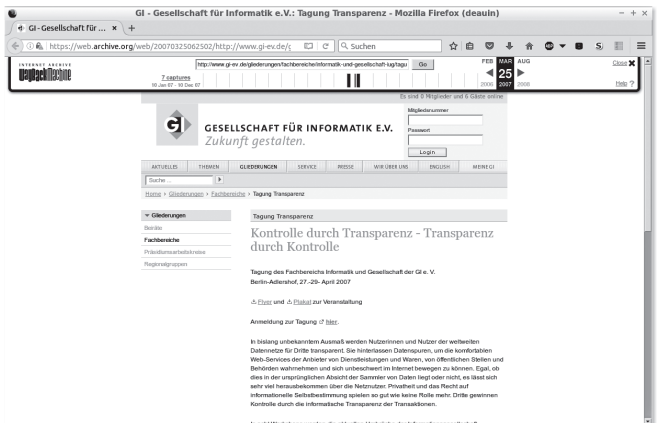
Das Verstecken von Zahnrädern, Kabeln und sonstigen technischen Bestandteilen hat Tradition, man denke nur an Vaucansons Flötenspieler oder den doppelten Boden in den Serverräumen von IBM. Interessierte oder gar versierte Nutzerinnen und Nutzer sind in der Schönen Neuen Welt nicht erwünscht: „You Press the Button, We Do the Rest". Doch was passiert, wenn wir die Wartungsklappe öffnen?

Ich werde gleich umfänglich über die Technikgeschichte des Okkulten referieren. Danach zwei Kapitel aus meiner Dissertation über unsichtbare Mechanismen der Öffentlichkeit, gefolgt von einer Eloge auf den technischen Äther. Dann haben wir Zeit für eine Diskussion.[1]

Kontrolle durch Transparenz

Vor knapp zehn Jahren veranstaltete der Fachbereich *Informatik und Gesellschaft* der Gesellschaft für Informatik eine Tagung zum Thema *Transparenz*.[2] Die Veranstaltungswebsite ist allerdings selbst ziemlich transparent geworden, der geneigte Internaut findet sie glücklicherweise über die Wayback-Machine des Internet-Archivs von *archive.org* wieder. Die Informatik-und-Gesellschaft-Community war damals sehr besorgt über die Einführung von ELENA, dem elektronischen Einkommensnachweis, und anderen staatlichen und behördlichen Datensammelprogrammen. Einige der zentralen Forderungen klingen recht hilflos, beispielsweise heißt es in der Pressemitteilung der GI vom 31. Mai 2007:

> *„Die Bürger müssen die Hoheit über ihre Daten dauerhaft zurückerhalten. Um dies zu erreichen, müssen Gesetze und Verwaltungsverfahren entsprechend umgestaltet werden."*



Tagungsankündigung der GI aus dem Jahre 2007

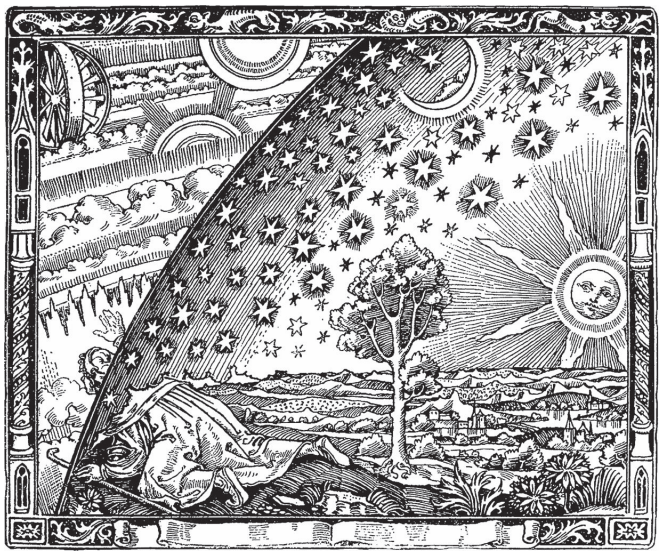
„Zurückerhalten!" Die Hoheit über die eigenen Daten sei also schon längst verloren, so die Einschätzung der damaligen Teilnehmerinnen und Teilnehmer der Tagung *Kontrolle durch Transparenz – Transparenz durch Kontrolle*. Hier im Publikum sehe ich ein paar Teilnehmende, die, ihrem Gesichtsausdruck nach zu urteilen, tatsächlich die Forderung noch immer nicht erfüllt sehen. 2007 hatte die GI allerdings auch nicht die Geheimdienste auf dem Schirm, das FIfF ist in dieser Hinsicht, also wenn es den industriell-militärischen Komplex betrifft, schon immer etwas sensibler gewesen; und so freut es mich, dass wir mit dieser Konferenz ein wenig Licht ins Dunkel geheim operierender Akteure bringen werden.

Der naive Wanderer am Weltenrand

Der Verdacht, dass hinter der *Schönen Neuen Welt* irgendetwas Düsteres oder zumindest Geheimnisvolles stecken muss, ergab sich natürlich schon wesentlich früher, es ist eine Grundbedingung des vernunftbegabten neugierigen Menschen, sich zu fragen, was denn das alles hier soll, das Leben, das Universum und der ganze Rest. Die Mythen der Menschheit sind voller Bilder über Geheimtechniken geheim agierender Gottheiten oder anderer allmächtiger Wesen.

Zunächst verschlangen die bis dahin unmündigen Bewohner des Langeweileparadieses die Frucht des Erkenntnisvermögens, danach entbarg der prometheische Mensch die okkulte Technik des Feuermachens, schließlich veräußerten die Geisteswesen ihre verborgenen Gedanken mit Hilfe von Rede, Bild, Schrift und Zahl in der Hoffnung, dass ihr Gegenüber durch diese Medien in der Lage wäre, sich in andere hineinzuversetzen.

Die Exegese heilig genannter Schriften und Bilder, das Betreiben von Zahlenmystik oder das laut gesprochene „aum“ (ॐ), sie alle sollen helfen, »Daß ich erkenne, was die Welt // Im Innersten zusammenhält«.



Flammarions Holzstich

Der Wanderer am Weltenrand, so berichtet Camille Flammarion 1888, war ein naiver Mensch des Mittelalters, der eine Stelle entdeckte, wo Himmel und Erde sich zwar berührten, aber nicht gut verschweißt waren. So war er in der Lage, einen Blick hinter den Horizont zu werfen.

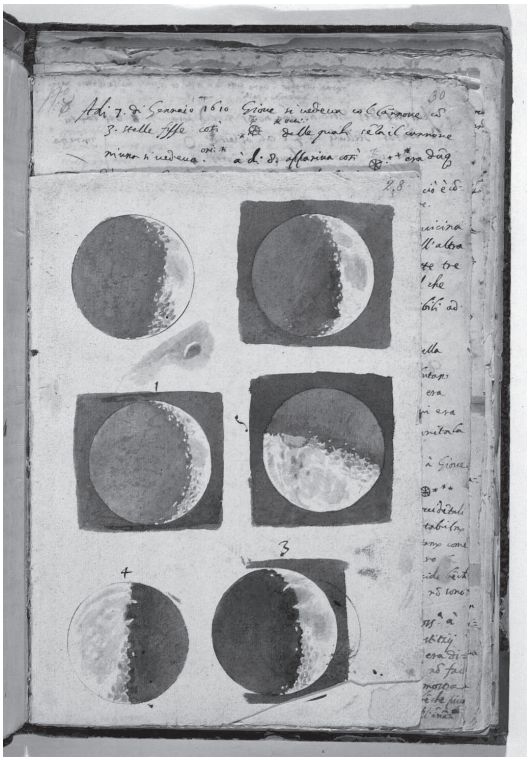
Der bekannte Holzstich zu der Geschichte dient bis heute als Illustration der kopernikanischen Wende und anderer Zäsuren der Wissenschaftsgeschichte. Das Motiv ist uns durch moderne dystopische Literatur ebenfalls bekannt: Die Protagonistin stolpert durch Zufall hinter die Bühne der Welt und wird auf die dort verborgenen Mechanismen aufmerksam, die nicht unbedingt zum Vorteil aller Menschen ihre Geschicke bestimmen.

Die technische Sprache von Flammarion, die *Schweißnaht* zwischen Himmel und Erde oder *couvercle*, Luke, Wartungsklappe, Verschlussdeckel, verrät ihn als Kind des 19. Jahrhunderts, auch wenn schon seit der Antike technische Metaphern für kosmologische Vorgänge verwendet wurden. Das Wort Himmelsgewölbe ist ja auch ein technischer Ausdruck.

Flammarion illustriert mit diesem Holzstich eine (populär-)wissenschaftliche Abhandlung über die Wetterbeobachtung. Zwei Absätze unterhalb des *Naiven Wanderers* schreibt er über die faszinierende Tatsache, dass wir tagsüber unsere Atmosphäre dank unserer Sonne und dank anderer physikalischer Wunder als blauen Himmel wahrnehmen. Die eigentlich transparenten Schichten, die in der Nacht den Blick auf die Sterne freigeben, werden opak, wir blicken in den Himmel und sehen doch unsere Erde.

Und sie bewegt sich doch

Nachts sehen wir ja nicht nur die Sterne, sondern auch Merkur, Venus, Mars, Jupiter, Saturn und natürlich den Mond. Momentan sind wir ein paar Tage vor Neumond, der Mond sieht heute ziemlich genau so aus wie in der ersten Abbildung von Galilei – wenn wir ihn rotieren, natürlich, denn die Zeichnung stellt einen zunehmenden Mond dar. Wäre auch zu schön gewesen…



Galileo Galilei (1564-1642) Drawings of the Moon

Im ersten Band der *edition*-Reihe des Suhrkamp-Verlags lässt Bertolt Brecht den berühmten Galileo Galilei seine Erfindung anpreisen:

> *„Mit tiefer Freude und aller schuldigen Demut kann ich Ihnen heute ein vollkommen neues Instrument vorführen und überreichen, mein Fernrohr oder Teleskop, angefertigt in Ihrem weltberühmten Großen Arsenal nach den höchsten wissenschaftlichen und christlichen Grundsätzen, Frucht siebenzehnjähriger geduldiger Forschung Ihres ergebenen Dieners.“*

Galileo tritt von dem Fernrohr zurück und lässt die Venture Capitalists und CEOs von Venedig durchschauen. Leise flüstert er seinem Freund Sagredo zu:

> *„Ich kann dir nicht versprechen, daß ich den Karneval hier durchstehen werde. Die meinen hier, sie kriegen einen einträglichen Schnickschnack, aber es ist viel mehr. Ich habe das Rohr gestern nacht auf den Mond gerichtet. […] Er leuchtet nicht von selbst.“*

Sie werden von den Ratsherren unterbrochen, die das Fernrohr auf weltliche Dinge, speisende und badende Frauen, gelenkt haben und sich höchst erfreut über die Erfindung zeigen.

Galileo wird die Freude trüben, denn obwohl er die holländische Erfindung nach christlichen Grundsätzen verbessert haben will, so stellt er doch kirchliche Dogmen fundamental in Frage. Der Mond war keine perfekte, leuchtende Kugel, sondern pockennarbig mit Tälern und Bergen. Was der Mond der Erde, ist die Erde dem Mond.

Die Verurteilung des Galilei fiel in das Pontifikat von Papst Urban VIII., Jesuit und doctor iurisprudentiae, der zwar ein Freund der Wissenschaft und der Kunst war, sich jedoch nicht gegen die mächtige Inquisition stellen konnte. Im Theaterstück von Brecht versucht er, die Wissenschaft, namentlich Sternenkarte und Rechentafel, zu verteidigen, der Inquisitor jedoch erwidert:

> *„Daß es die Rechentafel ist und nicht der Geist der Auflehnung und des Zweifels, das sagen diese Leute. Aber es ist nicht die Rechentafel. Sondern eine entsetzliche Unruhe ist in die Welt gekommen. Es ist die Unruhe ihres eigenen Gehirns, die diese auf die unbewegliche Erde übertragen. Sie schreien: die Zahlen zwingen uns! Aber woher kommen ihre Zahlen? Jedermann weiß, daß sie vom Zweifel kommen."*

In dieser Logik sei das Teleskop also ein Produkt des Zweifels und so verwundert es nicht, dass man alles in Frage stellt, was man damit sieht. Der Zweifel selbst sei quasi eingebrannt in die Hardware. Jeder, der durch das Fernrohr blickt, sieht nicht mit menschlichem Auge allein, sondern mit dem Auge des Zweifels. Das ist eine frühe Formulierung dessen, was wir später mit dem Schlagwort *Informationelles Vertrauen* beschreiben werden.

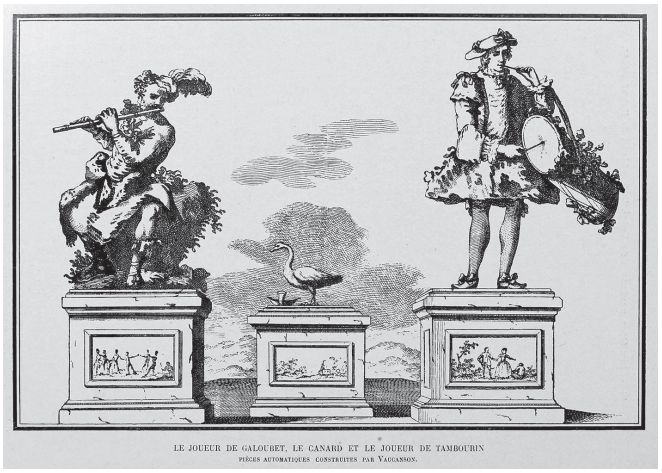
Ja, wir gelangen durch ein Instrument an Daten, doch um diese Daten zu überprüfen, müssen wir wieder das Instrument nutzen. Ob wir dem Instrument vertrauen oder nicht, ist eine fundamental epistemologische Frage. Auch dazu werden wir hier Vorträge hören.

Knowledge brings fear, so lautet das Motto der Marsianischen Universität in der Trickfilmserie *Futurama*. Auch im Theaterstück wird die bedingungslose Publizität aller Erkenntnis als etwas Schreckliches dargestellt: Die hart arbeitenden, armen und nicht selten hungernden Leute ziehen ihren Lebenswillen aus Gott, der über sie wacht und spätestens nach dem (frühen) Tod auch liebevoll umsorgt. Wenn sie nun erfahren, dass der feste Grund sich drehe, sie unendlich klein in der Unendlichkeit des Universums seien und Gott auch noch mies in Mathe und Physik, also fehlbar war, hätten sie nichts mehr, was sie noch hält. (Unser Innenminister wird ein paar Jahre später etwas sehr Ähnliches über die Wahrheit und die damit einhergehende Beunruhigung der Bevölkerung sagen.)

Die Ente von Jacques de Vaucanson

Ganz von der Hand zu weisen ist das Argument ja nicht. Neue Erkenntnisse, besonders auf technischem Gebiet, werfen stets neue Zweifel an vorherrschenden Welt- und Menschenbildern auf. Gerade technische Artefakte zeigen – wie der Himmel auf die Erde – auf den Hersteller solcher Artefakte. Acker- und Bergbau führte zum Bild des Menschen als aus Erde geformtes Wesen bzw. als ein tönendes Erz, der Descartes'sche Homunculus blickt von der Zirbeldrüse durch geschliffene Linsen auf die Welt und inzwischen ist den Informatikerinnen und Informatikern ja klar, dass das menschliche Gehirn wahrlich ein paar *security software updates* nötig hätte.

Auf der Abbildung in der rechten Spalte sehen wir drei Automaten, die mit lebensimitierenden Funktionen aufwarten konnten: Links der Flötenspieler, rechts der Trommler. Doch kaum ein anderer Automat beschäftigte die europäische Öffentlichkeit im Zeitalter der Aufklärung so nachhaltig wie die mechanische Ente (hier in der Mitte) des französischen Erfinders Jacques de Vaucanson. Nachdem der Sohn eines Handschuhmachers der französischen Akademie der Wissenschaften 1738 seinen mechanischen Flötenspieler vorgestellt hatte, der ein dutzend einfachste Lieder spielen konnte, wenn die entsprechende Walze eingelegt war, präsentierte er schließlich die berühmte Ente.



Automatischer Trommler und Flötenspieler (Jacques de Vaucanson 18. Jh.)

Die Ente konnte mit den Flügeln schlagen, Kopf wie Bürzel bewegen und imitierte aufs sorgfältigste auch weitere Funktionen ihres tierischen Pendants, wie der Erfinder selbst in einem Brief[3] an einen gewissen Monsieur l'Abbé D. F. schrieb, sie reckte ihren Hals, um eines Korns habhaft zu werden, sie schluckte und verdaute es. Der Vorgang der Verdauung ist im Brief sehr ausführlich beschrieben mit der jeweiligen Entsprechung in der Feinmechanik. Am Ende schied die Ente tatsächlich etwas aus, das als Verdauungsprodukt durchgehen konnte – Wissenschaft zum Greifen nahe. Die Metamorphose von Korn zu Kot in einem mechanischen Wesen beschäftigte die intellektuelle Elite noch Jahre später. Goethe war regelrecht enttäuscht, als er die Automaten um 1805 bei Gottfried Christoph Beireis sah: »Die Ente, unbefiedert, stand als Gerippe da, fraß den Haber noch ganz munter, verdaute jedoch nicht mehr.«[4]

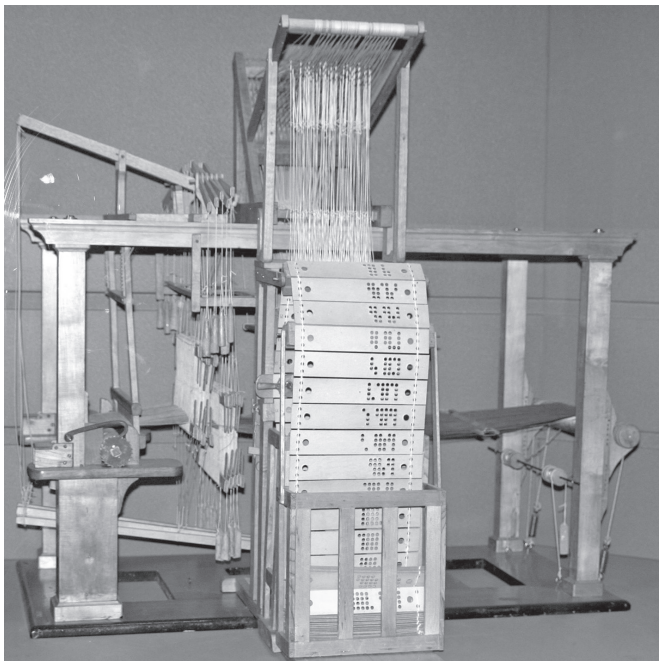
Dass Goethe nur ein Gerippe vorfand, war übrigens nicht allein dem Alter geschuldet: Vaucanson selbst wollte Bewegungs- und eben Verdauungsvorgänge so transparent wie möglich gestalten. Das Wunderwerk der Technik sollte für sich sprechen, «toute la mécanique du Canard artificiel sera vûë à découvert». Im gleichen Brief dachte er über eine eventuelle Ummantelung nach, die sensible Personen vor dem Anblick schützen sollte. Er lehnte dies jedoch strikt ab, ging es ihm doch um die Darlegung und nicht um eine Schau: « mon dessein étant plûtôt de démontrer, que de montrer simplement une machine ».[5]

Am Ende siegte der Ruhm: Jacques de Vaucanson schickte seine Automaten auf eine Tournee, nicht auf Vorlesungsreise. Die Ente war die Schau, ein Großteil der Mechanik war ohnehin im Sockel versteckt, eine perforierte Folie bedeckte nun das lebensgroße mechanische Tier.

Das Buch zum Film, pardon, zu den Automaten wurde vom königlichen Zensor freigegeben, sogar mit lobenden Worten, die uns daran erinnern, dass Zensur zu früheren Zeiten nicht negativ besetzt war. Heute würden wir vielleicht *kuratiert* sagen, wenn wir den Auswahlprozess populärwissenschaftlicher Werke beschreiben wollen. Der Zensor betont ausdrücklich, dass mit dem vorliegenden Buch von Vaucanson über seine Automaten die Neugier der Öffentlichkeit an technischen Erfindungen befriedigt wird und es daher wert ist, publiziert zu werden. Prädikat: Besonders wertvoll.

Der Jacquardwebstuhl

Der Erfinder selbst wandte sich später der Automatisierung von Webstühlen zu. Ich muss zugeben, dass ich am Anfang meines Informatik-Studiums nicht so recht wusste, warum mir der Professor da vorn etwas über Webstühle erzählte. Rückblickend wüsste ich allerdings nicht, wie man das Forschungsprogramm *Informatik und Gesellschaft* ohne Joseph Marie Jacquards Webstuhlprogrammierlochkarten aufziehen könnte.



Modell eines Jacquard-Webstuhls, für jeden unabhängig steuerbaren Kettensatz gibt es eine Lochreihe auf der Karte
Foto: Rama, CC BY-SA 2.0 fr

Die nie gebaute Analytical Engine von Charles Babbage nahm sich die automatisierten Webstühle mit ihrem Musterspeicher, der Lochkarte, zum Vorbild; Babbages Texte und Ideen zu Industriemaschinen wurden von Karl Marx aufgegriffen; kurz, die Industrielle Revolution und die Herausbildung einer Arbeitergesellschaft als Ausgangspunkt für Informatik und Gesellschaft zu nehmen, ist vielversprechend, gerade, wenn man sich aktuelle Diskurse zu *Industrie 4.0* ansieht.

Die (vielleicht doch eher herbeigeredete) *Vierte Industrielle Revolution*, ausgelöst durch die Vernetzung der allgegenwärtigen informationstechnischen Systeme, fokussiert die Information. Die Informatiker als neue Pythagoräer rufen mit Leibniz entzückt, nein verzückt: „Alles ist Binär-Zahl." Webmuster im wüllenen Tuch? Information! Hunger und Armut? Ein Verteilungsproblem, das optimierbar ist, also auch: Information! Zugang zu sauberem Trinkwasser? Wissen, also auch: Information!

Mit der größenwahnsinnigen Annahme, alle Probleme der Menschheit seien berechenbar und somit lösbar, geht die nicht minder irrsinnige Annahme einher, alle Probleme der Menschheit würden nun auch berechnet und gelöst werden. Wenn die Spinning Jenny die Produktivität vervielfacht, so dass nun ein einzelner Spinner einen Weber versorgen konnte, heißt das im Umkehrschluss, dass sieben Spinner ihren Job verloren. Wenn Industriemaschinen immer einfacher zu bedienen sind, heißt das auch, dass der Kinderarbeit nun weniger im Weg steht und dass die einzelnen Arbeiter austauschbar geworden sind.

> *„Ganze Regionen der Erde verwandeln sich in die hässliche Kehrseite der schönen neuen Digitalwelt. Wenn auf IT-Fachmessen wie der Hannover-Messe von* Industrie 4.0 *gesprochen wird, so sollte man dies nicht als Modewort auf einem Buzzword-Bingo-Feld abtun, sondern als Warnung begreifen: Die* Industrie 1.0 *war vielleicht nicht allein, aber sicher nicht zuletzt für die entstehende Armut eines großen Teils der Arbeiterschaft und der Landbevölkerung verantwortlich. Bequemerweise zeigt sich der* Pauperismus 4.0 *jedoch nicht hierzulande, sondern weit ab der* social media sphere.*"*[6]

Leider konnten wir in diesen Jahr keinen Workshop der Arbeitsgruppe *Faire Computer* anbieten, an dieser Stelle muss daher der Hinweis auf die Webseite *faire-computer.de* ausreichen, die sich diesem Themenkomplex annimmt. Ein Leitmotiv dabei: Fehlende Transparenz und mangelnde Kontrolle bei Vertriebswegen, Entsorgung und Arbeitsbedingungen.

Die giftige Seite der Technik

40°37'32.9"N 109°40'10.1"E

Der Giftsee bei Baotou, Quelle: © 2016 DigitalGlobe

Na, vielleicht sollte ich das dann doch jetzt einschieben, auch wenn ich mich bei Chronos entschuldigen muss. Was ihr hier seht, ist ein See aus Giften. Der Journalist Tim Maughan schrieb vor einem Jahr in *BBC Future* über den schrecklichsten Platz auf Erden, ich selbst schrieb in einem Artikel damals darüber:

> *„[Tim Maughan] besichtigte zusammen mit der Gestalter-Gruppe »Unknown Fields Division« die größte industrielle Siedlung in der Inneren Mongolei, Baotou (Buyutu). Die weltweit größten Vorräte an Metallen der*

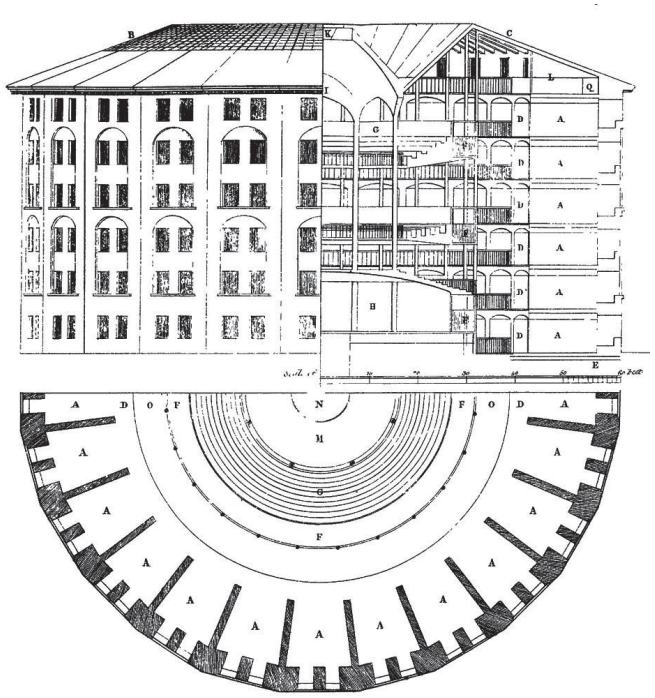
Seltenen Erden finden sich genau dort — also genau die Elemente, die der moderne Mensch so dringend für seine elektronischen Gadgets wie Tablets, Smartphones und dergleichen benötigt."[7]

Im Titel habe ich einmal die GPS-Koordinaten angegeben, um darauf hinzuweisen, dass dieser Aspekt zwar im gegenwärtigen Diskurs verborgen ist, sich jedoch nicht den Satellitenkameras entzieht. In meiner Diplomarbeit von 2009 beschäftigte ich mich erstmals mit den Millenniumszielen der Vereinten Nationen, die selbst gesetzte Frist ist inzwischen abgelaufen.

„Selbst die optimistischsten Technik-Liebhaber müssen sich eingestehen, dass die gesamten Protagonisten der so genannten Industrie 4.0 *keines der Ziele angegangen sind – zumindest nicht in den ärmsten Regionen der Welt. Im Gegenteil, die Möglichkeit zur Selbsthilfe wurde und wird systematisch untergraben. Fruchtbares Ackerland, das seltene Erden trägt und in der Folge durch gigantische Giftgewässer landwirtschaftlich unbrauchbar wurde, kann schlicht und ergreifend nicht mehr dem ersten, vierten, fünften oder siebten Millenniumsziel dienen. Allenfalls bei dem niemals abgeschlossenen Projekt der Aufklärung kann Technik ein wenig helfen […]"*[8]

Panoptikum reloaded

Ganz konträr zur Erwartungshaltung beim Thema *Aufklärung* gehe ich hier nicht auf Kant, Kaffeehäuser oder Kontroversen der Öffentlichkeit ein, sondern auf Jeremy Bentham. In seinem Entwurf eines Kontrollhauses, Panopticon genannt, zeigt sich sein aufklärerisches Spiel mit dem Spannungsfeld geheim/öffentlich, opak/transparent, security/safety.



Panopticon-Skizze von Jeremy Bentham (1791)

Obwohl das am Anfang eigentlich nicht ganz ernst gemeint war, werde ich doch drei, vier Worte aus meiner Dissertation zitieren (und hoffen, dass das nicht gegen die Promotionsordnung verstößt, immerhin ist die Dissertation noch nicht verteidigt):

In seinen Briefwechseln behandelt der Aufklärer Bentham einen zentralen Punkt der politischen Philosophie: quis custodiet ipsos custodes? Es greift zu kurz, das Panoptikum nur auf den Entwurf eines Gefängnisses zu reduzieren. Doch selbst wenn wir bei diesem einen Gebäudekomplex bleiben, so greift es auch hier zu kurz, nur die Kontrolle der Gefangenen zu betrachten. Nicht nur zu Benthams Zeiten waren die Gefangenen leider allzu oft der Willkür der Wärter oder Gefängnisbetreiber ausgesetzt. Wenn Bentham also fragt, wer denn die Wächter bewacht, so spielt er damit nicht auf ihre Unfähigkeit oder Unlust an, sondern auf den Machtmissbrauch:

(Zitat Bentham): „Die Kontrolle der Macht durch die Untergebenen wird gehörig sein und um nichts weniger straff die Kandare, an welche die Kriminalität genommen wird. Den Unschuldigen wird das ein Schild sein, den Schuldigen eine Geißel."

Die Ausführungen über die Kontrollen der Kontrolleure nehmen einen weit größeren Platz ein als die über die Gefangenenüberwachung. Er spielt in Gedanken Gefängnisinspektionen durch, einmal in klassischen Haftanstalten und einmal in seinem Panoptikum. Im ersteren Fall könne ein Inspekteur unmöglich die Situation aller Gefangenen erfassen, das erlaubten weder Zeit noch Sicherheit, also könne nur eine Stichprobe genauer untersucht werden. Diese Momentaufnahmen liefern kein repräsentatives Bild, selbst unangekündigte Kontrollen helfen da nicht weiter:

(Zitat Bentham): „So wie dieser Plan [des Gefängnisses] die Unannehmlichkeiten für die Aufsichtsbeamten senkt, so erhöht er kaum weniger auch die Effizienz ihrer Arbeit. Mag der Besuch des Aufsichtsbeamten auch vollkommen ohne vorherige Ankündigung erfolgen, mag er auch noch so flink vorgehen, in allen anderen Fällen wird doch immer genug Zeit bleiben, die wahre Lage der Dinge zu verschleiern. Nur eine nach der anderen dieser neunhundert Zellen kann er besuchen, während in der Zwischenzeit andere, die sich womöglich in einem üblen Zustand befinden, rasch zurechtgemacht werden; und auch die Häftlinge können eingeschüchtert und genau instruiert werden, wie sie ihm zu begegnen haben."

In einer weiteren Iteration der Wächter der Wächter der Wächter usw. sollen die Türen der Einrichtung dann (Zitat Bentham): „der Gesamtheit der Schaulustigen, diesem großen offenen Gremium des Gerichtshofs der Welt" offen stehen.

Die Öffentlichkeit als Kontrollinstanz gegen Machtmissbrauch, fließendes Trinkwasser und sanitäre Einrichtungen für Gefangene, keine körperliche oder seelische Gewalt nirgends – Bentham liest sich nicht als der Vordenker des Orwell'schen Großen Bruders*. Jeremy Benthams Panoptikum war ein Projekt der Aufklärung, das wird besonders deutlich, wenn er sein Prinzip auf Krankenhäuser und Schulen anwendet. Es wurde jedoch fälschlicherweise als architektonisch-technisches Projekt verstanden, wie Christian Welzbacher im Nachwort*

(zu seiner deutschen Übersetzung) zurecht bemerkt, und eben nicht als politisch-philosophisch-soziales Aufklärungsprojekt.

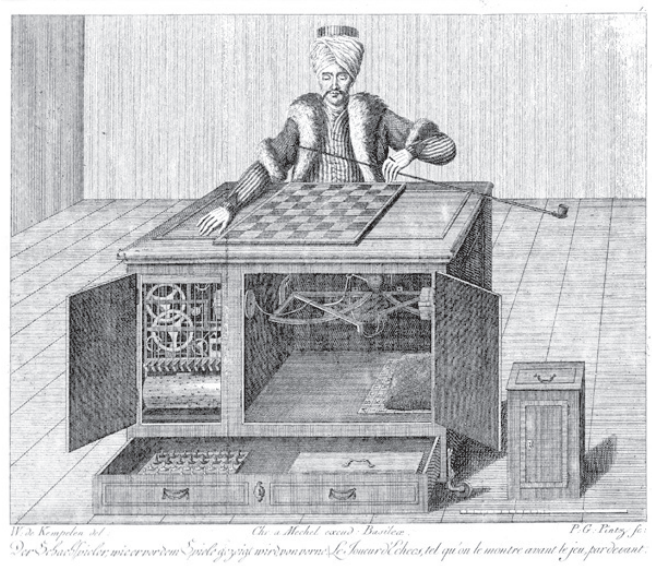
Die Verletzung des Geheimnisses als Schild oder als Geißel, dieses Motiv werden wir auf der Tagung sicher ebenfalls in mehreren Vorträgen behandeln. Amnesty nutzt die Brief-Öffentlichkeit als Schild, Edward Snowden floh in die publizistische Öffentlichkeit und verbarg Staatsgeheimnisse mit Hilfe von öffentlichen Kryptoschlüsseln.

Als ich Glenn Greenwalds Buch *No place to hide* in der Hand hielt, verstand ich den Titel als Verletzung der informationellen Selbstbestimmung, als Angriff auf die Privatheit. Doch nach der Lektüre wusste ich, dass es eine Drohung war, die Greenwald gegen die Geheimdienste aller Länder richtete, ganz im Duktus des letzten Satzes von Neo im Film *Matrix*.

Der Öffentlichkeit als großes Gremium der Gerechtigkeit im Politischen entspricht die Fachöffentlichkeit als kleines Gremium der Tatsachenprüfung, beides sind jedoch Kontrollinstanzen.

Schachspieler, Schach-„Spieler"

Vaucanson setzte die Transparenz in seinem technischen System zu didaktischen Zwecken ein, beschriebene Prinzipien sollten nicht nur gelesen, sondern nachvollzogen werden können. Offenheit bei technischen Systemen dient jedoch nicht zuletzt der Kontrolle des vermeintlichen Wissens über die Funktionsweise. Der französische Magier Jean Eugène Robert-Houdin sollte knapp einhundert Jahre später die Vaucanson'sche Ente reparieren und fand dabei heraus, dass der Kot in einem versteckten Beutel hinter dem Magen deponiert wurde. Die Ente war getürkt.



Kupferstich aus dem Buch: Karl Gottlieb von Windisch, Briefe über den Schachspieler des Hrn. von Kempelen, 1783

Der Ausdruck *getürkt* geht, mit dem in der Etymologie notorischen *vielleicht*, auf den so genannten Schachtürken Wolfgang von Kempelens zurück. Der österreichisch-ungarische Hofbeamte stellte 1769 der europäischen Öffentlichkeit einen mechanischen Schachspieler vor, der in türkischer Tracht gekleidet an einem Schachmöbel seine Gegner besiegte. Kempelen löste dabei die mechanischen Probleme des Schachspiels, also die Bewegung einer Hand zum Führen der Figur oder das dreifache Kopfnicken, das Schach ansagen sollte – aber eben nicht die kognitive Dimension. Um einen Menschen beim Schachspiel zu besiegen, musste damals noch ein Mensch mit von der Partie sein.

Wolfgang von Kempelen öffnete Interessierten gern die Türen des Schranks, zeigte die Zahnräder, Seilzüge, Rollen, Gelenkstangen und dergleichen mehr, die Figur jedoch konnte nur Schach spielen, wenn die Türen geschlossen waren. Vielen Zeitgenossen, die etwas intensiver nachdachten, war wahrscheinlich klar, dass sich ein Mensch im Möbel befand und die Zügel hielt, doch sie konnten es nicht nachprüfen. Denn dafür hätten sie die Schranktüren öffnen müssen, woran sie aber durch Kempelen mit zahlreichen Ausreden gehindert wurden.

Übrigens können wir auch bei zeitgenössischen Schachrobotern nicht sagen, ob sie wirklich „Schach spielen". Hat Deep Blue wirklich ein Verständnis für Schach? Der Neuseeländer Nigel Richards gewann letztes Jahr einen französischen Scrabble-Wettbewerb, ohne Französisch sprechen zu können. Dank seines fotografischen Gedächtnisses „lernte er einfach alle Wörter mit zwei bis zehn Buchstaben auswendig, die das offizielle französische Scrabble-Wörterbuch kennt".[9] Für seine Danksagung benötigte er einen Dolmetscher. Kann er nun die französische Version von *Scrabble spielen*?

Transparenz sorgt nicht automatisch für Verständnis. Abgesehen davon, dass Technikerinnen und Techniker das Wort Transparenz in einem Sinn konträr der Alltagsbedeutung verwenden, was auch wieder einen Hinweis auf Verständnisprobleme gibt, lieferte der Informatik-Pionier Joseph Weizenbaum die eindrucksvollste Demonstration.

Weizenbaum wollte mit wenigen hundert Zeilen Code die Parodie einer Unterhaltung programmieren und so auf die Unzulänglichkeiten der Technik in Bezug auf Verstand und Vernunft hinweisen. Die Maschine, der Computer, die Software versteht ja nichts, auch ist er ja niemand, der von seiner Vernunft Gebrauch machen kann. Er nannte das Programm ELIZA …

… und in diesem Kreis muss ich ja nicht weiter ausführen, welches Entsetzen Weizenbaum befiel, als er die Reaktion der Leute sah, die mit dem Computerprogramm interagierten. (Eigentlich war dies nur die experimentelle Bestätigung des Tests von Alan Turing, der Systeme mit so genannter *Künstlicher Intelligenz* an ihrer Akzeptanz durch die Nutzerinnen und Nutzer maß.)

Wenn Menschen also schon Bildschirmausgaben einem intelligenten Wesen zuschrieben, obwohl sie doch den Quelltext gesehen hatten, wie sollten diese Menschen reagieren, wenn es keinen Quelltext mehr in diesem strengen Sinne gäbe?

Ausrechnen statt Entscheiden

Mit Hilfe von biometrischen Systemen lässt sich sehr gut zeigen, dass die von Frieder Nake ausgerufene *Algorithmische Revolution* wohl doch eher eine heuristische ist. Korrelationen ersetzen

Kausalitäten. Bereits Alan Turing kritisierte die Entwicklung der elektronischen Computer, die immer mehr Operationen in ihrem Inneren durchführten, ohne dass vorher die zugrunde liegenden Probleme von Menschen *by thought* gelöst wurden.

Joseph Weizenbaum greift in dem Dokumentarfilm *Plug & Pray* von Jens Schanze diesen Gedanken auf: Früher musste ein berechenbares Problem verstanden werden, zutiefst und prinzipiell verstanden werden, bevor man es in den Computer eingeben konnte. Heute (also vor zehn Jahren) scheine es sich gerade umgekehrt zu verhalten: Wenn man ein Problem nicht verstanden hat, gibt man es in den Computer ein, in der Hoffnung, der Computer löse es, und in der Hoffnung, man verstehe die ausgegebene Lösung.

Da ich gerade in Elternzeit bin, kann ich mit eigenen Augen beobachten, wie einjährige Kinder ihre Umwelt begreifen und Sprache entwickeln. Das Foto eines Dackels, die Bleistiftzeichnung eines Bernhardiners, die Pixelgrafik eines Schäferhundes und nicht zuletzt der echte Pudel der Nachbarin – alles ist *wau wau*.

Wohlgemerkt auch bei Fotos, Zeichnungen und Begegnungen, die das Kind zum ersten Mal sieht. Ob da eine Platonische Hunde-Idee im Kopf sitzt oder die ganze Wittgenstein'sche Hundefamilie, ich vermag es nicht zu sagen und wage zu behaupten, dass es niemand sagen kann. Das hindert Google und andere aber nicht daran, ihre *neural networks* Bildunterschrift ausgeben zu lassen. (Das 2014 vorgestellte System von Google ist seit zwei Monaten Open Source, Interessierte können sich unter TensorFlow auf GitHub die Software ansehen und weiterentwickeln.)

Es funktioniert ja in 93 Prozent aller Fälle. Es sei denn, man erwischt die sieben Prozent, mit denen es zu 100 Prozent nicht klappt, dann ergeben sich die zum Teil amüsanten, zum Teil tödlichen Fehler. Hier auf der Folie sehen wir eine Abbildung aus einer Studie der Carnegie Mellon University mit dem Titel *Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition*. Dort wird beschrieben, wie man handelsübliche Gesichtserkennungssysteme überwindet, indem man übertriebene Merkmale auf Brillengestelle druckt. So verbirgt man nicht nur seine eigene Identität, man kann sogar die Identitäten wechseln. (Valentin Groebners *Schein der Person* blickte mich bei der Vorbereitung ganz böse an, weil ich den Begriff *Identität* tippte, wo es eigentlich um eine Fremd-Zuschreibung geht. Aber auch darüber werden wir im Laufe der Tagung sicher sprechen.)

Schon das Wort *Gesichtserkennungssystem* führt in die Irre, das System „erkennt" ja nichts, es rechnet aus. Was bei Leibniz eher böse Satire war, scheint nun einzutreten: Wir müssen uns beispielsweise in moralischen Konfliktsituationen nicht mehr für die eine oder andere Handlung entscheiden, wir rechnen einfach aus, was die richtige Handlung ist. Nein, noch besser: Wir lassen ausrechnen, was die richtige Entscheidung ist.

Komplexitätsreduktion

Es ist verführerisch, in diesem Rahmen über die verborgene Technik als etwas Schlechtes zu sprechen, die geheimen Welten großer Konzerne und Staatsorgane als demokratiefeindlich anzuprangern, zumal alle hier Versammelten ein gesundes Maß an Technikkritik mitbringen.

Im Gegensatz zur FIfF-Jahres-Konferenz 2014, die angesichts des offenkundigen Grundrechtsbruchs durch Geheimdienste ein Ausrufezeichen setzen wollte, möchten wir diesmal große Fragezeichen hinter Themen setzen, die unsere heutige, von Technik durchdrungene Welt uns auf dem gebürsteten Alutablett serviert.

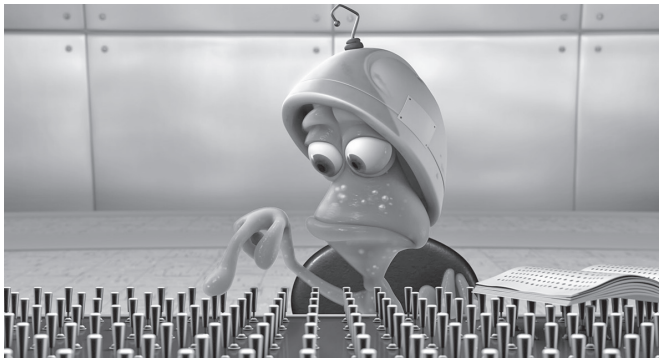
Die Motive, Technik zu verbergen – oder zu offenbaren – können ganz unterschiedlicher Natur sein. Eine Leitfrage der Kon-

Examples of successful impersonation and dodging attacks. Fig. (a) shows SA (top) and SB (bottom) dodging against DNNB. Fig. (b)–(d) show impersonations. Impersonators carrying out the attack are shown in the top row and corresponding impersonation targets in the bottom row. Fig. (b) shows SA impersonating Milla Jovovich (by Georges Biard / CC BY-SA / cropped from https://goo.gl/GlsWIC); (c) SB impersonating SC ; and (d) SC impersonating Carson Daly (by Anthony Quintano / CC BY / cropped from https://goo.gl/VfnDct).

ferenz ist daher auch „Wieviel Transparenz ist nötig und wieviel Transparenz ist (ohne Funktionseinbußen) möglich?“

Eine diskursanalytische Herangehensweise könnte darin bestehen, nicht nur die Technik, sondern auch die Akteure in entsprechenden Machtpositionen sowie die zugrunde liegenden Normen zu betrachten. Manche Akteure verstecken und verschleiern technische Funktionsweisen ihrer Systeme bewusst, etwa im Bereich *security by obscurity*. Andere legen sie offen, wie das Beispiel Open Source oder Benthams Panopticon zeigt, also *safety by publicity*. Wieder andere sind durch rechtliche Anforderungen (entstanden aufgrund historischer Kämpfe) zu einem gewisses Maß an Transparenz verpflichtet, der Staat etwa.

Und nicht zuletzt dient das Verbergen komplexer Vorgänge auch der besseren Bedienung informationstechnischer Systeme durch Nutzerinnen und Nutzer. Hier auf der Folie sehen wir ein Standbild aus dem Pixar-Kurzfilm *Lifted* von 2006, der kleine Außerirdische Stu muss seine Abschlussprüfung in *Alien Abduction* bestehen, woran er jedoch scheitert, weil er die aus tausenden identischen Schaltern bestehende Konsole nicht bedienen kann. Man beachte auch das aufgeschlagene Handbuch, das nur aus endlosen Reihen von Hebelpositionsabbildungen besteht.



Standbild aus dem Pixar-Kurzfilm Lifted von 2006

Im Ankündigungstext habe ich den Kodak-Werbespruch von George Eastman aus dem Jahre 1888, *You Press the Button, We Do the Rest*, als Vorlage genutzt, um auf die firmenverschuldete technische Unmündigkeit hinzuweisen. Man könnte das auch ins Gegenteil wenden: Nun kann endlich jeder fotografieren, aus Lust und Laune. Auch dem doppelten Boden in den von IBM gestalteten Serverräumen haftet ein Kubrick'sches Unbehagen an: Unter der leuchtend-weißen Fassade ist eine Unterwelt voller Kabel, Käfer und Co.

Wer kleine Kinder oder andere erratisch handelnde Wesen in der Nähe von Kabeln beobachtet, findet das Verbergen von kritischer Infrastruktur vor unbefugtem Zugriff vielleicht ganz gut – natürlich vorausgesetzt, dass es noch Wartungsklappen gibt, die sich von uns Technikerinnen und Technikern gut öffnen lassen und nicht verklebt und verlötet sind.

Flammarion 2.0, 3.0, 4.0

In diesem Sinne freut es mich, dass wir nun gemeinsam durch die von den Organisatoren dieser Konferenz aufgezeigte offene Schweißnaht blicken, an der die idealisierte Welt der Technik nicht ganz mit dem harten Boden der Realität verbunden ist.

Vielen Dank für Eure Aufmerksamkeit.

Anmerkungen

1 *https://www.youtube.com/watch?v=ghbj6iNPfCU#t=1m25s*

2 *Bereits 2007 beschäftigte sich die Jahrestagung des Fachbereichs Informatik und Gesellschaft der GI mit dem Thema Kontrolle durch Transparenz – Transparenz durch Kontrolle, das Internet-Archiv hat glücklicherweise noch den Ankündigungstext: „In bislang unbekanntem Ausmaß werden Nutzerinnen und Nutzer der weltweiten Datennetze für Dritte transparent. Sie hinterlassen Datenspuren, um die komfortablen Web-Services der Anbieter von Dienstleistungen und Waren, von öffentlichen Stellen und Behörden wahrnehmen und sich unbeschwert im Internet bewegen zu können. Egal, ob dies in der ursprünglichen Absicht der Sammler von Daten liegt oder nicht, es lässt sich sehr viel herausbekommen über die Netznutzer. Privatheit und das Recht auf informationelle Selbstbestimmung spielen so gut wie keine Rolle mehr. Dritte gewinnen Kontrolle durch die informatische Transparenz der Transaktionen.“ https://web.archive.org/web/20070811061034/http://www.gi-ev.de/gliederungen/fachbereiche/informatik-und-gesellschaft-iug/tagung-transparenz//*

3 *https://books.google.de/books?id=FE_qNQaKYiEC, S. 19ff.*

4 *»[D]ie Vaucansonischen Automaten fanden wir durchaus paralysiert. In einem alten Gartenhause saß der Flötenspieler in sehr unscheinbaren Kleidern; aber er flötete nicht mehr, und [Gottfried Christoph] Beireis zeigte die ursprüngliche Walze vor, deren erste einfache Stückchen ihm nicht genügt hatten. Dagegen ließ er eine zweite Walze sehen, die er von jahrelang im Hause unterhaltenen Orgelkünstlern unternehmen lassen, welche aber, da jene zu früh geschieden, nicht vollendet noch an die Stelle gesetzt werden können, weshalb denn der Flötenspieler gleich anfangs verstummte. Die Ente, unbefiedert, stand als Gerippe da, fraß den Haber noch ganz munter, verdaute jedoch nicht mehr: an allem dem ward er aber keineswegs irre, sondern sprach von diesen veralteten halbzerstörten Dingen mit solchem Behagen und so wichtigem Ausdruck, als wenn seit jener Zeit die höhere Mechanik nichts*

Stefan Ullrich

Stefan Ullrich ist Kritischer Informatiker und seit 2011 Sprecher der Fachgruppe *Informatik und Ethik* der Gesellschaft für Informatik (GI). Er forscht zu „neuen Öffentlichkeiten“.

frisches Bedeutenderes hervorgebracht hätte.« Johann Wolfgang von Goethe: Autobiographische Schriften II, 1805, S. 477. https://books.google.de/books?id=uNW5pruwuKEC&pg=PA477&lpg=PA477

5 *« Pour faire connaître que les mouvemens de ces aîles ne ressemblent point à ceux qu'on voit dans les grands chefs-d'œuvres du Coq de l'Horloge de Lyon & de Strasbourg, toute la mécanique du Canard artificiel sera vûë à découvert, mon dessein étant plûtôt de démontrer, que de montrer simplement une machine. Peut être que quelques Dames, ou des gens qui n'aiment que l'extérieur des animaux, auraient mieux aimé le voir tout couvert; mais outre que cela m'a été demandé, je suis bien aise qu'on ne prenne pas le change, & qu'on voye tout l'ouvrage intérieur. » Jacques de Vaucanson, Le mécanisme du fluteur automate: presenté a Messieurs de l'Académie royale francaise, 1738.*

6 *Stefan Ullrich: Pauperismus 4.0. Industriell hergestellte Armut. Beitrag im Blog Faire Computer, http://blog.faire-computer.de/pauperismus-4-0/.*

7 *ebenda.*

8 *ebenda.*

9 *http://www.faz.net/aktuell/gesellschaft/menschen/franzoesischer-scrabble-meister-kann-kein-franzoesisch-13715114.html*

FIfF-Konferenz 2016

CYBER! Der Staat als Krimineller

Zusammenfassung des Vortrags von Erich Möchel

Nach Stuxnet, Duqu, oder Zeus und Black Energy, nach dem Re-Engineering des Bundestrojaners und den Enthüllungen Edward Snowdens über den massiven Einsatz hochentwickelter Schadsoftware durch NSA und GCHQ ist klar, dass hier ein neuartiger Rüstungswettlauf außer Kontrolle geraten ist.

Erich Möchel hat seit 1995 lebhaft mitverfolgt, wie Staaten sich selbst trotz ihrer eigenen Verbote das Recht einzuräumen begannen, Schadsoftware einzusetzen. In seinem geschichtlichen Abriss über die Entwicklung wird das erschreckende Ausmaß deutlich: Staaten der westlichen Demokratien hätte auch er nicht für so skrupellos gehalten, zu allen verfügbaren Mitteln zu greifen.

Etymologische Bemerkungen zu dem Begriff *Cyber*

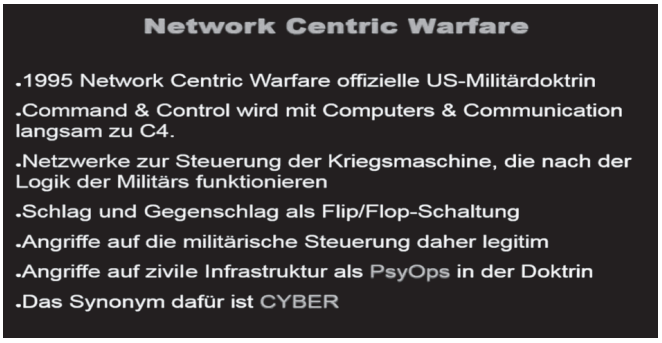
Cyber ist ein Begriff, der sehr viel unter sich subsumiert. Er wurde ursprünglich vom Staat beansprucht und beschrieb immer eine staatliche Aktion. Die ältesten Anwendungen des Wortes standen für Lenkung, Steuerung – für den Staat. Bei Homer ist der κυβέρνητης der Schiffssteuermann und auch in dem Wort Κυβέρνησις, wie die Regierung im alten Athen hieß, ist das Wort *Cyber* versteckt. Im Mittelalter ist daraus dann der Gouverneur – ein Militärbefehlshaber – geworden. 1948 prägte Norbert Wiener den Begriff *Cybernetics* für Steuerungs- und Regelungskunde, Maschinen, Organismen und soziale Organisationen. Der Begriff wurde daraufhin sehr breit angewendet. Im Zuge des Behavioristischen Modells der Psychologie, das damals langsam entstand, dachte man, man könnte alles lenken und gesellschaftliche Vorgänge nach Belieben manipulieren. Die Sowjetunion ist daran zugrunde gegangen, aber diese Art des Denkens war im Westen fast noch verbreiteter.

Der Begriff Kybernetik tauchte dann überall in der Wissenschaft auf: Claude Shannons Informationstheorie, bei Paul Watzlawick, bei Maturana/Varela bis zur Systemtheorie Niklas Luhmanns.

In den 60er-Jahren gab es sogar eine Kybernetische Pädagogik. Man nahm den Begriff wörtlich und wendete ihn auf alle Bereiche der Gesellschaft an. Einzug in die Gesellschaft selbst erhielt der Begriff in den 80er-Jahren, als die Alternativen zum ersten Mal nach dem Begriff griffen und die *Cyberpunk Fiction* schufen. Zu Ehren kam der Begriff *Cyber* schließlich in der *Cybercrime Convention* im Europarat (COE), als der Europarat, der sich sonst mit Menschenrechten beschäftigt, im Bereich *Cyber* Überwachungsgesetze beschloss, da „man ja alle möglichen Menschen vor dem Netz schützen muss".

Network Centric Warfare

Seit 1995 ist *Network Centric Warfare* die offizielle US-Militärdoktrin. Dies ist kein Geheimwissen und nicht unsichtbar, sondern wurde als Konzept des vernetzten Krieges festgeschrieben. *Command & Control Center* – die Gefechtsfeldzentralen – wurden erweitert um *Computers and Communication* und wurden langsam zu C4 (*Command, Control, Computer and Communication*). Die Kontrolle der Kommunikation wurde also zur üblichen Gefechtszentrale (das sind im Wesentlichen die Systeme, die jede Armee der Welt verwendet) einfach hinzugefügt. Die so entstandenen Netzwerke funktionieren nach der Logik der Militärs. Diese Logik ist unerbittlich: Schlag und Gegenschlag. In dem Moment, in dem man das Gebiet der Militärlogik betritt, gelten all unsere Regeln nicht mehr. Es gilt auf diesem Gebiet nur noch das furchtbare Gesetz des Krieges. Schlag und Gegenschlag wurden eingeplant wie eine Flip-Flop-Schaltung in der Elektronik. Wie zwei Transistoren, die sich gegenseitig ein- und ausschalten. Das Prinzip selbst galt aber beim Militär schon länger; selbst Angriffe auf die militärische Steuerung sind daher eine ganz legitime Handlung. Es war nur die Frage, zu welchem Zeitpunkt man den *Cyber*-Angriff starten kann und vor allem,



wie er von der Gegenseite eingeschätzt wird und wie diese darauf reagiert.

Angriffe auf die zivile Infrastruktur waren schon vorher als sogenannte PsyOps – Psychologische Operationen – Teil der Doktrin der Militärs. Derartige militärische Aktionen waren eine dem Schießkrieg vorgelagerte Art des Handelns und der gegenseitigen Schlagabtausche, zu denen z. B. auch Propaganda und somit Kommunikationsmedien und Breitenmedien gehören. Als weitere Stufe folgen dann aber auch direkte Angriffe auf Websites und Informationssysteme. Im Irak konnte man das 2003, kurz vor Einmarsch der Amerikaner, täglich verfolgen: Von einem Tag auf den anderen wurden plötzlich sämtliche irakischen Regierungswebsites gehackt. Die Amerikaner haben diese Angriffe eher unglaubwürdig, aber umso heftiger dementiert. Die Websites waren zwar miserabel gehostet, es konnte aber nicht sein, dass es sich bei dieser Gleichzeitigkeit um eine Vielzahl von Einzelaktionen handelte. Nachdem all diese Websites lahmgelegt waren, wurden die Radio- und Fernsehausstrahlungen im Irak angegriffen. Auch in diesem Bereich ist also *Cyber* angesiedelt; all diese Aktionen passieren im Vorfeld des Schießkrieges und inwiefern das vom tatsächlichen Krieg abzugrenzen ist, ist nicht festgelegt. *Cyber* dient als Synonym für all diese unsinnigen militärischen Aktionen. Er steht für alles: für Angriffe mit Mitteln der Kommunikation auf die Kommunikation, Angriffe, die keine herkömmlichen Waffen beinhalten und die nur sehr schwer zuzuordnen sind. In dieser ersten Phase des Angriffs bleibt der Angreifer unsichtbar – ein Musterbeispiel für ein *invisible system*, bis zu dem Punkt, an dem der Angreifer sich im Netzwerk des Gegners befindet und dort auffällt.

Die sogenannten Cryptowars

Ein hierzu passendes *Invisible Office* findet man in Wiens erstem Bezirk in der Mahlerstraße 14. Dieses *Wassenaar Office*, das seinen Namen vom sogenannten *Wassenaar Arrangement* bekam, beschäftigt sich mit *Cyber*, Schadsoftware und Crypto. Das Büro ist eigentlich niemandem bekannt, aber wichtig, denn es verwaltet die Nachfolge der CoCom-Listen, jenes Verfahren, mit dem sich die westlichen Staaten verpflichteten, keine Hochtechnologien an die Sowjetunion zu liefern, also Embargolisten. Das *Wassenaar Office* hat ebendies fortgeführt: Sie führen ordentliche Kataloge von Waffentechnologie, und was als Waffe verstanden wird, ist dort definiert. Darunter zählen z. B. Funkscanner, die mehrere Frequenzen gleichzeitig scannen, Geräte mit Technologien, die jenseits der 31 GHz operieren – im Prinzip die gesamte Palette an Dual-Use Goods – die vielen Güter also, die man sowohl in der Zivilgesellschaft als auch im Krieg benutzen kann. Der Konflikt der 90er-Jahre um das freie Bereitstellen von Verschlüsselungsprogrammen ist nun unter dem Begriff *Cryptowars* bekannt. Journalist.innen und die technikinteressierte Zivilgesellschaft haben das nie so genannt, und es vergingen viele Jahre, bis dieser Begriff überhaupt als Militärbegriff bekannt wurde.

Die österreichische Bundesregierung hatte sich noch nicht festgelegt, wie sie zu Kryptografie stand, wusste das Thema eigentlich auch noch gar nicht richtig einzuschätzen, konnte aber nicht wirklich etwas dagegen einwenden, da es auch in Österreich etwa ein Bankgeheimnis gab. An dieser Stelle nur ein ganz kurzer Abriss über die Eckdaten: 1976 begann die ideelle akademische Befreiung von Kryptografie, denn bis dahin hatten nur die Militärs Zugang zu den Fachbüchern. Whitfield Diffie und Martin Hellman befreiten Kryptosysteme 1976 aus Militärhaft, indem sie Kryptografie auf der Konzeptebene re-engineerten. 1991 stellte Phil Zimmermann PGP als Commandline-Version ins Netz und erhielt daraufhin Besuch vom FBI, wobei zu sagen ist, dass in der frühen Zeit des Netzes viele erst einmal „gemacht" haben, ob legal oder illegal war damals noch keine relevante Frage. Der Leak der OECD-Kryptobestimmungen durch den österreichischen Datenschutzverein *Quintessenz* schlug im Hintergrund diplomatische Wellen. 1994 führte Netscape SSL 1.0 als Kryptografiestandard ein, was für Banken von höchstem Interesse war, da Menschen nun selbst ihre Konten führen, Arbeitsplätze abgebaut und Filialen geschlossen werden konnten – was dann auch genauso geschah.

1995 wurde Kryptografie auf Betreiben der USA im *Wassenaar Arrangement* zu Munition. Jemand, der Verschlüsselungsanwendungen geschrieben hatte oder Software und Verschlüsselungshardware baute, durfte diese nicht ohne Genehmigung der eigenen Regierung exportieren. Wenn das Zielland nicht als Empfänger erwünscht war, wurde diese Genehmigung nicht erteilt. Kryptografie, welche ihrem Wesen nach rein defensiv eingesetzt wird, wurde damals als offensive Waffe eingestuft. Aus diesem Grund konnten Netscape und Microsoft keine sichere Verschlüsselung einbauen, weil sie nicht garantieren konnten, dass ihre Software nur in genehmigten Ländern heruntergeladen wird.

Die Banken hatten jedoch nach wie vor ein erhebliches Interesse an sicherer Kryptografie, und so entstand sehr plötzlich eine ungewöhnliche Allianz mit den zivilen Technik-Communities. „Banken, die E-Commerce betreiben wollten, taten sich zusammen mit solchen Narren wie uns", beschreibt Möchel. In einer weltweiten Allianz im Rahmen der *Global Liberty Campaign* hatten sich auch die American Civil Liberties Union, die Electronic Frontier Foundation und viele kleine europäische Gruppen, die sich gerade erst gebildet hatten, zusammengefunden. Zu dieser Zeit wurde heftig über die Zukunft der Kryptografie diskutiert. Die sogenannten *Spooks* wussten längst, dass sie dieses Match verlieren würden und die Blockade gegen Kryptografie nicht aufrechterhalten konnten, denn die gesamte Zivilgesellschaft war dafür. So kam es schließlich zu dem folgenreichen Beschluss, rund um die Welt ab sofort Kryptografie einzuführen. Damit konnte die Kommunikation nun nicht mehr so einfach auf der Strecke abgefangen werden, sodass diejenigen, die Kommunikation abhören wollten, sich neue Wege suchen mussten – vor dem Wirken der Verschlüsselungsmechanismen – und sich somit der Integrität der Hard- und Software des Kommunikationsverursachers zuwandten.

Plattenputzer, Makroviren, Würmer

Es folgte eine Welle von Schadsoftware, und niemand wusste, wer eine so unglaubliche Menge an Personenjahren zu investieren bereit war, nur um einen Virus zu schreiben und zu verbreiten. Dass dahinter lauter *Kiddies* stecken sollten, erschien eher unglaubwürdig. Die Frage aber war, wer so etwas zu welchem Zweck, d. h. zu welchem Vorteil tun würde. Die Antwort blieb

aus, stattdessen gab es immer mehr Schadsoftware. Ende der 80er waren die meisten Prototypen von Malware bereits bekannt und ausprobiert. Ab 1995 breitete sich Malware rasant aus, insbesondere seit der massenhafteren Verwendung des World Wide Web. 1995 tauchte der erste Makrovirus für Windows Software auf. Alle computerisierten Büros waren plötzlich in Gefahr, was zu der Zeit schon beachtlich viele waren. 1998 gab es dann die erste Software der CIH-Familie, der böseste unter ihr der *Tschernobyl*-Virus, der seinem Namen alle Ehre machte. Auf infizierten Systemen löschte er komplett Festplatte und BIOS.

Während es zunächst vor allem Viren im klassischen Sinne der Medizin gab, also Programme, die echten Schaden verursachen, kamen bald auch die ersten Würmer auf – Software, die sich selbst auf eine Weise verbreiten konnte, die es bei Viren nicht gegeben hatte. Das österreichische Technikmagazin *Futurezone*, bei dem Möchel Redakteur war, berichtete zur Jahrtausendwende über viele solcher Programme, von denen ebenfalls völlig unklar war, wer die beteiligten Programmierer bezahlt hatte. Viele hatten sicherlich auf eigene Faust gehandelt oder sich kaufen lassen. Doch für dieses Geschäftsmodell erschienen die Wellen von Schadsoftware zu massiv. Die Würmer *Melissa* und *ILOVEYOU* hatten keine nennenswert böse Payload, aber verbreiteten sich so rasch, dass sie die Internet-Exchanges lahmlegten. Sie funktionierten zum Teil nach dem Schema „Nimm alle Outlook-Adressen des angegriffenen Rechners und versende dich selbst". Das Phänomen artete dermaßen aus, dass um das Jahr 2000 teilweise im Wochenrhythmus die Internetknoten für Stunden ausfielen. Es ist sehr unwahrscheinlich, dass diese Angriffe nicht koordiniert geführt wurden; plausibler ist die Erklärung, dass die Angriffe einer bestimmten militärischen Regie folgten. Abwechselnd sind die Würmer um verschiedene Internetknoten herum zuerst aufgetaucht und erst später (abgeschwächt) anderswo, etwa zuerst in Hongkong, und wenn sie später am Tag nach Europa kamen oder noch später in die USA, dann waren sie bereits verhältnismäßig harmlos. Andere Angriffe sind wiederum zuerst in den USA an der Ostküste aufgeschlagen. Deutlich wird daran, dass dabei offenbar vor allem zwei Parteien im Spiel waren. Wären diese Beobachtungen damals öffentlich gemacht worden, wären sie als paranoid weggeschoben worden, zurückgeführt hat man die Angriffe auf „irgendwelche Gangster", deren Intentionen wir eben nicht kennen. Erklären konnte man diese offensichtlichen Zusammenhänge der einzelnen Ereignisse mit dieser Theorie jedoch nicht.

Zeitgleich ist das *ECHELON*-System aufgeflogen, zu dessen Aufklärung eine Untersuchungskommission im EU-Parlament eingesetzt wurde. Möchel selbst war geladen worden, um im Gremium auszusagen. Auch die Cybercrime-Konvention fand damals statt, weil diejenigen, die *Cyber* gemacht haben, inzwischen eingesehen hatten, dass ein Regelwerk geschaffen werden musste, um nicht in einem Chaos zu enden, in dem keiner mehr weiß, was der andere tut. Daraufhin wurden die Restriktionen für Kryptografie aus dem *Wassenaar Arrangement* herausgenommen; Banken, E-Commerce und die Internetwirtschaft forderten eine zumindest so sichere Verschlüsselung, wie sie die USA hatten, mindestens Triple DES (3DES) mit 128 Bit, was für die damalige Zeit schon recht akzeptabel war. Die NSA hatte ursprünglich auf einer 40-Bit-Verschlüsselung beharrt, die jedoch mit der entsprechenden Hardware schon damals in einer Tausendstelsekunde zu knacken war. Es wurden der Wirtschaft und den Banken schließlich 56 Bit zugestanden, während auf den Heimmaschinen der Community bereits eine 128-Bit-Verschlüsselung lief und die nötige Software im Internet zum Download verfügbar war. Die Beschränkungen waren also eher lächerlich und die gesellschaftlichen Ansprüche und wirtschaftlichen Begehrlichkeiten nach Kryptografie wiederum so hoch, dass die Militärs auf verlorenem Posten standen.

Das goldene Zeitalter nach 2000

Nach 2000 explodierte das Spam-Aufkommen, woran in erster Linie die Würmer beteiligt waren. Inzwischen war eine erste Infrastruktur mit Gegenmaßnahmen entstanden: In Österreich

Erich Möchel

wurden 1999 die ersten Gesetze gegen unerlaubte Massenmails verabschiedet; in ganz Europa gab es ähnliche Bestrebungen. Beliebige Mailadressen zu sammeln und diese auf Spam-Listen zu setzen, so wie es Firmen in den 90er-Jahren regelmäßig taten, wurde ab sofort untersagt. In verschiedensten Staaten begann sich so jedoch eine Schwarzmarktindustrie zu entwickeln, und man musste sich wiederum wundern, warum dagegen nicht eingegriffen wurde. Sowohl die russischen als auch die US-amerikanischen Geheimdienste haben diese Strukturen nicht nur geduldet, statt gegen sie vorzugehen, sondern sie auch selbst benutzt – innerhalb ihrer eigenen Logiken auch rechtmäßig.

2001 drang die NSA durch Exploits in verschiedenste Firewalls aller möglichen Netze ein – erst 2016 wurde diese Verantwortlichkeit im Übrigen durch die Shadow-Brokers-Leaks bekannt. Der *Dual Elliptic Curve Random Generator* der NSA (ein kryptografisch sicherer Zufallszahlengenerator) wurde NIST-Standard und fand als solcher Verbreitung im Mobilbereich. Schon kurz nach seiner Veröffentlichung 2007 stellte sich jedoch heraus, dass sein Pseudozufall doch leichter zu rekonstruieren war als gedacht und somit ein darauf basierendes Kryptografiesystem leicht zu brechen.

Ab 2005 bildete sich der Schwarzmarkt für Botnet-Schadsoftware als Infrastruktur für Spam, Betrug, Erpressung und andere Verbrechen. Diese zivilen Kriminalitätsstrukturen eignen sich jedoch auch als Nebelwerfer für Cyber-Aktivitäten der Militärs. Ein Schwarzmarkt für Zero-Day-Exploits (bis dato geheim gehaltene Sicherheitslücken) kam in Anfängen gegen 2006 auf. Mit ihnen kam für die Kriminalitätsverfolgung eine nötige Vorsicht ins

Spiel, denn die Verfolger mussten darauf aufpassen, dass sie bei ihren Ermittlungen nicht zufällig den Partner des eigenen Militärs erwischten und vor Gericht stellten. Z. B. wurde der Autor des *Melissa*-Wurms verhaftet und war davon vollkommen überrascht – es stellte sich heraus, dass das FBI einen eigenen Mitarbeiter verhaftet hatte, der zugleich im Auftrag anderer staatlicher Organisationen arbeitete.

Ein Sprung von den 2000ern zu Snowden nach 2010

2012 veröffentlichte die Nato eine neue Cyberwar-Doktrin, weil sich Angriffe nun immer stärker häuften. Es wurde öffentlich bekanntgegeben, dass im Ernstfall „zurückgecybert wird". Doch dies ist leichter gesagt als getan, denn um einen „Gegenschlag" auszuführen, muss erst identifiziert werden, wer der Verursacher ist. Die Verschleierung ist jedoch integraler Bestandteil einer Aktion, und es dauert lange, bis ein Angriff halbwegs genau zugeordnet werden kann. Die große Gefahr besteht also insbesondere auch darin, dass *Cyber* als eine Provokation einer dritten Seite zwei Mächte gegeneinander ausspielt und gegeneinander aufbringt.

2013 enttarnte die NSA öffentlich eine Einheit der chinesischen Armee, was zu einem offenen Schlagabtausch führte. Kurz darauf ereignete sich die Veröffentlichung der Snowden-Dokumente; eine der wichtigsten Folien darunter ist der Hinweis auf 50.000 bereitgehaltene Einnistungen in Großnetze von Providern und Staat. Andere weisen auf die Quantum-Projekte hin, welche eine Zwischenschaltung in Übertragungen zu z. B. Facebook ermöglichen. Auch werden Angriffe durch Zero-Day-Exploits etwa auf den Provider Belgacom dokumentiert.

Der Cyberwar eskalierte im Ukraine-Krieg 2014: Durch ihre Steuerungssysteme wurden die örtlichen Stromnetze angegriffen. Auch der NATO-Gipfel blieb nicht verschont: Seine organisatorischen Strukturen wurden angegriffen mit der Softwaresuite *Black Energy*, eine der gebräuchlichsten Steuersoftwares zum Spammen, die allerdings zu einem Überwachungstrojaner umgebaut worden war. Zum Ziel von Sabotage und Datenklau wird immer mehr auch die Privatindustrie, besonders *Sony*, die *OPM* (eine unabhängige US-Behörde zur Verwaltung öffentlich Angestellter) oder Kranken- und Pensionsversicherungen. Der Verkauf der Daten an Kriminelle dient schlicht der Schadensmaximierung. All dies waren die ersten Cyber-Auseinandersetzungen, die wir im Grunde live mitverfolgen konnten.

Das *Wassenaar Office* soll nun dafür sorgen, dass Schadprogramme aus der NATO nicht in falsche Hände geraten – es ist freilich aber schlicht und einfach festzustellen, dass jegliche Hände dafür falsch sind. Da das Wassenaar-Abkommen aber auch noch weitere Staaten einbezieht, wie z. B. Russland oder die Ukraine, schlägt sich zudem deren politischer Konflikt auf die Sitzungen nieder. Nach dem arabischen Frühling kam auf EU-Initiative die Kontrolle sogenannter Cyber-Waffen als neuer Punkt für das Abkommen hinzu, denn vor allem europäische Firmen liefern Überwachungssoftware an die Regime. Problematisch an der Arbeit des Office: Es gibt keine Öffentlichkeitsarbeit. Der Artikel über die Regulierungslisten 1998 in Telepolis von Möchel war der erste Bericht zum Thema überhaupt.

Schlussfolgerungen

Der Cyberwar ist kein herkömmlicher Krieg, sondern folgt anderen Regeln, die 6000 Jahre Militärgeschichte auf den Kopf stellen. Wo die Verteidiger bisher stets bei allen Strategien im Vorteil waren, ist es im Cyberbereich der Angreifer. Er wählt den Zeitpunkt, den Ort des Angriffes im Netz und die Angriffsweise. Allein schon durch die schiere Menge der Angriffsvektoren ergibt sich ein enormer Nachteil in der Verteidigung. Als Konsequenz ergeben sich mehr mögliche und schnell erreichbare Angriffsziele, je besser ein Land vernetzt ist und je dichter seine Infrastruktur ausgebaut ist. In weniger computerisierten und international vernetzen Ländern sind Cyber-Angriffe wesentlich weniger leicht durchzuführen. Für den Staat ist Angriff also billig und lässt sich sogar an halbstaatliche/kriminelle Gruppen auslagern; Verteidigung dagegen ist extrem teuer. Probleme ergeben sich aber durchaus auch innerstaatlich, wenn solche Gruppen wie in Russland z. B. ungeplant über ihren Auftrag hinaus auf Fang bei russischen Banken gehen. Sicherheit, Crypto und Cyber gehören somit zusammen als Verteidigungs- und Angriffstechnologien.

Wie sich unsere Cyber-Zukunft weiterentwickeln wird, das steht mehr als anderes in den Sternen, weil Cyber-Angriffe derzeit noch mitunter sehr konfus und anarchistisch ablaufen. Fest steht: Computer sind nach den Angriffen immer noch da und können mit Backups wieder gangfähig gemacht werden, werden auch selbst immer robuster. Aber es gibt im Cyberkrieg keine Verlierer und Gewinner. Nur temporäre Erfolge, und darum ist das, was alle unter *Cyber* verstehen, nicht nur eine (Kriegs-)Politik mit anderen Mitteln, sondern mehr noch die Fortsetzung der Diplomatie mit anderen Mitteln. Denn dann, wenn Diplomat.innen aufhören zu reden, beginnen Gesten, Militärmanöver und Flottenparaden. Noch haben Cyber-Operationen als Provokation keine konventionellen Gefechte ausgelöst, auch weil bisher vorsichtig damit umgegangen wurde. Trotz der Gefahr dieser Angriffe ist es zwar sehr unwahrscheinlich, dass Cyberwaffen konventionelle Waffen ablösen werden; nach mehr als zwanzig Jahren derartiger Computersabotage und -lücken bleibt es jedoch nun uns überlassen, einen Ausweg aus dem Cyberwar zu finden.

Erich Möchel

Erich Möchel ist seit 1983 Medienkritiker und Kulturjournalist; für den *Falter*, das Radio OE1, den Standard, das Wirtschaftsblatt, für heise.de, quintessenz, Futurezone, den ORF und einige mehr. Er beschäftigte sich schon lange vor Edward Snowden und Echelon kritisch mit geheimdienstlichen Abhörpraktiken. Darüber hinaus ist er Mitglied beim Österreichischen Journalisten-Club und im International Board of Advisors von Privacy International. Er ist zudem Autor mehrerer Romane und Theaterstücke.

Weitergehende Erkenntnisse aus den Verhandlungen zur EU-Datenschutzgrundverordnung

Zusammenfassung des Vortrags von Jan Philipp Albrecht

Welche Grundannahmen der Unternehmen und staatlichen Akteure haben sich in den DSGVO-Verhandlungen gezeigt? Welche Punkte waren ihnen sehr wichtig, welche eher weniger, und was kann man daraus ableiten, wie ihre zukünftigen Geschäftsmodelle aussehen?

Einleitend dankte Jan Philipp Albrecht dem FIfF für die Einladung. Es sei seine erste größere FIfF-Veranstaltung, er verfolge aber die Aktivitäten des FIfF regelmäßig und lese die *FIfF-Kommunikation*; während den Verhandlungen habe er die ganze Zeit die Cyberpeace-Taube auf dem Notebook gehabt. Es sei wichtig, deutlicher als bisher auf die Bedeutung von Technikregulierung, Technikfolgenabschätzung und Ethik für die Politik und die großen politischen Entscheidungen hinzuweisen; viele hätten das noch nicht erkannt. In der Politik Tätige müssten erkennen, dass der entsprechende Sachverstand und die Wahrnehmung dieser Themen ins Zentrum der politischen Auseinandersetzung rücken müssen – er ist aber auch der Ansicht, dass das in vielen Bereichen heute bereits passiert.

Die Arbeit an der Datenschutz-Grundverordnung habe ihren Teil dazu beigetragen, die Aufmerksamkeit für die Frage zu verstärken, wie Technik unser Leben verändert. Der Datenschutz als der Ausgangspunkt vieler weiterer Grundrechte und Regulierungsansätze in der Digitalisierung spiele dabei eine wichtige Rolle.

Bedeutung und Entwicklung der Datenschutz-Grundverordnung

Datenschutz und die damit verbundene informationelle Selbstbestimmung sind ein vorgelagertes Grundrecht; sie entspringen der Würde des Menschen. In Folge des Volkszählungsurteils findet sich damit der Datenschutz in den Verfassungen Deutschlands und aller europäischen Länder wieder. Seit 2009 ist er auch verbindlich im Vertrag der EU verankert. Artikel 16, einer der grundlegenden Vertragsgrundsätze, legt fest, dass jeder ein Recht auf den Schutz seiner persönlichen Daten hat. „Jeder" heißt auch wirklich *jeder*; der Datenschutz ist ein Menschenrecht, nicht nur ein Bürgerrecht. Auch in Artikel 8 der Charta der Grundrechte der Europäischen Union ist er als Schutzauftrag und Freiheitsrecht verankert.

Datenverarbeitung ist nur auf zwei Grundlagen zulässig: der Einwilligung des Betroffenen oder einer gesetzlichen Bestimmung. Artikel 16 enthält den Auftrag an den EU-Gesetzgeber, Gesetze zu verabschieden, um dieses Grundrecht zu schützen. Die EU-Kommission hat dies nach Inkrafttreten des Lissabon-Vertrags in Angriff genommen und 2009/10 ein entsprechendes Gesetzgebungsverfahren auf den Weg gebracht. Dieses Verfahren hat ca. 5–6 Jahre gedauert, begonnen mit dem in diesen Fällen üblichen Konsultationsverfahren. 2012 wurde ein Vorschlag für eine Verordnung unterbreitet, die nationale Gesetze in ihrem Regelungsbereich ersetzt. Im April 2016 wurde die Verordnung dann endgültig vom Ministerrat angenommen; sie gilt nach einer zweijährigen Übergangsphase ab dem 25. Mai 2018. Sowohl diejenigen, die mit Datenschutz befasst sind, als auch alle anderen sollten sich das Gesetz genau anschauen: Welche Rechte und Pflichten gibt es beim Datenschutz?

Jan Philipp Albrecht

Man darf sich dabei nicht abschrecken lassen von ungewohnten Begriffen. Es ist ein Gesetz für 28 Staaten in der Europäischen Union, und damit ein Kompromiss zwischen diesen 28 Staaten. Darin besteht gleichzeitig der große Mehrwert: Im europäischen Raum wird es künftig eine einheitliche Regelung für den Datenschutz im gesamten gemeinsamen Binnenmarkt geben; dies ist gegenüber der heutigen Situation ein großer Fortschritt. Viele Unternehmen verarbeiten eine große Menge an Daten – dabei war der Umfang der Verarbeitung in den letzten Jahren sehr expansiv. Es ist zu erwarten, dass sich dieser Trend fortsetzt und weiter verstärkt. Dabei versuchen Unternehmen, die heutigen Regelungen zu umgehen, indem sie sich in einem Land mit niedrigen Standards niederlassen und dessen Gesetze für sich nutzen. Außerdem überblicken viele Betroffene nicht, welche Datenschutzregelungen im konkreten Fall eigentlich gelten. Verbraucher.innen müssen durch alle Instanzen der Gerichte gehen, um ihre Rechte einzufordern – dies ist nicht zumutbar.

Der Datenschutzaktivist Max Schrems aus Österreich hat diesen Klageweg beschritten, um das Safe-Harbour-Abkommen anzugreifen; sein Fazit danach war: Wer seine Rechte einklagen will, sollte sich das zweimal überlegen; eigentlich funktioniert es so, wie es heute geregelt ist, nicht. Es muss immer klar sein, welche Regeln gelten, und es muss möglich sein, seine Rechte im eigenen Land einzuklagen. Das ist einer der großen Fortschritte der Verordnung: In ganz Europa gilt das gleiche Gesetz und kann an

allen Gerichten eingeklagt werden. Das Gesetz wird europaweit einheitlich ausgelegt. Die Datenschutzbehörden müssen sich europaweit vernetzen und eine gemeinsame Linie bei der Auslegung einnehmen.

Inhaltliche Regulierung

Welchen Datenschutz erhalten wir durch die neue Verordnung? Das Gesetz war sehr umstritten, wird aber hochrelevant sein für alle, die in der Datenverarbeitung tätig sind. Es wird ihre Tätigkeit künftig massiv bestimmen.

Die Interessenvertretungen einflussreicher Unternehmen haben von Beginn an versucht, massiv Einfluss auf die Verordnung zu nehmen. Es gab gegenüber dem ursprünglichen Parlamentsentwurf ca. 4.000 Änderungsanträge. Diese zu verarbeiten war eine umfangreiche Arbeit und es hat lange gedauert, die Gedanken hinter allen diesen Änderungsanträgen zu verstehen.

Es gibt eine anhaltende Debatte in Europa, welche Kontrolle der Einzelne über seine Daten haben soll, wenn es z. B. um Geschäftsmodelle geht, die darauf aufbauen, dass möglichst viele Leute ihre Daten preisgeben und man als Anwender nicht die Möglichkeit hat, sich der Datenverarbeitung zu entziehen. Zusätzlich gibt es ein öffentliches Interesse von Behörden, Daten zu erheben. All dies schränkt die Möglichkeit Einzelner ein, die Verwendung ihrer Daten zu kontrollieren.

Diese Auseinandersetzung findet ständig statt und wird intensiver, wenn sich die Gesellschaft einmal daran gewöhnt hat, dass bestimmte Informationen über alle zur Verfügung stehen, oder dass es Geschäftsmodelle gibt, die auf diesen Daten basieren. Im Nachhinein ist es schwierig, festzustellen und durchzusetzen, dass der Umfang der Datenverwendung über die Selbstbestimmung des Einzelnen hinausgeht. In vielen Bereichen sind wir heute schon zu weit gegangen, dies muss wieder revidiert werden. Einzelne Geschäftsmodelle sind bereits heute nicht mehr mit dem geltenden Datenschutzrecht vereinbar, zum Beispiel die Praxis der Datensammlung durch Browser-Apps. Doch die Durchsetzung des Rechts stößt auf Widerstand, wenn solche Geschäftsmodelle bereits umgesetzt sind.

Die europäischen Unternehmen stehen im Wettbewerb mit Unternehmen im Silicon Valley, die datenintensive Dienste marktbeherrschend anbieten. Konkurrenzfähig sind diese europäischen Unternehmen nur, wenn sie nicht unter unfairen Wettbewerbsbedingungen gegen die Konkurrenz unter unterschiedlichen Rechtsordnungen antreten müssen. Möglich ist dies unter zwei Bedingungen:

1. Man senkt die hiesigen Standards auf das im Silicon Valley geltende, niedrige Niveau ab – darauf haben viele gedrängt: Sonst würden die europäischen Unternehmen wettbewerbsunfähig.

2. Man gestaltet die Regelungen so, dass sich alle Wettbewerber an einen hohen Standard halten müssen. Dieser hohe Standard wird so fortgeführt, wie er über die letzten 30–40 Jahre entwickelt wurde. Wenn sich Wettbewerber nicht daran halten, werden angemessene Sanktionen verhängt.

Die EU-Datenschutzgrundverordnung setzt mit der Idee des Marktortprinzips die zweite Variante um: Jeder, der im Geltungsbereich der Verordnung Dienste oder Waren anbietet, muss sich an ihre Regeln halten, sonst drohen Strafen in Höhe von bis zu 4 % des weltweiten Umsatzes. Auf diese Weise kann der Standard gehalten und durchgesetzt werden.

Aus Sicht des Europäischen Parlaments darf die Verordnung nicht hinter den heutigen Standard zurückfallen; dies ist in der durch die Grundrechte gesetzten Situation gar nicht möglich. Deswegen haben sich auch große Unternehmensverbände hinter den Vorschlag gestellt. Dieser Vorschlag stellt das Vertrauen in das Recht wieder her. Weltweit werden Dienste aus Europa im Markt angenommen, auch technologisch anspruchsvolle Dienste.

Weitere Eckpunkte

Wichtige einklagbare und sanktionierbare Eckpunkte des Datenschutzes sind:

- Die Gestaltung der Einwilligung für den Anwender: Eine „stillschweigende“ Einwilligung, z. B. durch vorangekreuzte Kästchen, ist nicht als informierte Einwilligung gültig. Nur eine aktive Handlung zur Datenfreigabe zählt als Einwilligung.

- Die Verordnung macht einen großen Schritt hin zu mehr Transparenz: Verständlichkeit, einfache Sprache, wiedererkennbare standardisierte Symbole. Über alle wesentlichen Aspekte muss der Anwender informiert werden: Weitergabe in Drittstaaten, Automatisierung der Verarbeitung, nach welchen Kriterien Daten verarbeitet werden – all das muss in Zukunft offengelegt werden.

- Es werden neue Rechte geschaffen, z. B. auf Datenportabilität: Das Recht, dass Anwender.innen ihre Daten in maschinenlesbarem Format bekommen können oder dass der bisherige Anbieter die Daten an einen anderen Anbieter mit besseren Konditionen weitergibt.

- Es besteht nun eine verstärkte Löschungsverpflichtung auch im Internet. Das Recht auf Vergessenwerden wird etabliert.

- Datenverarbeiter erhalten deutlich weiter gehende Pflichten als bisher. Das Modell des Datenschutzbeauftragten wird europaweit verpflichtend gemacht. Bildung und Wahrnehmung von Datenverarbeitungsvorgängen soll verstärkt werden und sich durchsetzen; es soll deutlich mehr Aufmerksamkeit durch Technikfolgenabschätzung geben. Bei Data Breaches gibt es eine verbindliche Meldepflicht, dadurch wird mehr Aufmerksamkeit auf Datenschutz und Konsequenzen der Datenverarbeitung gelenkt.

Albrecht zieht ein positives Fazit: Es kann gelingen, über die Gesetzgebung deutliche Fortschritte zu erreichen, auch wenn das zunächst nicht erkennbar ist. Es gibt eine große Chance, über die EU und ihren globalen Machtfaktor Standards zu setzen. Das gilt auch für weitere Themen: IT-Sicherheitsstandards, die Nutzung von Open Source etc. – dafür müssen wir uns auf die entsprechenden Prozesse einlassen. Es geht um neue politische Debatten, die über die deutschen Debatten hinausgehen.

Diskussion

Wie kann das Bewusstsein für den Datenschutz und seine Bedeutung geweckt werden? Aufsichtsbehörden und Verbände müssen gerade bei alltäglichen Fällen darauf hinweisen, dass man immer überprüfen muss: Was wird mit den Daten gemacht? Es muss eine verpflichtende Technikfolgenabschätzung geben.

Die Verordnung wurde im Vortrag sehr positiv geschildert, dies ist auf europäischer Ebene nachvollziehbar. Aber: Im Vergleich zum heutigen Bundesdatenschutzgesetz gibt es teilweise große Rückschritte. Auch Albrecht hatte diese Befürchtung zu Beginn – aus seiner Sicht ist es dazu aber nicht gekommen. Die Unterstellung, dass es in anderen Ländern der EU keine vergleichbaren Datenschutzbestimmungen wie in Deutschland gibt, stimme so nicht. Die Datenschutz-Grundverordnung ist nicht vollkommen neu. Lediglich Begriffe wurden bisher unterschiedlich interpretiert. Hohe Standards waren schon bisher EU-weit vorhanden. Aus seiner Sicht gibt es fast keine Rückschritte, Ausnahmen dazu gibt es evtl. bei der Videoüberwachung (aber aus seiner Sicht keine niedrigeren Standards) und bei einem anderen Berechnungsschlüssel für betriebliche Datenschutzbeauftragte, aber auch hier gebe es keine Verschlechterung. Die EU-Datenschutzgrundverordnung geht in einigen Punkten über den bisherigen deutschen Datenschutz hinaus, z. B. durch konkrete Anforderungen an informierte Einwilligung – und das mit Gültigkeit in ganz Europa. Heute ist man zwar vom BDSG geschützt, das hilft aber nicht, wenn ausländische Dienste genutzt werden, wie z. B. Dienste von Facebook, Google, Apple, … Gleichzeitig kann man bei einem Kompromiss zwischen 28 Ländern nicht erwarten, dass die eigenen Formulierungen immer überall akzeptiert werden. Das ist der Preis der Globalisierung; die Alternative wäre der Rückzug ins Nationale. Das bedeutet nicht, dass alles perfekt ist. Weitergehende Regelungen zu Direktmarketing, Vertragsschluss mit Opt-out wären beispielsweise wünschenswert gewesen. Aber die Durchsetzbarkeit des Rechts macht die Verordnung zu einem großen Erfolg.

Großes Lob für die Transparenz, welche Lobbygruppe welche Vorschläge gemacht hat. Wie kann man diese Transparenz allgemein erreichen? Welche Visualisierungstechniken sind dafür geeignet, welche Erfahrungen gibt es dazu? Die Open-Data-Darstellung wurde von Aktivisten aus Hamburg erstellt. Damit wurde ein Einblick für Journalisten in ein sehr komplexes Themengebiet geschaffen. Wenn sich mehr Menschen engagieren, solche Projekte stärker gefördert werden und es Vereinfachungen und Möglichkeiten gibt, diese Informationen abzurufen, dann ist auch mehr Partizipation an solchen Prozessen möglich. Die Wahrnehmung für die Wichtigkeit dieser Transparenz ist noch nicht groß genug; wir müssen die Frage der Zugänglichmachung und Visualisierung zum Thema machen. Engagement im Bereich der Informationsfreiheit ist wichtig, aber ein dickes Brett. Es gibt bisher keine IFG-Regeln für Mitgliedsländer der EU.

Für die IT-Sicherheit brauchen wir eine europäische IT-Infrastruktur, die die europäischen Regeln einhält. Kann diese Infrastruktur erreicht werden? Ab Anfang des Jahres 2017 soll eine neue Richtlinie für IT-Sicherheit für kritische Infrastrukturen erarbeitet werden. Im Gesetzgebungsverfahren für Standards und Verbraucherschutz müssen Regeln für IT-Sicherheit durchgesetzt werden, die über Produkthaftung hinausgehen. EU-weite Standards sind dabei wichtig. Allerdings steht das heute industriepolitisch nicht im Vordergrund; z. B. bei Hardwareproduktion gibt es keine entsprechenden Angebote durch europäische Anbieter; es muss wieder ein wettbewerbsfähiges europäisches Angebot geben. Dazu brauchen wir Standards, die überprüfbar sind, z. B. sollte Open Source zum Standard gemacht werden. Produkte – beispielsweise von Microsoft – sind nicht überprüfbar; gleichzeitig kann durch die Transparenzforderung auch die europäische Industrie gefördert werden. Die Industrieverbände beschränken sich stattdessen leider auf den Kampf gegen ein Haftungsregime für Sicherheitsstandards.

Fast alle Regelungen der Verordnung sind auf dem Niveau des BDSG – gibt es eine Seite, wo es Konfliktfelder und Bruchstellen gibt? Dies sind Detailfragen; grundsätzlich gibt es keine großen Unterschiede. Die Linie des Datenschutzes wird weitestgehend gehalten; dies hängt aber auch von der nationalen Gesetzgebung ab. Die deutsche Initiative zielt auf Absenkung der Standards ab, z. B. bei der Zweckbindung. Deutschland entwickelt sich derzeit zum „Schmuddelkind" beim Datenschutz. Einen Vergleich der Verordnung mit dem bisherigen Recht gibt es bisher in Handbüchern; es existieren synoptische Darstellungen, auch in der eigenen Publikation.

Das Recht auf den Export eigener Daten aus sozialen Netzwerken und Recht auf Löschen wurden genannt. Ist das nun in der Verordnung enthalten? Ja, beides ist enthalten.

Was, wenn sich der Betreiber einer Webseite nicht an die Regelungen hält? Es gibt eine Beschwerdemöglichkeit bei Aufsichtsbehörden, auch bei eigenen Behörden. Diese ist einklagbar bei Gerichten im eigenen Land.

Welche Regelungen gelten für Tracking-Cookies? Tracking-Cookies sind durch die Regelungen abgedeckt; dies ist abhängig vom Zweck der Cookies: IT-Sicherheit und Gefahrenabwehr vs. Werbung. Hier ist auch die E-Privacy-Richtlinie zu beachten, diese soll ebenfalls demnächst reformiert werden. Hier muss die informierte Einwilligung auch eine zentrale Rolle spielen.

Jan Philipp Albrecht

Jan Philipp Albrecht sitzt für die Grünen im EU-Parlament und verhandelte dort wesentlich die EU-Datenschutzgrundverordnung. Zudem ist er dort stellvertretender Vorsitzender des Innenausschusses. Davor spezialisierte er sich in IT-Recht an den Universitäten Hannover und Oslo. Seither lehrt er neben seiner Abgeordnetentätigkeit Europäische Rechtsinformatik an der Universität Wien und schreibt juristische Fachbeiträge.

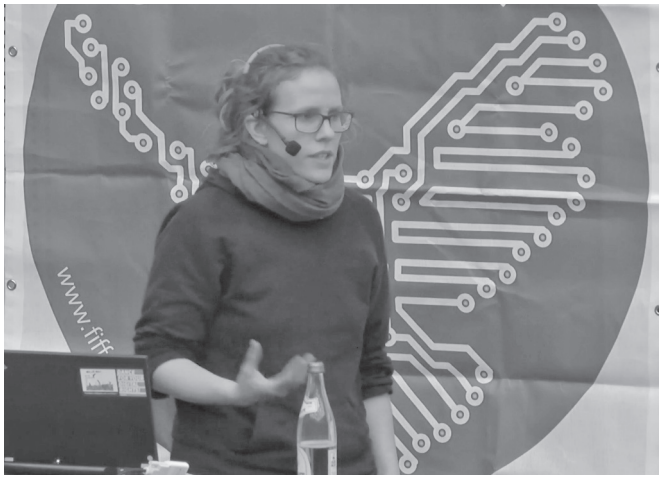
Geheimdienste außer Kontrolle und warum die BND-Reform keine ist

Zusammenfassung des Vortrags von Anna Biselli

In den letzten zweieinhalb Jahren sind im NSA-Untersuchungsausschuss des Bundestages zahlreiche Rechtsverstöße und fragwürdige Praktiken des BND zu Tage getreten. Doch anstatt dafür zu sorgen, dieses Vorgehen abzustellen, Geheimdienste zu beschränken und besser zu kontrollieren, werden ihre Befugnisse ausgeweitet und die bisherigen Aktivitäten weitgehend legalisiert. Es stellt sich die Frage, wie und ob Geheimdienste kontrollierbar sind, wenn ihre Haupteigenschaft ist, im Geheimen zu agieren, und selbst das Parlament nicht wissen soll, was sie genau tun. Und: Passen solche Institutionen überhaupt in eine demokratische Gesellschaft?

Geheimdienste außer Kontrolle

Es gibt nicht nur einen Geheimdienst in Deutschland. Es gibt den Bundesnachrichtendienst (BND), auf Bundesebene das Bundesamt für Verfassungsschutz (BfV), den Militärischen Abschirmdienst (MAD) und eine Reihe Landesverfassungsschutzämter. Da an dieser Stelle nicht die Kontrollierbarkeit all dieser Dienste angesprochen werden kann, soll der Fokus auf dem Bundesnachrichtendienst liegen.



Anna Biselli

Obwohl die sogenannte Bundesnachrichtendienstreform bzw. die Änderung des BND-Gesetzes noch nicht lange her ist, ist sie doch bei vielen schon wieder aus dem Fokus gerutscht. Die BND-Reform war eine eher traurige Angelegenheit – traurig besonders in Hinblick auf den NSA-Untersuchungsausschuss (NSAUA), der eigentlich eine echte Reform der Nachrichtendienste zur Folge haben sollte. Der Ausschuss wurde 2014 im Nachgang zu den ersten Snowden-Enthüllungen eingesetzt, weil es aufzuklären galt, was die Geheimdienste der *Five Eyes* – also Australiens, Neuseelands, Großbritanniens, Kanadas und der USA – in Deutschland genau tun. Im Verlauf des Ausschusses wurde schnell klar, dass diese Dienste nicht nur in Deutschland agieren, sondern dass auch die deutschen Dienste selbst an den Überwachungen beteiligt waren, und zwar in größerem Ausmaß als erwartet: Es wird mitgearbeitet und mitgeholfen. Damit stellte sich u. a. die Frage, wieviel die Regierung von den Aktivitäten ihrer eigenen Geheimdienste wusste, wieviel die politische Ebene davon wusste und wie diese Zusammenarbeit gelaufen ist. Der BND rückte im Verlauf der Untersuchungen daher immer mehr in den Vordergrund des Ausschusses, sodass aus dem NSAUA fast ein BND-Untersuchungsausschuss wurde. Erwartbar wäre gewesen, dass der NSAUA über mehrere Jahre seine Arbeit macht, einen Abschlussbericht vorlegt und dann entschieden wird, welche gesetzlichen und organisatorischen Maßnahmen sich daraus ergeben, um Geheimdienste besser zu kontrollieren.

Soweit kam es nicht. Zumindest noch nicht.

Der lange Weg zur „BND-Reform“

Bevor der Ausschuss abgeschlossen war, wurde eine BND-Reform angekündigt. Der Begriff „BND-Reform“ ist allerdings irreführend: einerseits schon der Begriff „Reform“ an sich, andererseits geht es nicht nur um das BND-Gesetz, sondern um eine ganze Reihe von Gesetzen. Was die Geheimdienste in Deutschland tun, wird nicht nur durch das jeweilige BND-Gesetz oder das Bundesverfassungsschutzgesetz geprägt, sondern auch durch Gesetze wie das Parlamentarische-Kontrollgremiums-Gesetz (PKG-Gesetz, das die Kontrolle der Nachrichtendienste regelt. Daher umfasst die „Reform“ ein ganzes Paket an Gesetzesänderungen.

Schon als die ersten Skandale um die Snowden-Enthüllungen aufkamen, wurden erste Gesetzesänderungen für die Arbeit der Geheimdienste gefordert. Im Juni 2015 legte die SPD ein sogenanntes Eckpunktepapier vor, in dem sie als erste Fraktion des Bundestages den Aufschlag machte, zu formulieren, was sie sich unter einer BND-Reform vorstellen. In diesem Papier forderten sie unter anderem, dass die Auslandsaufklärung des BND auf ein „erforderliches Maß“ beschränkt werden müsse. Gummibegriffe wie diese ließen allerdings Skepsis aufkommen, denn diese Formulierungen öffnen Tür und Tor dafür, dass die Dienste tatsächlich doch frei agieren können, wie sie wollen, weil solche Wendungen nach Belieben ausgelegt werden können. *Netzpolitik.org* hatte die Befürchtung, dass Forderungen wie diese so eher zu einer Manifestation der Zustände führen. Sommer 2015 war zudem die Zeit auch der Selektorenaffären, bei denen sich herausstellte, dass der BND für die NSA-Ziele in Europa unter anderem europäische Regierungen ausspioniert hat. Aus den Stellungnahmen zu diesen und ähnlichen öffentlich gewordenen Affären lässt sich heraushören, dass es wahrscheinlicher ist, dass diese skandalösen Aktivitäten legalisiert als dass sie unterbunden werden.

Im Januar 2016 wurde tatsächlich zum ersten Mal über den Entwurf eines konkreten BND-Änderungsgesetzes diskutiert. Die *Tagesschau* und die *Süddeutsche Zeitung* berichteten relativ positiv über das anstehende Gesetz: Es wurde der Eindruck vermittelt, das Abhören in der EU werde ab sofort eingeschränkt

und strikt reguliert, die parlamentarische Kontrolle verbessert und so der berühmte Satz von Bundeskanzlerin Merkel „Abhören unter Freunden geht gar nicht“ endlich auch umgesetzt. Alle Maßnahmen seien ab sofort auf ihre Zulässigkeit zu prüfen, der Skandal werde aufgearbeitet und in Zukunft könne uns das alles nicht mehr passieren, alles komme „wieder in Ordnung“. Man durfte skeptisch bleiben. Neue Gesetze vor ihrer Umsetzung zu beurteilen ist schwierig, besonders, wenn nur Auszüge zur Verfügung stehen. Eine lange Weile verging, in der der Gesetzesentwurf weiterhin unveröffentlicht blieb, bis irgendwann – nur vage begründet – bekanntgegeben wurde, die BND-Gesetzesreform liege auf Eis.

Im Juni 2016 lag *Netzpolitik* dann ein Entwurf vor, der allerdings erheblich von den Positivbotschaften vom Januar abwich und laut dem wesentlich weniger strikt geregelt werden soll als gehofft. Dann ging alles sehr, sehr schnell: Am 8. Juli war die erste Lesung des Gesetzes im Bundestag. Nach der Sommerpause fand Ende September eine Sachverständigenanhörung im Bundestag statt, im Oktober dann die zweite und dritte Lesung. Angesichts der üblichen Sommerpause der Politik ist das ein extremes Eiltempo. Innerhalb dieser kurzen Zeit konnte gar keine umfassende Kritik an diesem Gesetz entstehen, die hätte berücksichtigt werden können. Nach der ersten Veröffentlichung und der ersten Lesung gab es dennoch massenweise Stellungnahmen von verschiedensten Stellen, die dieses Gesetz für komplett untragbar hielten: Zum einen äußerte sich die Opposition (erwartbar), zum anderen äußerten sich aber auch unabhängige Juristen, ehemalige oberste Verfassungsrichter, Journalistenverbände, ARD und ZDF, viele Menschenrechtsorganisationen, die OSZE und drei UN-Sonderberichterstatter. Eine ganze Bandbreite von Experten kritisierte das Gesetz scharf und bescheinigte ihm mehr oder weniger Verfassungswidrigkeit.

Warum die Reform verfassungswidrig ist

Warum das neue BND-Gesetz verfassungswidrig ist, lässt sich an folgenden Kernpunkten festmachen:

Abhören im Inland

Der BND ist ein Auslandsnachrichtendienst, d. h. er soll Dinge und Personen im Ausland aufklären. Nun hört der BND aber nicht nur im Ausland Leitungen ab, sondern tut dies jetzt und in Zukunft auch im Inland. Es gab einen Aufschrei, als bekannt wurde, dass der BND an den Telekomleitungen mithört und auch im DE-CIX an die Leitungen gegangen ist, dem größten deutschen Internetknoten in Frankfurt, denn es ist nicht sein Aufgabenbereich, über Deutsche aufzuklären.

Der BND reagierte darauf mit der Behauptung, die eigene Bevölkerung werde herausgefiltert. Über die Leitungen am DE-CIX laufe aber ja auch Kommunikation, die von außerhalb Deutschlands nach außerhalb gehe. Man filtere alle Verkehre heraus, die einen Endpunkt ihrer Kommunikation in Deutschland hätten. Das Problem dabei ist jedoch, dass der BND gar nicht in der Lage ist, die Kommunikation so spezifisch zu filtern. Ein Zeuge der NSAUA wurde zur Umstellung von leitungsvermittelter auf paketvermittelte Kommunikation befragt. Er sagte aus, früher (zur Zeit der alleinigen Telefonkommunikation) sei alles sehr geordnet gewesen, wie in einer gut sortierten Apotheke mit vielen Schubladen. Man habe in eine Schublade hineingeschaut und gewusst, was man bekommt. Mit dem Internet sei es, als würde man alle Schränke und Schubladen auf dem Boden auskippen und in diesem Haufen müsse man nun finden, was man sucht. Viele der Zeugen gaben zu, dass die Filterung der Kommunikation nach Landeszugehörigkeit nicht möglich ist, auch nicht über Suchkriterien wie der Top-Level-Domain einer Mail-Adresse. So zu filtern ist fern jeder Lebensrealität und fern von einem Grundrechtsschutz, den der BND theoretisch gewährleisten muss. Ergänzend zu den Aussagen der Zeugen forderte der NSAUA sowohl vom Chaos Computer Club als auch von der Bundeswehruniversität in München Gutachten zur Filterbarkeit der Kommunikation an solchen Knotenpunkten an. Beide kamen zu dem erwartbaren Ergebnis, dass es nicht möglich ist, die Kommunikation aller Inländer zu hundert Prozent auszusortieren.

Hundert Prozent mag zunächst nach einer übertriebenen Anforderung klingen. Doch selbst mit einem Filter mit 99,5-prozentiger Genauigkeit muss man sich klarmachen, was das in Zahlen bedeutet. Am Frankfurter Internetknoten DE-CIX laufen mehrere Terabyte Daten pro Tag durch die Leitungen. Laut dem Geschäftsführer vom DE-CIX ginge es selbst mit dem weltbesten Filter noch um Millionen falsch gefilterter Verbindungen an einem einzigen Tag allein an diesem einen Internetknoten in Frankfurt. Diese Millionen falsch eingeordneter Verbindungen sind Millionen von Grundrechtsverletzungen. Um Deutsche abzuhören, braucht der BND jedoch eine besondere Anordnung, die er bei der G10-Kommission beantragen muss – für eine spezielle Person und mit der jeweiligen Begründung, dass bei dieser Maßnahme relevante Informationen zu erwarten sind.

Ungerichtete Massenüberwachung der Kommunikation

Vor der Gesetzesänderung musste der BND beantragen, einzelne Leitungen zu überwachen. Der BND konnte nicht einfach den gesamten DE-CIX abhören, sondern musste das Bundeskanzleramt bitten, eine bestimmte Leitung abzuhören, bei der der Verdacht bestand, dass über diese Leitung Kommunikation eines Verdächtigen laufe. Dies wurde nun geändert: Der BND kann jetzt vom DE-CIX fordern, ihm das komplette Kommunikationsnetz zum Abhören freizugeben – und muss dies gestattet bekommen. Ebenfalls abgeschafft wurde mit dem neuen BND-Gesetz die Regel, dass nur 20 Prozent des Verkehrs überwacht werden durfte. Ganz eindeutig war diese Regel zwar nie gewe-

sen, aber eine unbestimmte Massenüberwachung war so nicht möglich, sondern der BND hatte zu selektieren. Auch das hat er jedoch nie getan. Laut Experten, die die Systeme unter die Lupe genommen haben, war die 20-Prozent-Regel nicht einmal technisch implementiert. Allerdings war sie so ohnehin absurd, denn selbst zu Spitzenzeiten beträgt die Auslastung der Internetknoten nur etwa 11 Prozent.

Unbeschränkte Verwendung der Metadaten

Metadaten sind die Daten, die die Umstände einer Kommunikation verraten: Wer mit wem wann von wo aus mit welchem Kommunikationsmittel kommuniziert. Wenn der BND diese Daten sammelt, erfährt er zwar nicht den Kommunikationsinhalt, erhält aber die Möglichkeit, die Kommunikation auf ganz anderer Ebene auszuwerten. Darum geht es bei der Vorratsdatenspeicherung, worüber es viele Proteste gab – und die 2012 vom Bundesverfassungsgericht als verfassungswidrig verworfen wurde. Jetzt darf der BND das – ohne Beschränkung. Er darf Metadaten – ohne einen Anlass anzugeben – sammeln und verstößt damit gegen alle Bestimmungen, die das Bundesverfassungsgericht 2012 auferlegt hat. Er verstößt damit auch gegen alle Bestimmungen des Europäischen Gerichtshofs von 2014, laut dem niemals ein Generalzugriff auf Metadaten stattfinden darf, der ohne jegliche Einschränkung, d. h. spezifischen Anlass, stattfindet. Weder das Bundesverfassungsgericht noch der Europäische Gerichtshof haben eine Ausnahmeregelung für Geheimdienste festgelegt, beides waren allgemeingültige Urteile, die sich uneingeschränkt auf die Verfassungsmäßigkeit beziehen. Der BND darf laut BND-Gesetz nun nicht nur Verkehrs- und Metadaten für sechs Monate ohne Einschränkung speichern, sondern dies gilt beispielsweise auch für Inhaltsdaten, wenn sie einem Test der Systeme dienen – und der BND testet gerne Systeme. Es ist bekannt, dass es sowohl beim BND als auch beim Verfassungsschutz Systeme gibt, die jahrelang im Testbetrieb und (offiziell) niemals tatsächlich produktiv im Einsatz sind. Die im Testbetrieb gespeicherten Daten dürfen darüber hinaus auch durchaus verwendet werden, sodass es im Endeffekt keinerlei Einschränkung gibt.

Der BND hat in der Vergangenheit immer wieder Recht so ausgelegt, wie es ihm maximale Handlungsspielräume ermöglicht hat. Dem BND dieses Ausmaß der Interpretation zu gestatten ist angesichts der Aussagekraft von Metadaten nicht klug. Sie sind keine harmlosen Informationskrümel, wie etwa die Aussage von General Keith Alexander – ehemaliger Direktor der NSA – zeigt: „*We kill people based on metadata*" – Menschen werden anhand von Metadaten getötet. Metadaten, die auch der BND einfach so an die USA weiterleitet. Mit dem neuen Gesetz darf er das nun sogar vollkommen automatisiert; was vorher illegale Praxis war, ist nun nicht eingeschränkt, sondern legalisiert worden. Die Daten werden vom BND zudem ungefiltert weitergegeben. Dabei handelt es sich jedoch nicht nur um Daten über „böse Terroristen, die man so gerne fangen will". Bekannt ist, dass es im Zuge der Weitergabe von Daten aus Deutschland an die USA zu Korrelationen kam, durch die Zivilisten durch Drohnen getötet worden sind. Der BND, der Verfassungsschutz und die Zeugen im NSAUA reden sich damit heraus, dass bei der Datenweitergabe ein Vorbehalt – ein sogenannter Disclaimer – mit den Daten verknüpft wird, sodass mit den Daten „nichts Böses" gemacht werden darf und sie nur für nachrichtendienstliche Zwecke benutzt werden dürfen. Menschen mit Drohnen zu töten fällt jedoch ganz offensichtlich nicht unter die Kategorie nachrichtendienstliche Zwecke. Überraschenderweise hat keiner der Zeugen den zweiten Absatz des sogenannten Disclaimers erwähnt, nach dem die Daten für Tötung nur dann frei zur Verwendung sind, wenn ein Angriff zu erwarten ist. Dieser Absatz war geheim, bis er von *Zeit Online* veröffentlicht wurde. Da sich aber z. B. die USA in ihrem permanenten Krieg gegen den Terror befinden und stets einen Angriff durch den Terror befürchten, muss man nicht lange überlegen, wie sich aus Sicht der USA argumentieren lässt, auch im Einklang mit diesem Disclaimer Menschen anhand der vom BND übermittelten Daten umzubringen.

Mangelhafte Kontrolle des BND

Das riesige Problem an der Kontrolle der Nachrichtendienste ist, dass sie per se geheim arbeiten und man normalerweise nicht weiß, was sie tun. Der Verfassungsschutzchef von Sachsen-Anhalt äußerte sich gegenüber Anna Biselli in einem Gespräch mit Unverständnis darüber, warum man die Geheimdienste immer so kritisiere: Man habe doch gar keine Ahnung, was sie machen würden. Genau das ist aber Teil des Problems: Momentan ist die Arbeit der Nachrichtendienste massiv intransparent. Die Kontrollgremien können ihre staatliche Aufgabe kaum wahrnehmen, die Arbeit der Nachrichtendienste zu kontrollieren. Diese drei zuständigen Gremien sind die G10-Kommission, die die G10-Anordnungen zum Eingriff in Grundrechte von Deutschen genehmigen muss, das parlamentarische Kontrollgremium (PKG), das eine generelle Aufsicht über die Nachrichtendienste hat, und das Bundeskanzleramt, das die sogenannte Dienst- und Fachaufsicht über den BND hat.

Mit dem neuen BND-Gesetz gibt es nun ein weiteres Gremium – das sogenannte *Unabhängige Gremium*. Unabhängig klingt erst einmal ganz gut, dies ist aber angesichts dessen, dass es von der Bundesregierung bestimmt wird, unrealistisch – insbesondere, wenn man sich vor Augen führt, was die Bundesregierung in Kooperation mit den Nachrichtendiensten in den letzten Jahren vertuscht hat. Die *G10-Kommission* hat das Problem, dass sie immer nur das kontrollieren kann, was sie weiß. Sie ist immer dann hilflos, wenn der BND nicht berichtet, was er tut, was sie bereits vor Gericht bemängelt hat (die Klage wurde leider aus formalen Gründen abgewiesen). Beispielsweise hat die G10-Kommission nie die Liste mit den Selektoren und Suchbegriffen bekommen, auf deren Grundlage die USA europäische Ziele ausgespäht haben. Das *PKG* hat zusätzlich zum Informationsproblem das der Geheimhaltung, denn absurderweise dürfen die zwei Gremien, die die Nachrichtendienste kontrollieren sollen, nicht miteinander reden, d. h. untereinander nachfragen. Denjenigen (wenigen und auch zu anderweitigen Aufgaben Verpflichteten), die alle deutschen Geheimdienste kontrollieren sollen, werden also alle möglichen Steine in den Weg gelegt.

Das *Bundeskanzleramt* wiederum, als Fach- und Dienstaufsicht des BND, hat sich unglaubwürdig gemacht. Im NSAUA wurde bekannt, wie es selbst sich die Rechtsauffassung und Praktiken des BND angeeignet und diese abgenickt hat. Ein Beispiel hierfür ist die „Weltraumtheorie": Der BND begründete, wenn er in Bad Aibling Daten von einem Satelliten abhören würde, dann brauche er sich nicht an deutsche Gesetze zu halten, da die Sa-

telliten sich im Weltraum befinden, wo keine deutschen Gesetze gelten – eine Praxis, der der BND schon vor den Snowden-Enthüllungen folgte, und zu der er erst nach den Enthüllungen eine Rechtsauffassung formulierte und nach einigen Tagen Kopfzerbrechens per Mail dem Bundeskanzleramt mitteilte. Das Bundeskanzleramt wiederum besprach diese intern und übernahm trotz Zweifeln an der Glaubwürdigkeit der „Weltraumtheorie" letztlich die Rechtsauffassung des BND. Dieser Schulterschluss zeigt deutlich eine Zusammenarbeit zwischen der beaufsichtigenden und der zu beaufsichtigenden Behörde. Ein weiteres Beispiel für die Unglaubwürdigkeit des Bundeskanzleramtes ist eine inzwischen berühmt gewordene Weisung aus dem Jahr 2013, die offenbart, dass teilweise nicht einmal die Mitarbeiter.innen selbst von den Dingen wissen, von denen sie eigentlich wissen müssten: Die Anordnung, dass der BND das Ausspionieren europäischer Ziele zu unterlassen hat, war für eineinhalb Jahre verlorengegangen und tauchte dann wieder auf. Der zuständige Abteilungsleiter saß im NSAUA und gab zu, es wäre sicherlich besser gewesen, wenn er das vielleicht gewusst hätte, aber es habe ihm damals niemand etwas gesagt. Folglich gibt es innerhalb der Behörde einen extremen Informationsverlust. Diese Behörde nun, die weder sich noch den BND gut kontrolliert, soll also das „unabhängige" Kontrollgremium besetzen.

Mangelhafte Einschränkung der innereuropäischen Überwachung

In der BND-Gesetzesnovelle gibt es noch eine ganze Reihe von *Gummiparagraphen*, die gern so dargestellt werden, als sei es auf ihrer Grundlage nun viel schwieriger, Europäer abzuhören. Nach den diplomatischen Problemen – dem Abhören aller europäischen Regierungen – wurde gefordert, diese Praxis qua Gesetz zu begrenzen. In der Tat dürfen Europäer nur noch unter bestimmten Bedingungen abgehört werden; eine dieser Bedingungen ist, dass das Abhören für „Erkenntnisse von außen- oder sonstiger sicherheitspolitischer Bedeutung" sein muss. Das kann jedoch alles heißen und ist de facto keine Einschränkung. Der BND darf nun außerdem auch bei den sogenannten „Cybergefahren" überwachen – wozu auch banale DDoS-Angriffe zählen, die nicht einem Nachrichtendienst überlassen werden sollten.

Eingeschränkte Gültigkeit der Grundrechte

Der Hauptkritikpunkt am BND-Gesetz ist jedoch noch ein anderer. Abseits von der Kritik, dass es keine Filter gibt, die die Kommunikation von Deutschen vor Überwachung schützt, stellt sich die Frage, warum Politiker die Vorstellung haben, dass das Recht auf eine vertrauliche Kommunikation eigentlich nur für Deutsche gilt. Artikel 10 des Grundgesetzes zum Post- und Fernmeldegeheimnis gilt nicht nur für Deutsche, sondern für alle Menschen. Hier offenbart sich ein sehr fragwürdiges Verständnis von Grundrechten. Betrachtet man die BND-Gesetzdebatte im Nachhinein, dann hört man Politiker sagen: „Wenn ein Terrorist in Belgien wohnt, wo kommen wir denn da hin, wenn wir dabei noch auf irgendwelche Grundrechte achten?" Gießt man dieses Verständnis in ein Gesetz, demnach Grundrechte nur für Deutsche gelten, werden Europäer eventuell noch zu Menschen zweiter, alle anderen aber Menschen dritter Klasse – oder wie einige BND-Mitarbeiter sagen: *vogelfrei*. Ob so ein Dienst überhaupt in der demokratischen Gesellschaft seinen Platz haben sollte, darüber lässt sich also auch ganz grundlegend nachdenken.

Hintertüren für den BND

Neben dieser sogenannten BND-Reform sorgen auch eine Reihe anderer neuer Gesetzesentwürfe dafür, dass Geheimdienste in Zukunft ein leichteres Leben haben, weil sie ihnen – auf den ersten Blick nicht sichtbar – eine Hintertür bieten. Ein Beispiel ist das Bundesarchivgesetz, das erneuert werden soll. Scheinbar haben Geheimdienste hiermit nicht viel zu tun. Doch die Novelle soll dafür sorgen, dass Geheimdienste Akten nicht mehr an das Bundesarchiv geben müssen. Bisher müssen Akten nach 30 Jahren dort landen und verlieren mit Ablauf der Frist ihren Status *geheim*, sodass jeder sie einsehen kann. Wenn die Geheimdienste die Akten nicht mehr herausgeben müssen, sondern sie in ihrem Keller verbrennen, dann hat eine historische Aufarbeitung überhaupt keine Chance, mehr nachzuvollziehen, wie die Dienste tätig waren. Das beeinflusst zwar unsere jetzige Situation nicht, ist aber für die zukünftige Aufarbeitung eine Katastrophe.

Ein anderes gesetzliches Problem ist, dass das Lügen in Kontrollgremien immer noch straffrei ist: Gegen Falschaussagen gibt es bislang keine strafrechtlichen Maßnahmen. Mitarbeiter.innen der Geheimdienste können dem PKG das Blaue vom Himmel erzählen und haben maximal disziplinarrechtliche Konsequenzen zu fürchten, also nur die, die ihr Arbeitgeber veranlasst. Da aber anzunehmen ist, dass sie im Auftrag oder zumindest im Interesse ihres Arbeitgebers Unwahrheiten erzählen, gibt es praktisch keine Handhabe.

Durch die EU-Datenschutzgrundverordnung wird es nötig, dass auch das Bundesdatenschutzgesetz angepasst wird, und es scheint, dass die deutsche Regierung dabei unter sein bisheriges Datenschutzniveau zurücksinken will. In der Datenschutzgrundverordnung sind Regelungen festgehalten, die die Kontroll-

Anna Biselli

Anna Biselli schreibt für *netzpolitik.org* und dokumentiert zusammen mit Andre Meister jede öffentliche Sitzung des NSA-Untersuchungsausschusses. Da die Originalprotokolle erst nach dem Abschluss des Ausschusses veröffentlicht werden sollen, sind die Live-Blogs derzeit die einzige Möglichkeit, einen umfassenden Einblick in die Sitzungen zu bekommen. Anna versucht herauszufinden, was man gegen Geheimdienste und andere Spielarten der Überwachung tun kann.

möglichkeiten der Bundesdatenschutzbeauftragten noch weiter beschneiden. Außerdem sollen öffentliche Stellen, vor allem Sicherheitsstellen, bei Datenschutzverstößen in Zukunft einerseits straffrei sein und sich andererseits selbst kontrollieren: Behörden haben sich an ihren internen Datenschutzbeauftragten zu wenden, sodass Angelegenheiten intern geklärt werden können und nicht mehr nach außen dringen.

Was tun?

Wie lässt sich ein Geheimdienst kontrollieren? Nicht durch die Öffentlichkeit, weil diese nicht weiß, was er tut. Nicht durch die existierenden Kontrollgremien, denn selbst wenn diese gute Arbeit leisten wollen, sind sie in ihren Handlungen beschränkt und personell unterbesetzt. Die einzige Möglichkeit, das Agieren eines Geheimdienstes zu kontrollieren, ist, ihn mit weniger Geld auszustatten und damit seine Ressourcen und so wiederum seine Möglichkeiten – insbesondere so massenhaft zu überwachen – einzuschränken. Tatsächlich ist aber eine kontinuierliche Aufstockung der Etats zu beobachten. Der Bundeshaushalt hat den Etat für das Bundesamt für Verfassungsschutz (BfV) um 90 Millionen Euro auf 350 Millionen Euro aufgestockt. Für den BND gab es 110 Millionen Euro mehr, womit er bei 830 Millionen steht. Diese nicht unwesentlichen Aufstockungen zeigen recht gut, wohin die Entwicklung geht. Der Wille, Geheimdienste zu beschränken, ist offensichtlich nicht da. Man will ihnen stattdessen die Möglichkeit geben, immer mehr zu tun und immer mehr Daten zu sammeln. Der BND will laut *Süddeutsche Zeitung* einen Teil des Geldes einsetzen, um Verbindungen von Satellitentelefonen abzugreifen, aber auch um Messenger wie *Signal* oder *WhatsApp* zu knacken, die er mit seinen momentanen Ressourcen nicht auswerten kann, weil deren Codes in zu kurzen Abständen aktualisiert werden.

Der NSA-Untersuchungsausschuss hat einige Antworten ans Licht gebracht, viel mehr liegt aber noch im Dunkeln. Das liegt einerseits an der geringen zur Verfügung stehenden Zeit, andererseits aber auch an den Hindernissen der Aufklärung. Der NSAUA kann z. B. immer nur so lange arbeiten, wie die Legislaturperiode dauert. Natürlich müssten die Untersuchungen auch danach fortgesetzt werden, denn es gibt noch einen großen Aufklärungsbedarf. Dieser lässt sich jedoch nur von der neuen Regierung einfordern, wenn klar weiterhin ein öffentliches Interesse dafür erkennbar ist, wenn es uns allen also nicht egal ist, wir uns empören und uns mit dem BND beschäftigen. Wir müssen verhindern, dass sich die von Snowden aufgedeckten Vorkommnisse wiederholen, alle Erkenntnisse des Ausschusses vergessen werden und wir uns immer wieder neu überraschen lassen. Um die gewonnenen Erkenntnisse und Geschehnisse der NSAUA zu dokumentieren, wurde die Website *werkontrolliert-wen.de* ins Leben gerufen. Dokumente, Hinweise und Fragen sind dort willkommen.

FIfF-Konferenz 2016

Transparenz zwischen normativem Anspruch und kultivierter Unsichtbarkeit

Zusammenfassung des Vortrags von Leon Hempel

Beobachtung erfolgt in sozialen Situationen. Sie verlangt Kooperation zwischen den Akteur.innen: der beobachtenden Instanz und den Beobachteten – und dies in Kontexten von erzwungener Überwachung und Kontrolle. Wird die Lebenswelt zunehmend in eine Art Laborsituation verwandelt, in der jede soziale Situation ihrer Analysierbarkeit unterworfen ist, so verflüchtigt sich die Tatsache, dass permanent ins Unbewusste kooperiert wird. An drei unterschiedlichen Praktiken alltäglicher Techniknutzung wird das Problem der Transparenz in diesem Raum kooperativen Zwangs diskutiert.

Transparenz als politischer Begriff

Im Fokus stehen soll im Folgenden die Transparenz, wobei Transparenz hier als politischer Begriff auf die Verteilung von Sichtbarkeit und Unsichtbarkeit hinweist. Mit dem französischen Philosophen Jacques Rancière gesprochen, ist das die ästhetische Dimension von Politik: Es geht um die sinnliche Aufteilung des sozialen Raumes. Dabei agieren politische Institutionen als „Polizei“ und nehmen eine Aufteilung vor, wer sichtbar ist und wer eben auch nicht.

Üblicherweise machen gesellschaftliche Umwälzungen vormals Unsichtbares sichtbar; erst dann kann eigentlich von Politik gesprochen werden. Üblicherweise werden im politischen Prozess die Ränder der Gesellschaft invisibilisiert. Egal ob links oder rechts, die Extreme werden ausgeblendet. Aktuell sehen wir jedoch, wie die Mitte invisibilisiert wird. Dabei werden die Ränder

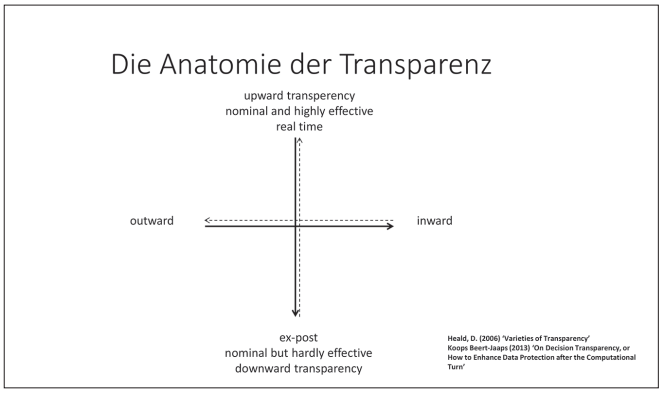
Leon Hempel

übermäßig sichtbar und geben in der vorliegenden Situtation sogar vor, das Ganze zu repräsentieren. Diese Pars-pro-toto-Argumentation ist natürlich ungerecht, denn wer spricht hier legitimerweise für wen?

Transparenz ist also die Frage nach der Verteilung von Sichtbarkeit. Diese Problemstellung hat es insbesondere bei technischen Infrastrukturen immer schon gegeben, aber sie gilt auch insgesamt für die Gesellschaft. David Heald fragt beispielsweise unabhängig von Technik danach, wie der Begriff der Transparenz – oder auch des Sichtbarkeitsregimes – in einer Gesellschaft verstanden werden kann.

Anatomie der Transparenz

Grundsätzlich beschreibt Heald dabei zwei Dimensionen: einerseits die Beziehung zwischen oben und unten, wobei *oben* die mächtigen Akteure wie Staaten, Behörden, große Organisationen wie größere Firmen/Konzerne oder internationale NGOs bezeichnet und *unten* im Gegensatz dazu die schwachen Akteure wie Individuen, kleine Gruppen oder kleine Organisationen beziehungsweise kleinere Firmen. Die horizontale Ebene bildet den Umgang der Akteure mit ihrer Umwelt ab. Innerhalb dieser Anatomie können nun verschiedene Blickrichtungen betrachtet werden.



Anatomie der Transparenz

Zum einen lässt sich so die Aufwärtstransparenz (*upward transparency*) analysieren, also inwiefern die Akteure unten in der Hierarchie nach oben hin sichtbar sind und somit von oben aus beobachtet werden können. Diese Sichtweise ist hochrelevant für den Datenschutz. Dem gegenüber steht die Abwärtstransparenz (*downward transparency*), also inwieweit Akteure oben in der Hierarchie nach unten hin sichtbar sind und daher von unten aus beobachtet werden können. Diese Richtung ist wiederum hochrelevant für die Informationsfreiheit.

Aus soziologischer Sicht ist jedoch eher die horizontale Ebene interessant. Dabei geht es um inwärts oder nach innen gerichtete Transparenz (*inward transparency*) und auswärts oder nach außen gerichtete Transparenz (*outward transparency*). Dabei bedeutet nach innen gerichtete Transparenz, inwiefern das *Außen* für die Organisation selbst sichtbar wird und daher beobachtet werden kann. Diese Richtung deutet an, auf welche Weise Sachverhalte außerhalb der organisationalen Grenzen innerhalb der Organisation „wahrgenommen" und verarbeitet werden können. Dieser Aspekt ist gerade in Bezug auf die Fähigkeiten von Geheimdiensten wie der National Security Agency der USA (NSA) hochinteressant.

Die zweite Richtung der horizontalen Differenzierung ist die nach außen gerichtete Transparenz. Dieser Begriff umfasst, auf welche Weise die Organisation für einen außerorganisationalen Akteur sichtbar und damit beobachtbar ist. Darum geht es immer, wenn Geheimdienste „kontrolliert" werden sollen, denn die Frage lautet ja: Wie gespenstisch ist es denn dort drinnen? Genau das wollen wir wissen. Aus dem Blick methodischer Ethnologie heraus geht man, soweit möglich, auf die fragliche Organisation zu, überschreitet die Grenzen und guckt sie sich dann – wenn möglich – von innen an. Die Kernfrage einer solchen Expedition lautet: Was ist transparent zu machen?

Diese Analyse der Verteilung von Sichtbarkeiten ist nicht nur auf explizit geheime Strukturen anwendbar, sondern lässt sich auch in anderen Bereichen der Gesellschaft sehen. Ein Beispiel ist die sogenannte *Infrastructural Inversion*, also das (Wieder-)Sichtbarmachen einer sonst unsichtbaren Infrastruktur. Bildlich und auch konkret auf eine Stadt bezogen könnte man sagen, die unsichtbare Stadt sorgt dafür, dass die sichtbare Stadt funktioniert. Dort „unten" (Bruno Latour) gibt es eben auch Berufe, Menschen und Orte, die überhaupt erst das gesellschaftliche Leben „oben" ermöglichen und aufrechterhalten, die aber in der Regel unsichtbar sind.

Laut Heald gibt es jedoch noch weitere Ausprägungen von Transparenz, beispielsweise Input/Output-Transparenz, also kann Ein- und Ausgehendes beobachtet werden. Aber auch eine Transparenz des gesamten Prozesses ist denkbar, insofern zusätzlich alle Zwischen- und Verarbeitungsschritte sichtbar sind. Weiterhin kann man Echtzeittransparenz und retrospektive Transparenz unterscheiden, wobei ersteres sich immer auf den aktuellen Status bezieht und letzteres nur auf vergangene Ereignisse. Zuletzt lässt sich zudem die gewünschte, nominelle Forderung nach Transparenz von der effektiven, tatsächlich vorhandenen Transparenz unterscheiden.

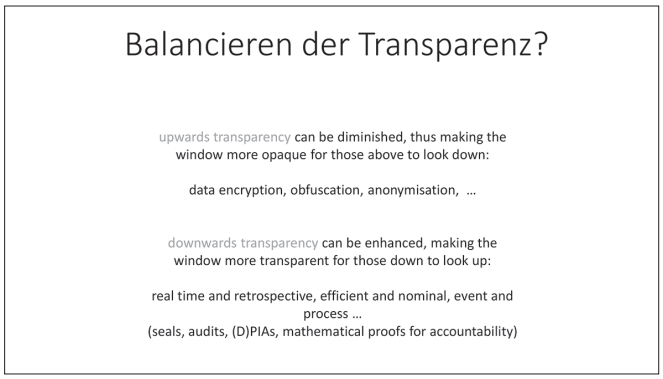
Massenhafte (In-)Transparenz und der Datenschutz

Von E. J. Koops (Universität Tilburg) werden diese Konzepte aktuell auf den Datenschutz oder genauer: auf dessen Verstöße angewendet, gerade in ihrer Ausprägung als Massenüberwachung. Mit dem obigen Theoriegebäude lässt sich die Situation wie folgt beschreiben: Bei staatlicher Massenüberwachung ist die *upward transparency* nominell und sehr effektiv, sie hat nicht nur das Einzelereignis, sondern den ganzen Prozess im Blick. Sie erfolgt in Echtzeit und ist auch retrospektiv wirksam. Möglich ist damit sowohl Strafverfolgung im Speziellen als auch Internetbeobachtung im Allgemeinen. Diese Art von Aufwärtstransparenz ist quasi *Full-Spectrum*.

Bei der entsprechenden *downward transparency* hingegen, also der Sichtbarkeit staatlichen Handelns für beispielsweise das Individuum, muss festgestellt werden, dass die Transparenz vollständig retrospektiv und größtenteils eher nominell, aber nicht effektiv abläuft.

Balance der Transparenz?

Aus dieser Analyse ergibt sich, dass eine Balance der Transparenzen nötig ist. Einer der Lösungswege dafür wäre die Stärkung – oder Modernisierung – des Datenschutzes. Um die Fähigkeiten anzugleichen, müssten gleichermaßen eine Hemmung von *upward transparency* und eine Förderung von *downward transparency* in Angriff genommen werden. Ersteres kann durch breitflächige Nutzung von Verschlüsselung oder engeren Datenschutzregelungen bewerkstelligt werden. Letztere Aufgabe kann durch Informationsfreiheitsrechte, externe Audits, glaubwürdige Siegel oder andersartige „Beweise" angegangen werden. Ziel sollten auch für die *downward transparency* letztendlich die Eigenschaften echtzeitlich, retrospektiv, nominal, effizient, event- und prozessfähig sein.



Balance der Transparenz

Natürlich haben die verschiedenen Akteure ungleiche Mittel im Kampf um die Sichtbarkeit zur Verfügung; ist ein Ausgleich also überhaupt denkbar? Am Beispiel des Attributionsproblems lässt sich diese Ungleichheit gut verdeutlichen: Das Attributionsproblem meint hier die Nichtidentifizierbarkeit derer, die sich im Netz bewegen und durch das Netz agieren. Das ist insbesondere bei *Cyberwar* und *Cybercrime* wichtig. Der US-Terror-Experte und ehemalige Sonderberater für Cybersecurity, Informationssicherheit und Cyberwar Richard Clarke sagte im Jahre 2010: „Das Attributionsproblem ist grundsätzlich gelöst." Wenn der Ursprung auch nicht sofort gefunden werde, so könne danach die Forensik bemüht werden und zur Not und bei Bedarf könne die NSA auch alles hacken. „*The NSA can do it*", das behauptet sie auch selbst und damit steht sie potent da, denn als Geheimdienst muss sie nichts groß begründen.

Andererseits erwiderte der IT-Sicherheitsexperte und bekannte Befürworter der Anonymisierungssoftware *Tor*[1], dass die vorwiegenden staatlichen Ziele sicherlich die Nichtidentifizierbarkeit staatlichen Handelns und die Totalüberwachung der Bevölkerung seien, aber so einfach umsetzen lässt sich das eben nicht, ja vielleicht niemals – siehe *Tor* und ähnliche Software, die ja auch von Polizeien und dem Bundesnachrichtendienst (BND) selbst benutzt werden, weil sie so gut funktionieren. Gibt es also vielleicht doch eine Art Gleichstand?

Der NSA-Untersuchungsausschuss des Bundestages ist ja längst zu einem NSA- und BND-Untersuchungsausschuss geworden (siehe Vortrag von Anna Biselli in diesem Heft), wodurch wir so einiges über die internen Vorgänge und Ängste erfuhren. Wir wissen jetzt, dass die drakonischen Strafen in Bezug auf „unerwünschte Computernutzung", von CFAA (Computer Fraud and Abuse Act, USA) bis StGB 202c (sogenannter *Hackerparagraph*, Deutschland) aus dieser Furcht heraus geboren sind. Diese Überreaktion hat dann sogar den US-amerikanischen Wissensfreiheitsaktivisten Aaron Schwartz[2] in den Tod getrieben.

Ungleiche Mittel

Diese vehemente Kriminalisierung unerwünschten Verhaltens findet statt, auch wenn wir – mit Jacob Appelbaums Worten – nach wie vor „experimentell im Netz unterwegs sind". Diese Schieflagen verdeutlichen die tatsächliche Sichtbarkeitsverteilung.

Transparenzparadoxon bei Infrastrukturen

Kommen wir nun zu einer gänzlich anderen Sichtweise auf den Transparenzbegriff. Betrachten wir dazu einmal das Transparenzparadoxon bei Infrastrukturen, denn die vorherige Sicht ist vielleicht zu einfach gedacht. Bestimmte Dinge wollen wir ja auch unsichtbar werden lassen, damit sichtbar wird, was dahinter liegt. Es werden also Objekte, Prozesse und Organisationen invisibilisiert, um etwas anderes sichtbar zu machen, das vorher verdeckt war. Dieses Verständnis gehört demnach in die normative Kategorie.

Setzen wir also gegen den politischen Transparenzbegriff eine zweite normative Ebene: die praktische Transparenz. Susan Leigh Star nannte dies eine *Transparenz des Nutzens*, nachzulesen in ihrem Aufsatz *Ethnography of infrastructure*. So gemeint, wird ein Wasserhahn transparent genutzt, denn er wird während seines Gebrauchs nicht verstanden oder reflektiert. Verwendete Technik wird eben dann zu Infrastruktur, wenn sie bei ihrer Verwendung nicht immer wieder neu zusammengesetzt oder durchdrungen werden muss, sondern transparent und damit unsichtbar wird. Das hat auch mit Routine zu tun, derartige Technik nennen wir *invisibly support tasks*. Nur im Fehlerfall wird Infrastruktur als solche sichtbar, aber auch der Fehlerbegriff basiert auf Zuschreibungen. In der Regel will und soll sie jedoch unsichtbar sein.

Bekannt ist diese Problematik hierzulande auch durch die Diskussion um die Sichtbarkeit von Windkraftanlagen und oberirdischen Stromleitungen. Schnell geht es dann um die „Verschandelung" von Landschaften. Unabhängig von der inhaltlichen Diskussion um diese Themen führt diese Art von Widerständen zu „kultivierter Unsichtbarkeit". In diesem Beispiel hieße das, die „Landschaft bleibt schön", z. B. durch Erdkabel. Kultivierte Unsichtbarkeit bedeutet an anderer Stelle jedoch auch, dass Unter-

nehmen sich bei Fehlern nicht rechtfertigen müssen, wenn die Probleme in unbeobachtbaren Bereichen auftreten.

Gerade die Informationstechnik ist ein Paradebeispiel für die Kultivierung der Unsichtbarkeit: Alles ist verborgen und in der Regel nur streng kontrolliert durch das *human-computer-interface* nutz- und erfahrbar. Diese Eigenschaft offenbart sich erst dann, wenn nicht alles wie erwartet funktioniert. Sehr schön kann das bei der „*mother of all demos*" (1968) nachvollzogen werden: Douglas Engelbart präsentiert darin eine der überhaupt ersten graphischen Benutzeroberflächen inklusive Computermaus, und plötzlich gibt es Fehler im Programm und es reagiert anders als erwartet. Engelbart ist absolut hilflos und fragt hilfesuchend nach einem Programmierer. Mit einem „*I haven't warmed up yet*", in etwa „ich bin noch nicht in Übung", macht er sich letztendlich zum prototypischen sich selbst für die Fehler der Maschine anklagenden User. Es braucht offensichtlich Übung, bis derartige Technik transparent nutzbar ist, so zumindest die Fehlerrationalisierung.

Verschwundene Technik

Doch die Transparenz der Technik reicht noch viel weiter. Nehmen wir das Beispiel *Google Glass*, bei dessen Funktionsdemonstrationen der Blick stets auf „schöne" Objekte gerichtet war, z. B. auf ein Baby. Der eigene Blick soll ganz natürlich sein, die Technik als Technik soll nicht mehr in den Blick kommen. Auch in der Werbung sieht man das *Glass*-Gerät niemals. Wir sprechen also von Technisierung, aber meinen eigentlich, die Visibilität der Technik herauszunehmen.

Favorit bei der Kultivierung der Unsichtbarkeit ist sicherlich Mark Weiser, der um die 1990er-Jahre am Forschungszentrum Xerox PARC forschte. Er reaktivierte den bürgerlich-romantischen Traum der „Waldwelt" für eine erstrebenswerte Mensch-Maschine-Interaktion. Dabei sollten sich die Maschinen dem Menschen anpassen, nicht andersherum. Dies vorausgesetzt, sei die Computernutzung nach Weiser stets so erfrischend wie ein Waldspaziergang. Wenn man so will, ist Weiser ein Propagandist des Erdkabels der Computerisierung. Er wünscht sich folglich, die Sichtbarkeit von Technik komplett aufzuheben – es ist dies der Wunsch nach Ganzheitlichkeit diesseits aller dinglichen Entfremdung durch Technik, nach einer selig-träumerischen unbewussten Techniknutzung.

Beobachtung im technisch Unbewussten

Kommen wir genau vor diesem Hintergrund wieder zurück zur Beobachtung. Eine wesentliche Folge des Versteckens technischer Mechanismen ist die Entstehung des technisch Unbewussten. Dieser Begriff kann gut durch ein Gegenbild erklärt werden: Jede Person kennt Kontrollen am Flughafen. In diesen Situationen ist explizit Kooperation für Kontrolle und Beobachtung nötig; es wird erwartet und vorausgesetzt, dass alle Reisenden mitmachen und sich beispielsweise für eine Abtastung richtig hinstellen oder stillhalten.

Ganz anders verhält es sich bei eher transparenter Beobachtung wie der Videoüberwachung mit Gesichtserkennung. Je transparenter Beobachtung wird, umso mehr bedarf es der Kontrolle des Raumes selbst. Es braucht „Mausefallen", damit Menschen unbewusst kooperieren. Bei Videoüberwachung wären das beispielsweise Rolltreppen, durch die Kooperation „erzwungen" wird, denn fahrend innerhalb eines definierten Bereichs kann das Gesicht sehr gut erfasst werden.

Um diese Art von Beobachtung weiterzutreiben, ist eine „*McDonaldisierung*" des Raumes nötig. Er muss vorhersehbar, berechenbar, standardisiert und kontrollierbar sein. Auch vielfältige Kontexte müssen beachtet werden, um die Nutzenden ohne ihre bewusste Mitarbeit beobachtbar zu machen. Dabei werden die Möglichkeiten der Raumbeeinflussung immer weitreichender, vom taktilen Internet bis zu cyber-physischen Systemen. In dieser kontrollierten Umgebung kann nun auch der Sicherheitsabstand zwischen Mensch und Maschine aufgehoben werden.

Steering asleep

Es lässt sich also recht treffend behaupten, wir bewegten uns schlafend oder schlafwandelnd durch die informationstechnische Infrastruktur. Doch diese Unwissenheit wird aufgrund des dadurch bedingen Kontrollverlustes der User als größte Schwachstelle dargestellt. Das technische Design wird in Folge ein paranoides, angstgetriebenes. Systeme dieser Art werden, wo es möglich ist, abgeschlossen und dann auch geschlossen gehalten. Frederick P. Brooks formulierte das in positiver Weise als „*konzeptionelle Integrität* angesichts der *Wilderness* der praktischen Welt". Im Softwaredesign sollten demnach Entwurfsentscheidungen immer konsequent umgesetzt werden, auch wenn das möglicherweise unzulässige Vereinfachungen und Verzerrungen nach sich zieht. Im Zweifel sollte also lieber einfache, aber nutzbare Software entstehen.

Diesem Ansatz entgegen steht die Sichtweise des *Maintenance and Repair*: Oberflächen werden absichtlich durchbrochen, denn das Hineinschlagen in die und das Öffnen der Technik ist nötig, um sie letztendlich besser zu machen. Dieser eher emanzipative Ansatz findet seine Ausprägung wesentlich in der Hacker- und Maker-Kultur.

Leon Hempel

Leon Hempel leitet den Forschungsbereich *Sicherheit – Risiko – Privatheit* am Zentrum für Technik und Gesellschaft (ZTG) der Technischen Universität Berlin. Er beschäftigt sich u. a. mit Beobachtungstechnologien und ihrer Geschichte, mit der Relation von Sichtbarkeit und Unsichtbarkeit im Kontext vergleichender Infrastrukturforschung sowie mit dem Thema Sicherheit und Zeit(-Bindung). Er hat zudem eine Gastprofessur für interdisziplinäre Lehre an der Technischen Universität Darmstadt inne.

Transparenz und Verantwortungsverlust

Eine weitere Anwendung des Transparenzbegriffs wurde von Barbara van Schewick entwickelt. Sie betrachtet die Transparenzebenen bezüglich des End-to-End-Prinzips des Internets. Vereinfacht gesprochen: Um Anwendungen über Netzverbindungen miteinander kommunizieren zu lassen und die Infrastruktur z. B. nur mit dem Transport zu betrauen, sind die technischen Netzwerkfunktionen des Internets in Schichten aufgeteilt. Allgemeine Funktionen wie Signalaushandlung oder Routing sind in den unteren Schichten des OSI-Netzwerk-Modells angesiedelt. Spezielle Anwendungsfunktionen sind wiederum in den oberen Schichten verortet. Van Schewick weist in ihren Arbeiten nach, dass dieses im Kern arbeitsteilige Prinzip zu dynamischer Innovation führt. Oder – um mit Bernard Stiegler zu sprechen – diese Struktur produziert eine Architektur der permanenten Innovation.

Arbeitsteilung bedeutet aber auch kognitive Unterscheidung zwischen den Agierenden des Internets. Egal auf welcher Schicht sie aktiv sind, die Verantwortlichkeiten sind – gleichlaufend zur Arbeitsteilung – ebenso verteilt. Das Resultat ist Verantwortungsdiffusion bis hin zu ihrem Verlust. Auch um diesem zu begegnen, forderte Barbara van Schewick, dass die tieferen Schichten in staatliche/öffentliche Hand gehören. Arbeitsteiligkeit ist im Grunde ein ökonomisches Prinzip.

Wir betrachteten bislang die politische Normativität des Transparenzbegriffs, die praktische Normativität des Transparenzbegriffs und zuletzt auch die ökonomische Normativität des Transparenzbegriffs. Mittlerweile ist die Beschreibung des Netzes auch nicht mehr ausschließlich in Begriffen der Technik möglich, sondern erfolgt besser primär in ökonomischen Organisationseinheiten.

Abschluss

Für alle angesprochenen Problemfelder kann hier freilich keine Lösung angeboten werden. Vielleicht aber sollte ein ganz neues Internet erdacht werden, das im Vorhinein auf bestimmte Eigenschaften überprüft wird. Sicherlich sind die nötigen theoretischen, technischen und praktischen Grundlagen dafür noch nicht hinreichend gelegt, denn man kann nur Systeme verifizieren, von denen man genau weiß, was sie tun sollen. An diese braucht es also zunächst klare Anforderungen, und auch die können wiederum Fehler enthalten. Eine ausreichend genaue Analyse ist schon bei ganz simplen SCADA-Systemen schwierig, ganz zu schweigen von komplexeren Anforderungen wie beim E-Voting. Dennoch müssen wir das angehen. Diese Überlegungen sollten jedenfalls nicht erst im Vollbetrieb angestellt werden, weil es dann für grundlegende Änderungen zu spät ist. Als nichttechnische Person kann ich daher vielleicht nur eine Bitte an die Technikerinnen und Techniker richten: Baut bitte ein neues Netz!

Zumindest muss aber die technische Featuritis zurückgefahren werden, um überschaubarere und damit nutzbarere Systeme zu schaffen.

Anmerkungen

1 *https://www.torproject.org*

2 *https://www.theguardian.com/commentisfree/2015/feb/07/aaron-swartz-suicide-internets-own-boy*

FIfF-Konferenz 2016

Sozial gerechte Algorithmen? Problematiken, theoretische Konzepte und Perspektiven der Geschlechterforschung

Zusammenfassung des Vortrags von Corinna Bath

Dass Algorithmen häufig als neutral gelten, setzt voraus, sie zunächst von ihren jeweiligen sozialen Kontexten der Entstehung und Wirkung abzutrennen. Im Vortrag möchte ich – aus der Tradition der Geschlechterforschung heraus – Unsichtbares sichtbarer machen und damit Problematiken dieses Neutralisierungstricks verdeutlichen. Im Fokus stehen Verzerrungen, die als sexistisch, rassistisch oder anderweitig ungerecht bezeichnet werden können. Zugleich geht es mir darum, ein performatives Verständnis von Algorithmen vorzustellen, welches diese Kontextualisierungen theoretisch zu fassen sucht. Ziel ist es, damit Möglichkeiten der Analyse ungerechter und der Gestaltung sozial gerechterer Algorithmen zu eröffnen.

Immer wieder wird Corinna Bath von Studierenden gefragt, warum sich die Informatik mit *Gender Studies* befasst, weil man in der Informatik doch lediglich formale Spezifikationen abarbeitet. Bath hält das jedoch für ein sehr unzutreffendes Berufsverständnis – bereits 1993 hatte sie mit Dirk Siefkes in einer Arbeitsgruppe intensiv diese Fragen diskutiert und ist zu dem Schluss gekommen: „Man kann die Informatik nicht als etwas Abgeschlossenes verstehen, das nur im technischen Raum und ohne die sozialen Kontexte steht." Nicht nur für Studierende der Informatik scheint diese Sichtweise jedoch als unnötig zu gelten – auch Professor.innen sprechen bei Forschungsprojekten noch immer von „neutraler Technik", die von ihren sozialen Kontexten losgelöst sei.

Als Bath über sexistische Algorithmen schrieb, bekam sie im Februar 2016 in der öffentlichen Debatte starken Gegenwind: Hadmut Danisch wollte ihr diesen Ansatz prinzipiell ausreden und veröffentlichte im *Focus* einen Artikel, mit dem er die „Neutralität der Algorithmen" zu retten versuchte:

Wer behaupte, Algorithmen seien „sexistisch“ und träfen sexistische Entscheidungen, habe „elementare Grundlagen der Informatik nicht verstanden und wisse nicht, was ein Algorithmus ist. Denn Algorithmen entscheiden nicht über das Ergebnis. Was ein Algorithmus als richtiges Ergebnis liefern soll, ist ihm vorgegeben. Er beschreibt, wie man das geforderte Ergebnis auf einem bestimmten Rechnertyp – möglichst effizient – berechnet, legt aber das Ergebnis nicht fest.“[1] Letztendlich ist es natürlich gleichgültig, wo genau die Ursachen dafür liegen, dass ein System automatisiert sexistische Entscheidungen erzeugt, denn offensichtlich liegen diese innerhalb der Informatik – was der Grund ist, warum diese sich damit beschäftigen muss.

Corinna Bath

Über die Rolle von Algorithmen wurde bereits Anfang der 2000er-Jahre viel diskutiert. Schon damals wurden Thesen wie die Danischs als zu kurz gedacht kritisiert und ein Paradigmenwechsel eingeleitet: Um Probleme effektiv mit dem Computer zu lösen, ist es wesentlich sinnvoller, ja sogar notwendig, die gesamte Interaktion mit den Systemen zu betrachten, statt auf der Ebene der Algorithmen zu verharren, die lediglich formalisierte Probleme lösen können.[2] Trotzdem steht auch heute wieder der Begriff des Algorithmus im Zentrum der Informatik – vor allem aber zunehmend im öffentlichen Interesse, wobei mit dem umgangssprachlichen Gebrauch des Begriffs Algorithmus auch Heuristiken, Apps, Programme und ganz allgemein technische Systeme gemeint zu sein scheinen.

Dass Geschlechterforschung allerdings auch in der Informatik von Bedeutung ist, lässt sich bereits bei der alltäglichen Verwendung des Internets beobachten, welche Vorschläge beispielsweise zur Vervollständigung einer Suchanfrage vorgeschlagen werden. 2013 machte die Kampagne *women should* von *UN Women* darauf aufmerksam, dass auf die Eingabe der Worte *women should* (dt. *Frauen sollten*) oder *women cannot* an erster Stelle klar sexistische und diskriminierende Ergänzungen vorgeschlagen werden.[3] Demnach sollten Frauen „… zuhause bleiben“, „… Sklaven sein“, „… in der Küche sein“, „… nicht in der Kirche reden“ oder es wird ergänzt: Frauen können nicht „… Auto fahren“, „… Bischof sein“ und ihnen könne nicht „… vertraut werden“.

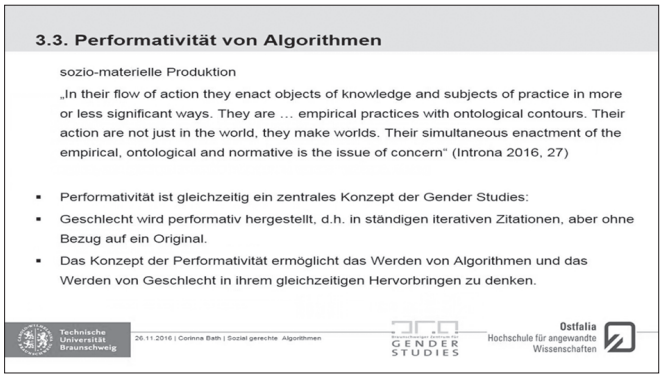
Gender Studies beschäftigt sich jedoch nicht nur mit der Kategorie *Geschlecht*, sondern versteht sich als intersektional und betreibt auch geschlechtsunabhängige Ungleichheitsforschung. Auch in dieser Hinsicht stellen sich die Ergänzungen der Suchanfragen oft als problematisch heraus. Suchte man etwa vor einiger Zeit bei der Google-Bildersuche nach *Hand*, so erschienen ausschließlich Hände mit weißer Haut. Inzwischen haben diverse Untersuchungen im Bereich Gender Studies explizit aufzeigen können, wie kritisch die Diskriminierung durch Algorithmen sein kann. Wissenschaftlerinnen und Wissenschaftler der Carnegie Mellon University konnten beispielsweise zeigen, dass Frauen bei Google weniger Anzeigen für gut bezahlte Jobs mit Führungspositionen angezeigt werden als Männern.[4] Eine Forscherin der Harvard University fand heraus, dass eine Google-Suche nach afroamerikanisch klingenden Namen diese häufiger mit Anzeigen in Zusammenhang bringt, die einen Eintrag im Vorstrafenregister implizieren.[5]

Dass zunehmend Entscheidungen automatisiert auf Basis von Algorithmen getroffenen werden, bedeutet jedoch, dass es nicht nur um die Frage der Darstellung von Inhalten, wie Suchanfragen und Bilder, geht, sondern dass auch etwa konkrete politische Entscheidungen von ihnen abhängen. Diesen Zusammenhang macht auch Cathy O‘Neil in ihrem 2016 erschienenen Buch *Weapons of Math destruction*[6] deutlich. Sie führt als Beispiel an, dass in US-amerikanischen Schulen Lehrende wegen „ungerechten“, dem gesunden Menschenverstand widersprechenden Kriterien ihren Job verloren haben. Grundlage in ihrem Beispiel waren von Algorithmen erzeugte Bewertungsmuster, die nicht noch einmal von einem Menschen überprüft wurden. Auch die Vorsortierung von Bewerbungen oder die Vergabe von Krediten und Versicherungen führt O‘Neil als Beispiele für diskriminierende, automatisiert getroffene Entscheidungen an. Sie stellt anhand verschiedener Fallbeispiele fest, dass durch solche Praktiken insbesondere die Armen ärmer werden, weniger Zugangschancen zu Jobs oder Krediten bekommen und so ein sich selbstverstärkender Prozess einsetzt, dessen Ergebnisse Entscheidungsträger als Grundlage ihrer oft folgenreichen Entscheidungen wählen.

Auch in der Wissenschaft wird über Algorithmen Geschlecht und damit Ungerechtigkeit hergestellt. Ergebnisse von Anelis Kaiser, einer Kollegin von Bath, zeigen, wie zwei verschiedene Verfahren zur Visualisierung von Gehirnaktivitäten bei gleichem Datensatz verschiedene Ergebnisse hervorbringen können: Mit einem der zwei Algorithmen ließen sich signifikante Geschlechterunterschiede feststellen, mit dem anderen jedoch nicht.[7] Folglich können sich durchaus auch ohne Intentionen, also unwissentlich und damit womöglich unbemerkt, diskriminierende Eigenschaften in Algorithmen einschleichen. Für die Geschlechterforschung ist dieses Phänomen nicht unwesentlich, wenn man davon ausgeht, dass die Zuordnung zu einem Geschlecht auch sozial hergestellt wird und ein Gehirn oder ein menschlicher Körper generell einer Plastizität unterliegt, also geformt werden kann. Um solche Phänomene wissenschaftlich zu untersuchen, muss sowohl eine sozialwissenschaftliche als auch informatische Perspektive eingenommen werden.

Die Soziologie untersucht dabei die Frage, warum wir den Algorithmen immer mehr Macht zugestehen. Lucas Introna, Soziologieprofessor der Lancaster University Management School gibt

hier eine mögliche Antwort: Algorithmen seien sehr unergründlich – man könne sie nicht direkt inspizieren. Selbst wenn man den Code lesen könne, heiße das nicht, dass man ein Gesamtverständnis erzielen kann. So werden zum Beispiel im Kontext von Big Data immer mehr Prozesse zu Black Boxes. Gleichzeitig merken wir, dass Algorithmen uns und unser Leben zunehmend konfigurieren. Lucas Introna zufolge ist die Performativität von Algorithmen das Hauptproblem. Algorithmen seien in einen Flow eingebettet, haben also ein zeitliches Element und bringen in ihrer Ausführung auch Empirisches.



Performativität ist in der Geschlechterforschung ein sehr zentraler Begriff. Hier wird Geschlecht als etwas Performatives verstanden, das immer wieder neu hergestellt werden muss. Dies geschieht in einem iterativen Zitationsprozess, aber nicht unbedingt mit Bezug auf ein Original. Wir haben keine prototypische Frau und nicht den prototypischen Mann. Nichtsdestotrotz wissen wir immer wieder, worauf wir uns beziehen, wenn wir unsere Geschlechtlichkeit im Alltag darstellen und bei anderen wahrnehmen – nämlich weil wir sie auf bestimmte (erlernte) Vorstellungen beziehen. Performativität bedeutet darüber hinaus, diesen Prozess zu verstehen als das gleichzeitige Hervorbringen von etwas. Denkt man nun Technik und Algorithmen in diesen Prozess mit hinein, so werden auch diese gleichzeitig hervorgebracht. Wir haben keine präexistierenden Subjekte als Männer und Frauen und präexistierende Algorithmen, die weiterentwickelt werden, sondern in dem Prozess des Werdens werden sowohl die Algorithmen, die Technologien als auch die Subjekte, die damit handeln, als solche hervorgebracht – als Männer und Frauen und eben auch als Technologie. Dies ist eine Grenze, die vorher noch nicht unbedingt dagewesen ist. So können Vergeschlechtlichungsprozesse von Technik noch einmal neu gedacht und begriffen werden. In den letzten Jahrzehnten, so Bath, haben wir aus dieser Erkenntnis heraus große Fortschritte gemacht, wie wir theoretisch begreifen können, was Algorithmen und Technologien sind.

Bath reicht das aber nicht aus. Als Informatikerin denkt sie immer wieder auch daran, dass gegen problematische Vergeschlechtlichungen vorgegangen werden muss. Es kann nicht nur darum gehen, zu analysieren und zu verstehen. Wir müssen einen Schritt weiter gehen und in der Informatik zur Entvergeschlechtlichung der informatischen Artefakte kommen. Aus wissenschaftlicher Sicht stellt sich dabei als erstes die Frage, wie sich dieses Problem definieren lässt – wie kann etwas Negatives – das *Ent* in Entvergeschlechtlichung – gefasst werden? Dazu ist es sinnvoll definieren zu können, was *Bias* – manchmal übersetzt mit „Vorurteile in Maschinen" – heißt. Allein darüber gibt es jedoch seit mindestens zwanzig Jahren kontroverse Diskussionen. Fruchtbar sein könnten für die Definitionsfrage darüber hinaus aktuelle Debatten über Fairness. Cynthia Dwork schrieb 2012 darüber, wie sich die Repräsentativität von bestimmten Bevölkerungsgruppen in den USA durch bestimmte Klassifikationen herstellt. Das schafft den Übergang von den eher soziologisch inspirierten Gedanken hin zu konkreten Herangehensweisen der Informatik – wie Ungerechtigkeiten und Biases ganz konkret mit Hilfe von Algorithmen gemessen und erkannt werden können bzw. wie diese mit Hilfe von Algorithmen vermieden werden können. In ihrem Paper veröffentlichte Cynthia Dwork einen „Catalog of Evil" mit Verhaltensweisen, die von Algorithmen vermieden werden sollen.

Die Forschungsliteratur zur Frage, wie Algorithmen fairer werden können, ist direkt in den Monaten vor der FIfF-Konferenz 2016 schier explodiert, berichtet Bath über ihre Vorbereitung zum Vortrag. Für sehr spezifische und sehr unterschiedliche Fälle wurde mit dem Ansatz der Performativität ausprobiert, wie diskriminierende Praktiken technisch zu vermeiden sind. In einigen Fällen geht es eher um die dem Algorithmus zugrundeliegenden Modelle, in anderen um die Daten, die eingespeist werden, z. B. bei Maschinenlernverfahren. Manche Fälle wiederum sind ganz explizit darauf ausgerichtet, dass bestimmte Menschengruppen diskriminiert werden sollen, in anderen Fällen geschieht das auch ohne Intention. Es gibt bereits einige partizipative Ansätze der Mensch-Technik-Interaktion (wie *Human Centered Design*), die bestimmten Problematiken der Vergeschlechtlichung entgegenwirken könnten. Hinsichtlich der Algorithmen sind wir aber noch in den Anfängen – hier bleibt viel zu tun. Verschiedene Ansätze der Messung und Vermeidung von Diskriminierung durch Algorithmen zusammenzubringen, um eine Methodik für kritische Technikgestaltung zu entwickeln, erscheint Bath als ein großes Vorhaben, das wissenschaftlich dringlichst auf den Weg gebracht werden muss.

Das Entwickeln praktischer Ansätze geht jedoch Hand in Hand mit einer Erhöhung der Sichtbarkeit der Problematik überhaupt. All die genannten Beispiele machen deutlich, wie wichtig es ist, sich auch bei informatischen Prozessen mit dem Einfluss von Algorithmen auf Geschlecht und andere Ungleichheitskriterien zu beschäftigen. Entscheidungsträger müssen hierfür viel mehr sensibilisiert werden. Bath ruft hierzu Journalist.innen auf, aber auch in die Lehre der Informatik müssten diese Fragen verstärkt

Corinna Bath

Corinna Bath ist derzeit Gastprofessorin für *Gender&Technik* an der TU Graz. Sie hat seit 2012 die Maria-Goeppert-Mayer-Professur für Gender, Technik und Mobilität an der TU Braunschweig inne. Als Informatikerin und Geschlechterforscherin interessiert sie sich für Vergeschlechtlichungen informatischer Artefakte wie Algorithmen und Möglichkeiten, den damit verbundenen Problematiken entgegenzuwirken.

hineingebracht werden, sodass eine gleichberechtigte Diskussion der verschiedenen beteiligten Felder auf Augenhöhe stattfinden kann: zwischen denen, die sich als Geschlechterforschungsexpert.innen verstehen, den Sozial- und Geisteswissenschaften und denjenigen, die in der Informatik zuhause sind.

Referenzen

1 *Focus 6/2016 (Februar) http://www.focus.de/magazin/archiv/politik-und-gesellschaft-sexistische-technik_id_5262519.html*

2 *Peter Wegener, http://www.wit.at/events/wegner/cacm_may97_p80-wegner.pdf*

3 *http://www.unwomen.org/en/news/stories/2013/10/women-should-ads*

4 *https://www.washingtonpost.com/news/the-intersect/wp/2015/07/06/googles-algorithm-shows-prestigious-job-ads-to-men-but-not-to-women-heres-why-that-should-worry-you/*

5 *https://www.technologyreview.com/s/510646/racism-is-poisoning-online-ad-delivery-says-harvard-professor/*

6 *Cathy O'Neil (2016): Weapons of Math Destruction, UK: Allen Lane*

7 *Anelis Kaiser et al. (2009)*

FIfF-Konferenz 2016

Funktioniert Datenschutz im Unsichtbaren?

Datenschutzgarantien, Transparenz und Intervenierbarkeit in versteckter Informationstechnik

Zusammenfassung des Vortrags von Marit Hansen

Datenschutz bedeutet nicht nur informationelle Selbstbestimmung, sondern dient auch als Korrektiv beim Machtgefälle zwischen Datenverarbeitern und betroffenen Personen. In dem Vortrag geht es um die folgenden Fragen: Kann Datenschutz in versteckter Informationstechnik überhaupt realisiert werden? Bedeutet „Privacy by Default", dass Datenschutz fest eingebaut ist und gar nicht mehr im Blickfeld der Nutzenden stehen müsste? Welche Herausforderungen bestehen angesichts einer für die Betroffenen (und sogar für so manchen Datenverarbeiter) unsichtbaren Funktionalität?

Beim Datenschutz geht es nicht um Daten, sondern um Menschen mit ihren Rechten. Damit ergeben sich bei der Gestaltung von datenschutzfreundlichen Systemen zwei Prüffragen: Welche Auswirkungen hat das System und seine Datenverarbeitung auf Menschen und welche Auswirkungen hat das System und seine Datenverarbeitung auf die Gesellschaft? Die Notwendigkeit des Datenschutzes ergibt sich dabei aus dem Machtgefälle, wichtig ist die Perspektive der Betroffenen. Der Ansatzpunkt des Datenschutzes, um die Menschen zu schützen, sind die personenbezogenen Daten, die durch IT-Systeme verarbeitet werden.

Die klassische Perspektive der IT-Sicherheit sind zwei Personen, die miteinander kommunizieren wollen: häufig Alice und Bob genannt. Bei ihrer Kommunikation werden sie von einer dritten Person – z. B. Eve oder Mallory – bedroht. Der Datenschutz nimmt hier eine neue Sicht ein: Sendet Alice Daten an Bob, so kann auch dieser als Angreifer fungieren, der Datenschutz muss Alice auch vor ihm schützen. Die Datenverarbeitung ist ein potenzieller „Eingreifer", die in Grundrechte (von Alice) eingreift.

Rechtlich wird der Datenschutz durch zwei Grundrechte geschützt, die das Bundesverfassungsgericht aus Artikeln des Grundgesetzes abgeleitet hat: dem Recht auf informationelle Selbstbestimmung und dem sogenannten IT-Grundrecht:

- Datenschutz-Grundrecht 1: „Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen" (informationelle Selbstbestimmung). Aus Anlass der Volkszählung urteilte das Bundesverfassungsgericht am 15. Dezember 1983, dass jeder wissen können soll, wer was über ihn weiß (1 BvR 65/1).

- Datenschutz-Grundrecht 2: „Recht auf Gewährleistung der Vertraulichkeit und der Integrität informationstechnischer Systeme". Zur Online-Durchsuchung urteilte das Bundesverfassungsgericht am 27. Februar 2008, dass es ein Grundrecht gibt auf digitale Intimsphäre und damit präventive staatliche Zugriffe nur bei tatsächlichen Anhaltspunkten einer konkreten Gefahr für ein überragend wichtiges Rechtsgut zulässig sind (1 BvR 37/07, 1 BvR 595/07).

Marit Hansen

Der Datenschutz legt mehrere Grundsätze fest, die bei der Verarbeitung personenbezogener Daten gelten:

- Existenz einer Rechtsgrundlage, in Form einer gesetzlichen Grundlage oder der Einwilligung des Betroffenen

- Zweckbindung
- Erforderlichkeit
- Transparenz
- Betroffenenrechte
- Datensicherheit

Der Datenschutz zielt auf die Sicherheit personenbezogener Daten. Zu den klassischen Schutzzielen der IT-Sicherheit (die durch weitere Schutzziele ergänzt werden können)

- Vertraulichkeit
- Verfügbarkeit
- Integrität

kommen die zusätzlichen Schutzziele des Datenschutzes

- Nicht-Verkettbarkeit
- Intervenierbarkeit
- Transparenz
- Datensparsamkeit

In der heutigen Realität haben wir es mit einigen dominierenden Anbietern zu tun, die in allen Lebenslagen hinter Datenverarbeitungsprozessen stehen können. In Teilen sind diese Anbieter unsichtbar bzw. nicht wahrnehmbar oder unbekannt. Während Anbieter wie PayPal, Apple, Microsoft, Twitter, Amazon, Google, Facebook weithin bekannt sein dürften, sind beispielsweise Anbieter von IT-Infrastruktur wie Akamai möglicherweise vielen Nutzern unbekannt. Es stellen sich Fragen danach, wo und wann die Verarbeitung der Daten stattfindet, wie genau die Datenverarbeitung durchgeführt wird und durch welche Dritten auf die Daten zugegriffen wird.

In der heutigen Realität ist die Datenverarbeitung durch eine komplexe Arbeitsteilung geprägt. Die Endanwender.in, die (vermeintlich) auf eine Webseite zugreift, löst dadurch den Zugriff auf weitere Seiten, häufig sogar hunderte von weiteren Zugriffen aus, die im Hintergrund, also versteckt, stattfinden. Die unsichtbare (und unerwartete) massenhafte Einbindung von Dienstleistern führt zu Sicherheits- und Datenschutzrisiken, es stellt sich die Frage nach der Transparenz der Datenverarbeitung. Selbst wenn der Anwender.in diese Zugriffe im Hintergrund bewusst sind, ist die Praktikabilität von Interventionen angesichts der Menge von Zugriffen zweifelhaft. Zuletzt stellt sich die Frage nach der Verantwortung. Es bleibt festzuhalten, dass es in der heutigen Realität eine massive Marketing-Macht für (unsichtbare) Integration in Angebote gibt. Die Anzahl der Anbieter solcher Dienste ist nicht mehr überschaubar (Quelle: chiefmartec.com Marketing Technology Landscape).

Die Komplexität heutiger Geschäftsprozesse wird häufig in der Cloud verborgen. Neben der (scheinbaren) Vereinfachung ergeben sich dabei neue Fragestellungen: man begibt sich in eine Abhängigkeit von Dienstleistern, die die Cloud-Dienste anbieten, Fremdbestimmbarkeit tritt an die Stelle von Eigenkontrolle und auch hier stellt sich die Frage: „Durch welche Dritten wird auf meine Daten zugegriffen?“

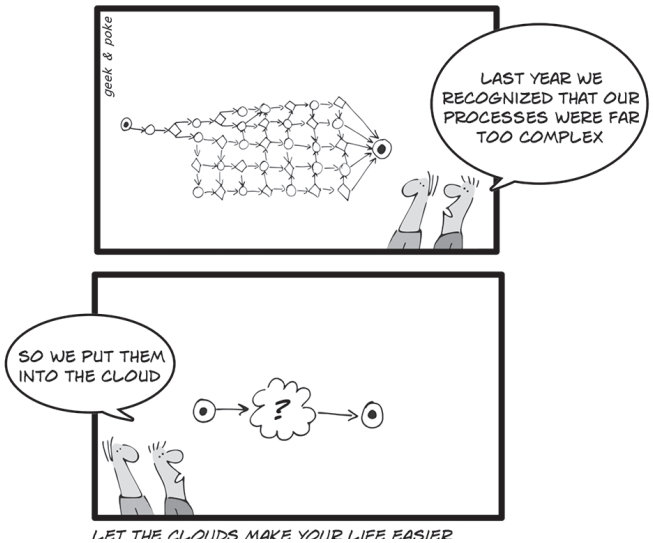
Dazu kommt in der heutigen Realität das „versteckte“ Internet: Internetanbindung zu Hause (im *Smart Home*), im Auto und am Körper (durch *Smart Watches* und Smartphone-Apps). Das Beispiel der Smart-TVs von Samsung ging vor einiger Zeit durch die Medien, wo es in den Bedienungshinweisen heißt:

> *„Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition“ (Samsung Smart TVs Do Not Monitor Living Room Conversations, http://global.samsungtomorrow.com/samsung-smart-tvs-do-not-monitor-living-room-conversations/).*

Samsung trat der Aussage entgegen, dass durch seine Fernsehgeräte die Wohnungen der Nutzer.innen ausgespäht würden.

Die „unsichtbare“ Datenverarbeitung im Smart Home ist auch nicht immer für jeden unsichtbar: Dem „Betreiber“ des Systems, z. B. dem Haushaltsvorstand, Vermieter oder Arbeitgeber sollte bekannt sein, dass im Hintergrund Daten erfasst werden und er ist verpflichtet, Mitnutzer unverzüglich zu warnen. Dies ist nicht neu und gilt schon immer für TK-Anlagen mit Einzelverbindungsnachweis:

> *„[…] Bei Anschlüssen im Haushalt ist die Mitteilung nur zulässig, wenn der Teilnehmer in Textform erklärt hat, dass er alle zum Haushalt gehörenden Mitbenutzer des Anschlusses darüber informiert hat und künftige Mitbenutzer unverzüglich darüber informieren wird, dass ihm die Verkehrsdaten zur Erteilung des Nachweises bekannt gegeben werden.*
>
> *Bei Anschlüssen in Betrieben und Behörden ist die Mitteilung nur zulässig, wenn der Teilnehmer in Textform erklärt hat, dass die Mitarbeiter informiert worden sind und künftige Mitarbeiter unverzüglich informiert werden und dass der Betriebsrat oder die Personalvertretung entsprechend den gesetzlichen Vorschriften beteiligt worden ist oder eine solche Beteiligung nicht erforderlich ist. […]“ (§99 Abs. 1 TKG).*



Oliver Widder, CC BY 3.0, http://geek-and-poke.com/something/

Auch die Nutzungsbedingungen von – beispielsweise – WhatsApp verlangen eine Bestätigung, dass Daten nur mit entsprechendem Einverständnis der Betroffenen weitergegeben werden:

> *„Du stellst uns regelmäßig die Telefonnummern von WhatsApp-Nutzern und deinen sonstigen Kontakten in deinem Mobiltelefon-Adressbuch zur Verfügung. Du bestätigst, dass Du autorisiert bist, uns solche Telefonnummern zur Verfügung zu stellen, damit wir unsere Dienste anbieten können"*
> *(https://www.whatsapp.com/legal/?l=de#terms-of-service).*

Doch nicht nur der Datenabfluss kann kritisch sein, auch die Fremdbeeinflussung, z. B. das Stilllegen von Fahrzeugen bei nicht rechtzeitig bezahlten Raten (während der Fahrt auf der Autobahn: „*Terrified driver almost crashes when loan company hit ‚kill switch' for missing repayments*", Mirror, *http://www.mirror.co.uk/news/technology-science/terrified-driver-crashes-car-loan-4325955*) oder die Fremdbeeinflussung des Weges bei Navigationsgeräten. Auch Sicherheitsbehörden träumen von solchen Möglichkeiten: „*I want to remotely disable Londoner's cars, says Met's top cop*" (The Register, *http://www.theregister.co.uk/2016/09/22/met_police_commissioner_i_want_remotely_kill_car_electronics/*).

Gerade bei Smart Homes wird man sich auch neue Gedanken über das Human Computer Interface (HCI) machen müssen – auch im Hinblick auf Datenschutzfunktionen. Die Komplexität dieser Systeme sollte verringert werden, auch die „historisch gewachsene".

In der Praxis der Entwicklung zeigt sich allerdings häufig, dass für den Fortschritt andere Prioritäten gesetzt werden. Das World Wide Web wurde ohne Berücksichtigung der Sicherheit entwickelt; dieses Vorgehen wird von Tim Berners-Lee verteidigt: Zielsetzung bei der Entwicklung war „ … *a platform that developers would find familiar and easy to use. Baking in security at that point might have worked against that goal …* " (The Register, http://www.theregister.co.uk/2014/10/08/sir_tim_bernerslee_defends_decision_not_to_bake_security_into_www/). Einen anderen Standpunkt hat heute Vint Cerf: „ … *Vint Cerf … regretted not building in security to basic internet protocols.*" Fest steht, dass Sicherheit (und Datenschutz) bei der Entwicklung als nachrangig eingestuft wurden.

Der Ansatz, ein Verständnis der Sicherheit von Systemen durch Reverse Engineering zu erzielen, ist in der Praxis mit Problemen behaftet: er ist nur für wenige Experten realistisch, es gibt dafür rechtliche Einschränkungen und auch dadurch sind die Systeme nicht vollständig verstehbar. Viktor Mayer-Schönberger erwartet: „Wir glauben, dass sich eine eigene Kaste von Experten entwickeln wird, die Algorithmiker" (Zeit Online 2013/09). Diese sollen die Systeme durchschauen. Die Forderung nach Open Source reicht dafür aber nicht!

Die neue gesetzliche Grundlage für den Datenschutz ist die Europäische Datenschutz-Grundverordnung mit den Prinzipien

- Marktortprinzip (Art. 3 – d. h. auch für außereuropäische Player mit Datenverarbeitung in der EU)

- Signifikante Sanktionen (Art. 83, 84)

- Insbesondere:
  1. Adäquater Umgang mit Risiken (Art. 24, 25, 32, 35, 36)
  2. Datenschutz durch Technikgestaltung (Art. 25, Sicherheit: Art. 32)
  3. Datenschutz durch datenschutzfreundliche Voreinstellungen (Art. 25)
  4. Transparenz für die betroffenen Personen (Art. 5, 12–15, 19, 22, 30, 33)
  5. Intervenierbarkeit für die betroffenen Personen (Art. 5, 7, 8, 16–18, 20, 21)
  6. Verantwortung des für die Verarbeitung Verantwortlichen (Art. 6 II, 24)

- Adressat ist dabei der Datenverarbeiter (Betreiber, Auftragnehmer, u. U. auch Privatpersonen; nicht unmittelbar Hersteller)

Ziel der Verordnung ist der Schutz der Rechte und Freiheiten natürlicher Personen.

Ein wesentlicher Aspekt ist die Transparenz, also die Verständlichkeit der Datenverarbeitung. Die Verordnung schreibt dafür eigentlich den Grundsatz der fairen und transparenten Datenverarbeitung vor. Es sind aber Ausnahmen möglich: Im Ermessen des Verantwortlichen kann die Information der Betroffenen unterbleiben, wenn „die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde" (Art. 14 Abs. 5 lit. b DS-GVO). Dies wirft die Frage nach Anwendungen auf, die Big-Data-Techniken nutzen oder nach Anwendungen des Ubiquitous Computing. Zu fragen ist auch, wie die Informationen über die Datennutzung zum Betroffenen gelangen sollen.

Marit Hansen

Marit Hansen ist seit 2015 die Landesbeauftragte für Datenschutz Schleswig-Holstein und leitet das Unabhängige Landeszentrum für Datenschutz (ULD). Davor war die Diplom-Informatikerin sieben Jahre lang stellvertretende Landesbeauftragte für Datenschutz. Im ULD hat sie den Bereich der Projekte für technischen Datenschutz und das Innovationszentrum Datenschutz & Datensicherheit (ULD-i) aufgebaut. Seit 1995 arbeitet sie zu Themen des Datenschutzes und der Informationssicherheit. Ihr Schwerpunkt liegt auf der grundrechtskonformen Gestaltung von Systemen, insbesondere durch Privacy by Design und Privacy by Default.

Für mehr Transparenz gibt es bereits Vorschläge: Nutzung einer klaren und einfachen Sprache für die Information der Betroffenen, Aufbau der Datenschutz-Policies in mehreren Ebenen (*layered policies*), durch standardisierte Bildsymbole (vgl. Art. 12 Abs. 7 DS-GVO) und in maschinenlesbarer Form. Auch für die Unterstützung der Selbstbestimmung gibt es Vorschläge:

- Datensparsamkeit und Privacy by Design als Grundprinzip [stark unter Beschuss von Politik und Wirtschaft, Gegenbegriffe: Datenreichtum, Datensouveränität]
- Binden der akzeptierten Verarbeitungsregeln an die Daten (z. B. Sticky Policies) [dabei sind aber Seiteneffekte zu beachten]
- Assistenten Technik/Menschen/Organisationen [das erfordert ein Vertrauensmodell!]
- Adäquate HCI

Art. 25 der EU-Datenschutz-Grundverordnung fordert Datenschutz by Design & by Default. Diese Forderung richtet sich primär an Datenverarbeiter (auch im Auftrag) und (nur indirekt) an die Hersteller von IT-Systemen. Ziel dabei ist die Gestaltung von Systemen und Diensten von Anfang an über den gesamten Lebenszyklus: Diese müssen datensparsam und mit möglichst datenschutzfreundlichen Voreinstellungen versehen sein:

> *„(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.*
>
> *(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen" (Art. 25 EU-DSGVO).*

Erwägungsgrund 78 der Verordnung fordert zu Datenschutz by Design & by Default Folgendes:

- Nachweis durch interne Strategien und technische und organisatorische Maßnahmen, u. a.:
  1. Datenminimierung
  2. schnellstmögliche Pseudonymisierung
  3. Transparenz in Bezug auf Funktionen und Verarbeitung
  4. Ermöglichung der Überwachung der Verarbeitung durch den Betroffenen
  5. Ermöglichung für Sicherheitsfunktionen *on top* durch Verantwortlichen
- Hersteller sollten zur Berücksichtigung des Rechts auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen ermutigt werden.
- Die Grundsätze sollten in öffentlichen Ausschreibungen berücksichtigt werden.

Zusätzlich zum Datenschutz sind die Grundsätze des Verbraucherschutzes zu beachten: Anforderung an eine gültige Einwilligung nach Datenschutzrecht ist, dass sie bewusst, informiert und freiwillig gegeben wird. Eine AGB-Vertragsklausel kann eingeschränkt gültig oder unwirksam sein, weil die AGB-Bestimmung unklar ist, die AGB-Bestimmung überraschend ist oder die AGB-Bestimmung den Kunden unangemessen benachteiligt. Frage ist: Wieviel ist dem Betroffenen zuzumuten?

Fazit

Informationelle Selbstbestimmung ist schon immer mehr Ziel als Realität. Bei versteckter Informationstechnik ist eine Selbstbestimmung im Einzelfall praktisch nicht möglich. Feingranulare Abfragen oder Konfigurationen sind zeitintensiv und anspruchsvoll, für die meisten unzumutbar. Die Umsetzung muss auf eine Weise geschehen, die analog zur Einwilligung in die Organspende oder zur Patientenverfügung ist.

Garantien durch eingebauten Datenschutz sind aber möglich: beispielsweise durch Privacy by design & by default. Der Default ist aber häufig nur der Startpunkt, von dem danach wieder abgewichen werden kann. Das Maß des technisch umgesetzten Datenschutzes hängt in der Praxis auch von der Anwendungssituation ab – *One size fits all* ist in vielen Bereichen nicht realistisch.

Die Realität der heutigen Informationstechnik und Informationsgesellschaft ist vom Datenschutz-Optimum – und sogar vom Akzeptablen – weit entfernt. Lösungen müssen sichtbarer werden, für Hersteller, Betreiber, Nutzer und Datenschutzbehörden; auch über die Community-Grenzen hinaus. Die Diskussion von Seiteneffekten und Technikfolgen ist nötig. Und zuletzt: Datenschützer.innen müssen sichtbarer werden.

Die weitgehend verborgene Entwicklung autonomer Waffen

Zusammenfassung des Vortrags von Hans-Jörg Kreowski

In den Waffenschmieden und Denkfabriken der NATO und sicher auch darüber hinaus findet seit einigen Jahren eine weitgehend vor der Öffentlichkeit verborgene Entwicklung autonomer Waffen statt. Sie sollen so programmiert werden, dass sie in der Luft, auf dem Boden, auf und unter Wasser eigenständig Ziele finden und zerstören können. Insbesondere sollen sie selbständig über Leben und Tod entscheiden können. In dem Vortrag geht der Autor auf den Stand der Technik, auf die technischen Herausforderungen autonomer Systeme und auf die Perversität des autonomen Tötens ein.

Der Vortrag befasste sich mit zwei Publikationen, die sich aus militärischer Sicht mit autonomen Waffen beschäftigen. Waffensysteme wie *Reaper*, *Predator*, *Swordfish*, *Talon SWORD* und *Protector* sind heute genutzte, unbemannte, aber nicht autonome Waffensysteme. Das Ziel ist es, vergleichbare Waffensysteme zu entwickeln, die autonom operieren.

Unmanned Systems Integrated Roadmap

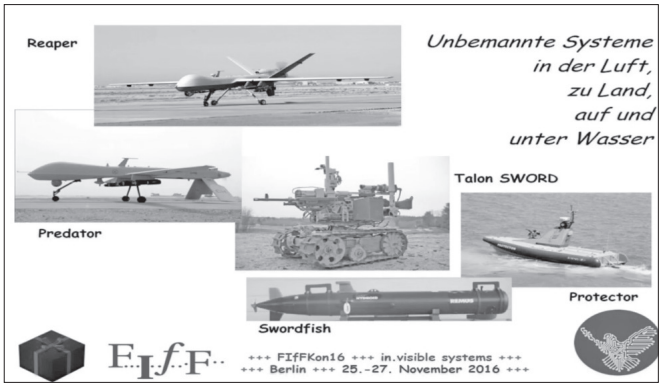
Das erste der behandelten Bücher ist der 160 Seiten starke Band *Unmanned Systems Integrated Roadmap*. Er erschien 2013 und schreibt die Entwicklung und Planung unbemannter und autonomer Waffen für 25 Jahre, bis 2038, fort. Die USA planen, einen erheblichen Teil ihrer Bewaffnung auf autonome Waffen umzustellen, und sehen dafür Ausgaben von 3–5 Mrd. US$ pro Jahr vor.

Was macht unbemannte Systeme für Politik und Militär interessant? Die Stichworte dafür sind „*dull – dirty – dangerous*“:

- *Dull:* Unbemannte Waffensysteme sind im Gegensatz zum Menschen in der Lage, über einen großen Zeitraum zu beobachten, ohne zu ermüden, abgelenkt zu werden, auf dumme Gedanken zu kommen oder sich zu langweilen.

- *Dirty:* Sie sollen weitgehend unbeschadet in einem biologisch, chemisch oder nuklear verseuchten Gebiet agieren können (wobei zweifelhaft ist, ob das auch für atomar verstrahlte Gebiete gilt).

- *Dangerous:* Sie können ohne Bedenken einer gefährlichen Situation ausgesetzt werden – im Verlustfall entsteht höchstens „Blechschaden“.



Für den Gegner bleibt es aber lebensgefährlich. Militärische Gefahren werden dadurch auch verlagert, z. B. wenn sich der Gegner durch Selbstmordattentate in anderen Gebieten zur Wehr setzt.

Was macht unbemannte Systeme für Politik und Militär interessant? Ein wesentlicher Aspekt ist Geld: Die USA wollen ihre militärische Überlegenheit trotz knapper Kassen wahren. Unbemannte Systeme sind kleiner, leichter, weniger gepanzert als entsprechende bemannte Systeme und deshalb billiger. Gleichzeitig folgen andere dem US-amerikanischen Beispiel der Entwicklung unbemannter Waffensysteme. Ein gigantisches Wettrüsten ist deswegen entbrannt. Dennoch herrschen in den USA weiterhin Allmachts- und Weltbeherrschungsphantasien; weitere Überlegenheit kann nur durch massive Aufrüstung erreicht werden. An den zugrundeliegenden Technologien ist die Informatik stark beteiligt. Kapitel 4 der Roadmap, *Technologies for Unmanned Systems*, das sich auf 50 Seiten mit bestehenden technologischen Lücken und offenen Forschungsfragen auseinandersetzt, identifiziert sechs Problembereiche:

- Interoperability and Modularity
- Communication Systems, Spectrum and Resilience
- Security: Research and Intelligence/Technology Protection (RITP)
- Persistent Resilience
- Autonomy and Cognitive Behavior
- Weaponry

Hier ist vor allem der fünfte Punkt der Aufzählung wichtig: *Autonomy and Cognitive Behavior*. Da vor allem Personalkosten das Budget des *U.S. Department of Defense* belasten, hat die Entwicklung autonomer Waffensysteme höchste Priorität. Autonomie bedeutet dabei, dass die Systeme selbst die Signifikanz der gesammelten Informationen erkennen und eigenständig über weitere Aktionen entscheiden, ohne dass Menschen direkt eingreifen.

Autonomous Systems – Issues for Defence Policymakers

Der zweite behandelte Band ist eine Veröffentlichung der NATO, ein 321-seitiger Sammelband, 2015 erschienen, mit Autorinnen und Autoren aus Militär, Wirtschaft und Wissenschaft. Er gliedert sich in vier Abschnitte und ein Nachwort:

Part 1: Introduction (60 Seiten)

Die Herausgeber beschreiben in der Einleitung Herausforderungen und Möglichkeiten autonomer Waffen einschließlich der Charakterisierung autonomer Systeme. Sie definieren autonome Systeme als Systeme, die auf der Basis integrierter Sensorik, Analytik, Kommunikationsmöglichkeit, Planung und Entscheidung agieren, um vorgegebene Ziele zu erreichen. Spezielles Charakteristikum autonomer Systeme ist, dass sie das in sich ändernder Umgebung mit potenziellem Nichtdeterminismus tun. In jeder gegebenen Situation kann es mehrere Handlungsoptionen geben, aus denen ausgewählt werden muss.

Part 2: Ethical, Legal, and Policy Perspectives (85 Seiten)

Die Anwendung und Einhaltung des Kriegsvölkerrechts muss beim Einsatz autonomer Waffen sichergestellt werden, sonst wären die Operationen Kriegsverbrechen. Militärische Entwicklungen haben eine Beziehung zu zivilen Entwicklungen, aus der zivilen Entwicklung autonomer Systeme wird für die militärische Entwicklung gelernt.

Part 3: Autonomous Systems and Operational Risk (80 Seiten)

Wichtig ist die Sicherstellung menschlicher Kontrolle. Das Autonomie-Level muss so gewählt werden, dass Menschen trotz autonomem Operieren letztendlich die Kontrolle behalten. Diese Systeme dürfen nicht außer Kontrolle geraten, damit ist immer ein möglichst niedriges Level an Autonomie sicherzustellen. Das erfordert prüffähige Strategien (die Forderung dabei ist: Überwachung muss möglich sein).

Part 4: Perspectives on Implementing Autonomy in Systems (90 Seiten)

Im Gefecht müssen (menschliche) Soldaten und autonome Waffen miteinander interagieren. Bei dieser Interaktion treten Schwierigkeiten auf, die zu berücksichtigen sind. Agenten-basierte Simulation wird vorgeschlagen, um autonome Waffensysteme zu testen – es ist aber fraglich, ob dies für die Beurteilung der korrekten Funktion ausreicht.

Für die Navigation in unbekannten Umgebungen sind vor allem optische Sensoren wichtig, die die Umgebung erfassen können. Doch bereits 1983, in der *Strategic Computing Initiative* der USA, finanziert mit 500 Mio. US$, war die Entwicklung autonomer Fahrzeuge eine der zentralen Forderungen. Die zugrundeliegende Problematik ist heute, nach über 30 Jahren, immer noch nicht gelöst.

Afterword (4 Seiten)

Das nur vier Seiten lange Nachwort enthält eine Forschungsagenda für die NATO, die vom *NATO Chief Scientist* Major-General Husniaux geschrieben wurde und besonders interessant ist.

Er benennt die Wissenschafts- und Technologieprioritäten der NATO, um Autonomie zu erreichen:

- advanced human performance
- cultural, social & organisational behaviours
- data collection & processing
- information analysis & decision support
- communications & networks
- power & energy
- advanced system concepts

Einer der wichtigsten Punkte dabei: die Systeme brauchen Energie, die heute übliche Energiespeichertechnik reicht für den Bedarf nicht aus. Doch auch *soft factors* spielen eine Rolle: Soldaten brauchen eine neue Einstellung, die Performanz muss verbessert werden. Kulturelle, organisatorische und soziale Aspekte müssen im militärischen Bereich neu gedacht werden.

Der Abschnitt schließt mit einem Zitat von *Theodore von Kármán*:

> *„Scientific results cannot be used efficiently by soldiers who have no understanding for them, and scientists cannot produce results useful for warfare without an understanding of the operations."*

Kritik

Die Kritik beginnt mit der Frage: Was ist Autonomie?

In der Wissenschaft wird immer auf die Autonomie von Menschen verwiesen, es geht um Entscheidungen für unser menschliches Handeln. Doch heute ist in der Biologie bekannt: Auch Tiere sind in der Lage, autonom zu handeln, Pflanzen können es in bestimmtem Umfang auch; die Mechanismen der Autonomie in der Natur sind uns aber weitgehend unbekannt.

In der Technik agieren Roboter, Systeme, Prozesse autonom; die Mechanismen sind vom Menschen gemacht – vorgedacht und programmiert –, im Rahmen des algorithmisch Möglichen.

Hans-Jörg Kreowski

Hans-Jörg Kreowski ist Professor (i.R.) für Theoretische Informatik an der Universität Bremen und Vorstandsmitglied des *Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung*. Neben seinen fachlichen Schwerpunkten hat er seit vielen Jahren auch immer wieder zur unheilvollen Verflechtung von Informatik und Rüstung in Wort und Schrift Stellung genommen.

Mit autonomen unbemannten Waffensystemen überlässt man die Entscheidung über Leben und Tod autonomen Maschinen. Daraus ergeben sich Fragen:

- Ist es verantwortbar?
- Darf das sein?
- Ist das ethisch vertretbar?
- Können Maschinen das Kriegsvölkerrecht beachten?

Beide Bücher sagen zur letzten Frage: Ja, das können sie. Maschinen können das Kriegsvölkerrecht beachten.

Die Antwort Hans-Jörg Kreowskis dagegen ist: Nein.

Ein autonomes Waffensystem führt programmierte Planungs- und Entscheidungsalgorithmen aus. Programmsysteme sind fast immer fehlerhaft, bei Entscheidung und Planung sind Fehler nahezu zwangsläufig. Planungs- und Entscheidungsprobleme sind meist NP-schwer, d. h. es sind keine effizienten Lösungen bekannt, sondern nur näherungsweise und heuristische. Können wir *näherungsweises* und *heuristisches* Töten akzeptieren? *Fehlerhaftes* Töten würde damit in Kauf genommen.

Testen, Validieren, Simulieren und Verifizieren der Systeme ist nötig, man braucht aber immer ein Vergleichsmodell. Das Wissen über die Modellierung von Autonomie ist unterentwickelt; es ist noch nicht einmal vollständig klar, was Autonomie überhaupt ist. Letztlich werden auch „autonome" Entscheidungen von Menschen gemacht, der Eingriff der Menschen ist nur zeitlich vorverlegt (und damit noch viel weniger beherrschbar).

Die Genfer Konvention und vergleichbare Bestimmungen sind Gesetzestexte, die keine eindeutigen Interpretationen besitzen, auch nicht vollständig und widerspruchsfrei sind. Ethik ist nicht berechen- und programmierbar. (Was allerdings Politik, Wissenschaft und Wirtschaft nicht aufhalten wird, es zu versuchen, wenn wir es nicht schaffen, dies zu verhindern.) Maschinen mit Entscheidungsverfahren über Tod und Leben auszustatten, ist abgründig und pervers, weil sie weder technisch einwandfrei funktionieren noch ethische Anforderungen erfüllen können. Fazit: Es ist weder ethisch noch technisch möglich, solche Waffensysteme zu bauen, die nach den Regeln des Kriegsvölkerrechts operieren.

Gegenentwurf

Es gibt verschiedene Initiativen gegen unbemannte und autonome Waffen:

- Weltweiter Aufruf zum Bann autonomer Waffen: *Autonomous Weapons: an Open Letter from AI & Robotics Researchers*. Bisher wurden 20806 Unterschriften gesammelt, davon rund 3000 von AI- und Robotik-Fachleuten (Stand November 2016).

- International Committee for Robot Arms Control (ICRAC).

- Kampagne Stopp Ramstein: Kein Drohnenkrieg!

Hans-Jörg Kreowski

- Cyberpeace-Kampagne des FIfF, unter anderem mit den Ausgaben der FIfF-Kommunikation *1/2014 – Schwerpunkt Cyberpeace* und *3/2015 – Schwerpunkt Rüstung und Informatik*.

Der Vortrag schloss mit einem Zitat von Albert Einstein:

„Das Denken der Zukunft muss Kriege unmöglich machen."

Diskussion

Bei der anschließenden Diskussion wurden folgende Aspekte angesprochen:

- Wichtig ist zusätzlich der Aspekt der Verantwortung: Wer hat die Entscheidung getroffen, durch die die Ereigniskette in Gang gesetzt wurde?

- Ist die Problematik vollkommen neu? Beispiel Landminen: Keiner kann letztlich beeinflussen, ob ein Soldat oder ein Kind davon getroffen wird; damit ist auch keiner für diese *Entscheidung* verantwortlich. Minen sind aber passive Waffen; autonome Waffen suchen sich ihre Ziele selbständig, deswegen haben sie eine andere Qualität. Landminen sind bereits verboten, es gibt politische Initiativen, auch autonome Waffensysteme zu verbieten.

- Es gibt das Problem der Asymmetrie: der Angegriffene hat keine Möglichkeit, gegen den Angreifer anzugehen, nur die Maschine kann zerstört werden. Eine „asymmetrische" Antwort auf Angriffe mit unbemannten Waffen sind z. B. Selbstmordattentate.

- Es mangelt an Vertrauen in die „guten" Intentionen der Hersteller autonomer Waffensysteme. Vergleichbar mit dem Abgasskandal kann ein „Genfer-Konventions-Modul" abgeschaltet werden, es kann am ernsthaften Bemühen fehlen, Ethik in die Systeme zu integrieren.

- Es stellt sich die Frage, wie kontrolliert werden kann, ob andere Staaten ebenfalls solche Waffen bauen – diese Kontrolle ist evtl. nicht möglich. Die USA machen Pläne öffent-

lich (zumindest teilweise), viele andere tun das nicht. Die Waffen sind vergleichsweise billig und leicht zu bauen; das führt zu einer Rüstungsspirale. Durch internationale Verträge wird heute auf biologische und chemische Waffen verzichtet; dieser Versuch sollte auch bei autonomen Waffen gemacht werden.

- Das Problem am autonomen Waffensystem ist, dass es ein Waffensystem ist, nicht dass es autonom ist. Dennoch ist es für Informatiker.innen wichtig, sich klar zu machen, was sie in ihrer Arbeit tun. Die Informatik darf als Disziplin nicht missbraucht werden.

- Es ist eine neue Qualität autonomer Systeme, dass sie sich verselbständigen und autonom weiterentwickeln können; evtl. können sie im Gegensatz zu normalen Waffen auch nicht mehr deaktiviert werden. Zumindest die Energie kann ihnen jedoch entzogen werden; es ist skeptisch zu beurteilen, ob solche Systeme wirklich im menschlichen Sinne intelligent werden können.

- Größte Gefahr ist, dass Entscheidungen irgendwann nicht mehr nachvollziehbar sind, dass nicht mehr klar ist, ob der Mensch den Krieg begonnen hat oder die Maschine.

- Programmierer sind verantwortlich für die von ihnen produzierten Systeme. Doch auch diejenigen tragen eine Verantwortung für die Folgen, die unbegründete Theorien von der Möglichkeit einer Maschinenethik in die Welt setzen.

FIfF-Konferenz 2016

Die neue Globalisierung – wenn das Inland zum Ausland wird

Zusammenfassung des Vortrags von Klaus Landefeld

Was hat die Klage gegen den BND wegen Überwachung am Internetknoten DE-CIX mit der BND-Reform nach dem Beschluss zur Ausland-Ausland-Fernmeldeaufklärung zu tun? Sehr, sehr viel – darum ging es im Beitrag von Klaus Landefeld.

Klaus Landefeld leitete seinen Vortrag mit einem Zitat des Bundesverfassungsgerichts ein, in dem es deutlich machte, dass Überwachung nicht in Einklang zu bringen ist mit der verfassungsrechtlichen Identität der Bundesrepublik Deutschland:

> *„Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss." (BVerfG, 2010)*

Ähnlich sieht es der Europäische Gerichtshof (EuGH); er betont:

> *„Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert werden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren." (EuGH, 2014)*

Anders sieht es Bundesinnenminister Thomas de Maizière:

> *„Es ist nicht Aufgabe des Gerichts, ständig dem Gesetzgeber in Sachen Sicherheit in den Arm zu fallen." (Bundesinnenminister Thomas de Maizière, 2016)*

Landefeld unterschied zwischen zwei Kategorien der Fernmeldeüberwachung: Gezielte behördliche Maßnahmen, die unmittelbar auf einzelne Personen zielen, und ungezielte Maßnahmen, die die übergreifende strategische Überwachung zum Ziel haben. Zur ersten Kategorie zählt er anbietergestützte Maßnahmen nach § 110ff. TKG – Quellen-TKÜ, Vorratsdatenspeicherung, Funkzellenabfrage, Bestandsdatenauskunft und Online-Durchsuchung; Maßnahmen im Rahmen des G10-Gesetzes im Inland. Zu den strategischen Maßnahmen zählen die Maßnahmen nach G10-Gesetz mit Auslandsbezug (§ 5 G10-Gesetz): z. B. Ausland-Ausland-Fernmeldeüberwachung und Überwachung durch den Verfassungsschutz, um „Cyberbedrohungen" im Inland zu erkennen.

Klaus Landefeld

Seit den Enthüllungen durch Edward Snowden wurden die Überwachungsbefugnisse durch mehrere Gesetzesinitiativen systematisch ausgeweitet:

- Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 20.11.2015

- Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10.12.2015
- Gesetz zur Ausland-Ausland-Fernmeldeaufklärung vom 21.10.2016

Aus Sicht der Sicherheitsbehörden ist diese Ausweitung der Überwachung erforderlich, um den aktuellen Gefahren zu begegnen: Es gibt heute nur unzureichende Maßnahmen gegen globalen Terrorismus und *Cyber Threats*; die Diskrepanz zwischen Sicherheitsbehörden und Geheimdiensten, die ersteren nicht erlaubt, strategische Überwachungsmaßnahmen durchzuführen, muss überwunden werden. Als ein zunehmendes Problem sei die Tendenz zum „going dark" anzusehen, d. h. die Geräte- und Diensteverschlüsselung durch Internet-Nutzer. Zuletzt sei auch eine systematische Verkehrsdatenerfassung notwendig, um Beziehungen zwischen Gefährdern darzustellen.

Überwachung global und in Deutschland

Massenerhebung und Filterung haben sich zu einem globalen Trend entwickelt. Sicherheitsbehörden wollen systematischen Zugang („bulk access") zu Daten erhalten, um diese systematisch auswerten zu können. Dies umfasst sowohl Verkehrsdaten, den Inhalt der Kommunikation und auch private Datensammlungen aus Social Networks und Daten zu persönlichen Interessen, z. B. aus Suchmaschinen. Überwachung und Datenspeicherung erfolgen anlasslos, dabei werden unterschiedliche Formen von Spionagesoftware eingesetzt (Trojaner, Malware, Spyware). In Deutschland dagegen ist die Überwachung nach G10-Gesetz bisher nur in relativ engem Rahmen zulässig. Überwacht werden dürfen nur Leitungen mit Auslandsbezug; dabei gilt eine Begrenzung auf 20 % der Leitungskapazität. Zielgebiet und Suchbegriffe müssen im Antrag genannt werden; die Genehmigung muss alle drei Monate überprüft werden.

Das Aufgabenprofil des BND sieht Folgendes vor:

> *Die grundsätzliche Aufgabe des Bundesnachrichtendienstes ist es, seine Abnehmer zur richtigen Zeit bedarfsgerecht mit belastbaren Informationen umfassend zu versorgen. Als Dienstleister für Bundesregierung, Ressorts und auch Bundeswehr umfasst dies Informationen zu*
>
> - *wichtigen politischen, wirtschaftlichen aber auch technischen Entwicklungen,*
> - *militärischen Fragestellungen und*
> - *abstrakten oder konkreten Bedrohungen für die Sicherheit der Bundesrepublik Deutschland und ihrer Bürger.*

Derzeitige prioritäre thematische Aufklärungsziele des BND sind Proliferation, internationaler Terrorismus, Zerfall von Staaten und Auseinandersetzungen um Ressourcen. Aktuelle regionale Aufklärungsziele mit höchster Priorität sind der nahe und mittlere Osten, Nordafrika, West- und Zentralasien.

Der BND darf nur im Ausland tätig werden. Dieser Rechtsrahmen wird dabei vom BND aber sehr frei interpretiert: Satellitenüberwachung wird generell als „Ausland" angesehen (Prinzip des „freien Himmels"). Dabei argumentiert der BND, die Erfassung erfolge ausschließlich am Satellit, nur die Speicherung und Auswertung erfolge im Inland (in Bad Aibling). Filter zur Sicherstellung des Grundrechtsschutzes seien notwendig (wegen Art. 10 GG); alle weiteren Daten könne der BND frei verwenden.

Diese Interpretation führt dazu, dass auch der Netzknoten DE-CIX in Frankfurt am Main als „virtuelles Ausland" aufgefasst wird: DE-CIX sei ein „internationaler Netzknoten", an dem Carrier aus vielen Ländern aufeinanderträfen. Damit sei Auslandsbezug für alle Leitungen gegeben. Die Ausleitung erfolge auf Basis einer G10-Anordnung. Dabei sei wiederum ein G10-Filter erforderlich, weitere Daten seien frei verwendbar.

DE-CIX äußerte bereits 2009 Bedenken:

- das G10-Gesetz sei nicht ohne weiteres auf paketorientierte Kommunikation anwendbar, da es keinen Leitungsbezug gäbe,
- es ist unklar, ob die Leitungskapazität oder der Verkehr für die Ermittlung der 20 % maßgeblich sind,
- der Transport erfolge von Router zu Router innerhalb Frankfurts, ein Auslandsbezug sei daraus nicht erkennbar,
- die Abgrenzung der Carrier in national/international sei schwierig,
- die Zwischenspeicherung aller Verkehre sei notwendig,
- die trennscharfe Filterung zur Sicherstellung von Art. 10 sei nicht möglich.

Das Kanzleramt sicherte dagegen zu, dass alles innerhalb des zulässigen Rechtsrahmens stattfinden würde.

Anders ist die Sichtweise des NSA-Untersuchungsausschusses:

- im Gegensatz zur Rechtsauffassung des BND gilt der Grundrechtsschutz auch für Ausländer,
- das Konzept des „freien Himmels" ist nicht haltbar,
- das Programm DAFIS, das die Filterung inländischer Personen zur Sicherstellung von Art. 10 GG leisten soll, ist äußerst rudimentär, weniger effektiv als zunächst erwartet,
- nicht als G10-Verkehre markierte Daten werden mit anderen Geheimdiensten getauscht,
- wie sich herausstellt, empfindet auch die G10-Kommission das „Vorgehen als unredlich", da G10-Anordnungen dafür verwendet werden, Daten zu erlangen, für die es keine Gesetzesgrundlage gibt.

Dies hat DE-CIX dazu bewogen, gegen die Überwachungsmaßnahmen zu klagen. Basis dafür ist ein Gutachten des früheren Verfassungsrichters H. J. Papier, in dem er zu folgenden Ergebnissen kommt:

- Art. 10 ist Menschenrecht, kein „Deutschenrecht“, und gilt für alle Menschen, unabhängig von der Nationalität,
- die Regeln der Verfassung gelten bereits immer dann, wenn ein deutscher Dienst tätig ist,
- der Grundrechtsschutz bei der Tätigkeit eines deutschen Dienstes im Inland steht außer Frage,
- im Ergebnis sind die Anordnungen insgesamt unzulässig.

Damit werden sämtliche Bedenken des DE-CIX aus 2009 bestätigt; die gerichtliche Klärung der Zulässigkeit zwingend erforderlich. Deswegen wird Klage vor dem Bundesverwaltungsgericht Leipzig geführt.

Das neue BND-Gesetz zur Ausland-Ausland-Fernmeldeaufklärung legalisiert dagegen die bestehenden Praktiken:

- Verfassungsrechtliche Fragen aus G10 werden durch das neue Gesetz nicht berührt,
- Kommunikation wird nach Kommunikation von Deutschen, EU-Bürgern und anderen Ausländern unterschieden,
- Datenweitergabe an Partnerdienste ist nach dem neuen Gesetz möglich,
- es wird eine neue Kontrollinstanz geschaffen – diese soll mehr Vorgänge bearbeiten, aber mit weniger inhaltlicher Tiefe.

Staatssekretär Klaus-Dieter Fritsche aus dem Bundeskanzleramt erklärte dazu:

> *„Mit der Frage von Rechtssicherheit für die Angestellten des BND gegenüber der Rechtsstaatlichkeit für Bürger konfrontiert muss ich sagen, dass mich primär die Rechtssicherheit interessiert.“*

Selbst wenn man zugutehält, dass sich Fritsche in der Rolle des Arbeitgebers hinter seine Mitarbeiter stellt, ist diese Aussage für einen Staatssekretär sehr fragwürdig.

Inhaltlich regelt das Gesetz die Erhebungsgrundlage neu:

- Wegfall des Leitungsbezugs
- Wegfall der Kapazitätsschranken
- Einschränkung des Auslandsbezugs
- Verlängerung der Anordnungsdauer von 3 auf 9 Monate
- Erhebung im Inland ausdrücklich zulässig
- Umfang der Erhebung unterliegt keiner Kontrolle

Im Ergebnis ist die Erhebung nach dem neuen Gesetz ausschließlich durch die finanziellen Ressourcen des Dienstes beschränkt.

Filterung

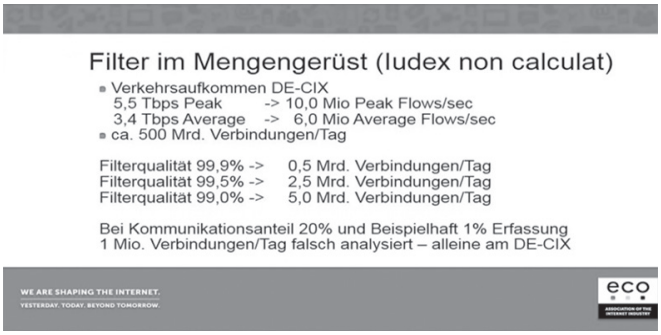
Der Grundrechtsschutz wird beim neuen Gesetz alleine durch das Filtersystem DAFIS sichergestellt. Bewertung, Filterung etc. erfolgen dabei vollständig im Kontrollbereich des BND. Das Filtersystem unterliegt keiner Kontrolle durch ein unabhängiges Gremium, wie z. B. das G10-Gremium oder das parlamentarische Kontrollgremium.

Darüber hinaus kann das Filtersystem für bis zu 6 Monate abgeschaltet werden, um die Verkehre zur „Eignungsprüfung“ zu analysieren, diese Anordnung unterliegt keiner externen Kontrolle.

Das Filtersystem DAFIS ist mehrstufig aufgebaut:

- IP-Filter zur Filterung nach Geo-Location
- Typfilter zur Filterung nach Dateitypen (http, smtp, video, chat etc.)
- Metadatenfilter zur Vorfilterung von Inhalten (z. B. E-Mail-Header, SIP)
- Inhaltsfilter (RTP, E-Mail, Kurznachricht etc.)

Einem Gutachten von eco zufolge beträgt die Qualität des Systems DAFIS geschätzt 98,5–99 % korrekter Filterung. Kommerzielle Filter leisten bis maximal 99,5 %. Analysen der Stufe 3 und 4 sind aus Sicht des DE-CIX bereits ein Grundrechtseingriff mit Notifizierungspflicht.



Betrachtet man die Zahlen, so muss man am Knoten DE-CIX von einem Verkehrsaufkommen von 5,5 Tbps (10,0 Mio. Peak Flows/sec) in der Spitze und 3,4 Tbps im Schnitt (6,0 Mio. Average Flows/sec) ausgehen. Es gibt ca. 500.000.000.000 Verbindungen pro Tag.

Klaus Landefeld

Klaus Landefeld ist Vorstand für Infrastruktur und Netze beim eco e. V., dem größten Verband der Internetwirtschaft in Europa. Er ist Beirat der DE-CIX Management GmbH, Betreiberin des weltgrößten Internetknotens. Darüber hinaus ist er selbständiger Unternehmer und Gründungsmitglied der DENIC eG, AMS-IX, MINX und weiteren IP-Exchanges weltweit. Er war geladener Sachverständiger im NSA-Untersuchungsausschuss des Bundestages.

- Bei einer Filterqualität von 99,9 % ergeben sich 0,5 Mrd. falsch zugeordnete Verbindungen/Tag.
- Bei einer Filterqualität von 99,5 % ergeben sich 2,5 Mrd. falsch zugeordnete Verbindungen/Tag.
- Bei einer Filterqualität von 99,0 % ergeben sich 5,0 Mrd. falsch zugeordnete Verbindungen/Tag.

D. h. bei einem Kommunikationsanteil von 20 % und beispielhaft 1 % Erfassung werden 1 Mio. Verbindungen/Tag falsch analysiert – alleine am DE-CIX –, d. h. es gibt pro Tag 1 Mio. Grundrechtsverstöße.

Bei einem Grundrechtseingriff muss der Betroffene informiert werden. Diese Information kann ausgesetzt werden; die Entscheidung darüber trifft die G10-Kommission. Eine Aussetzung ist alle drei Monate zu überprüfen – wie eine Einzelfallprüfung bei potenziell mehr als 100.000.000 Fällen erfolgen soll, bleibt offen. Der endgültige Verzicht auf Information ist nach fünf Jahren möglich; in diesem Zeitraum dürfen die Daten nicht gelöscht werden.

Einordnung des Gesetzes

Der Gesetzgeber sieht das Gesetz positiv: Es werde kein Grundrecht eingeschränkt – mindestens wird im Gesetzentwurf kein eingeschränktes Grundrecht angegeben, was erforderlich wäre – und die Grenze für die Überwachung sei hinreichend bestimmt (durch das Budget des Bundesnachrichtendienstes). Nach Auffassung der Koalition ist es ein „sehr gutes Gesetz mit internationalem Beispielcharakter".

Sachverständige haben eine andere Auffassung: der Wissenschaftliche Dienst des Deutschen Bundestags beurteilt das Gesetz sehr kritisch; auch unabhängige Sachverständige sehen es durchweg überaus kritisch. Beim Bundesverfassungsgericht sind erste Klagen anhängig, z. B. durch Amnesty International; weitere sind in Vorbereitung. DE-CIX wird bei Empfang der ersten Anordnung umgehend Klage beim BVerwG in Leipzig einreichen.

FIfF-Konferenz 2016

Un.Sichtbare Datenpraktiken?

Big Data in Wirtschaft, Wissenschaft & Politik

Zusammenfassung des Vortrags von Judith Simon

Die Proliferation von Big-Data-Praktiken ist ein relativ neues und komplexes Thema. Insbesondere die Intransparenz der verwendeten – häufig zudem proprietären – Systeme bereitet dabei Schwierigkeiten. Dabei muss man zwischen funktionaler Intransparenz („kein Zugriff") und epistemischer Intransparenz („Schnelligkeit", „Komplexität der Prozesse", usw.) unterscheiden, um sinnvolle Desiderate für die Governance von Big Data ableiten zu können. Ein wesentlicher Teil solcher Governance-Bemühungen ist neben den rechtlichen Regelungen natürlich auch die transparenzförderliche Gestaltung der IT-Systeme (Stichwort: value-sensitive Design).

Warum und in welcher Weise müssen wir uns mit Big Data beschäftigen?

Die meisten werden das folgende Beispiel kennen: 2012 ging durch die Medien die Geschichte eines US-amerikanischen Vaters, der sich bei der Supermarktkette Target beschwerte, weil er Werbematerial zu schwangerschaftsbezogenen Produkten zugesendet bekommen hatte. Schließlich stellte sich jedoch heraus, dass seine 16-jährige Tochter tatsächlich schwanger war und es ihm bis dahin verschwiegen hatte. Target wusste also mehr als der eigene Vater. Bei aller anfänglichen Empörung oder Überraschung über diesen Fall müssen wir jedoch kritisch fragen: Liegt hier überhaupt ein Problem vor? Wenn ja, wo, und wie kann man es konzeptuell fassen?

Der naheliegendste Ansatz sind die Punkte *Verletzung der Privatsphäre* und *illegitime Datensammlung* – durch die rechtlich legitime Praxis der *Informed-consent*-Verfahren (Einwilligung nach vorheriger Aufklärung) stimmen wir allerdings der Nutzung unserer Daten zu, sodass im Grunde rechtlich hier gar kein Problem vorliegt, denn auch die Tochter hat dem Sammeln und Auswerten ihrer Daten zugestimmt. Die Verletzung der Privatsphäre ist hier jedoch nicht auf Grund des Datensammelns passiert, sondern erst durch die Inferenzen, die auf Basis der Daten, d. h. der Verarbeitung der Daten und der Prognosen, gemacht wurden. Big-Data-Praktiken müssen also zunächst als epistemische, d. h. wissenschaftliche Praktiken betrachtet werden, die

Judith Simon

als solche wiederum ethische und politische Auswirkungen haben, denn Big Data durchdringt mit seinen Verfahren unsere Lebenswelt ganz grundlegend und ist damit natürlich keine rein erkenntnistheoretische Frage. Der Fokus muss dabei auf den konkreten Praktiken des Datensammelns selbst liegen, erst im zweiten Schritt auf ihrer Interpretation, denn ich kann Daten erst dann interpretieren, wenn ich weiß, wo, wie und in welcher Qualität sie erhoben worden sind. Hierzu sind detaillierte und vor allem interdisziplinäre Analysen der Datenpraktiken in Wirtschaft, Politik und Wissenschaft nötig. Die Blickweisen der Ethik müssen wiederum mit der Erkenntnistheorie und den Entscheidungsprozessen der Politik verknüpft werden, sodass daraus rechtliche oder auch ökonomische Konsequenzen abgeleitet werden können.

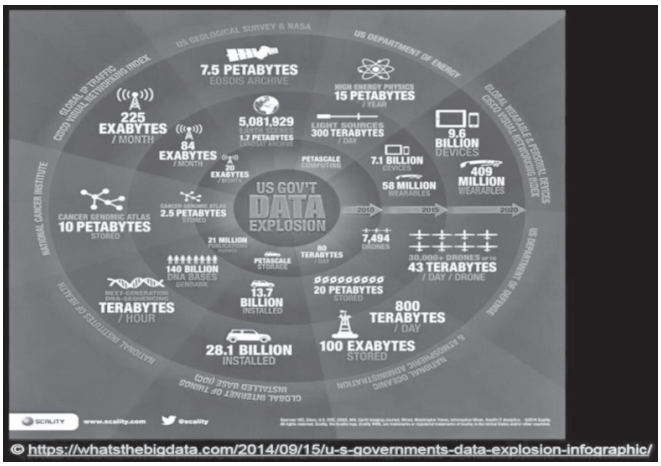
Was ist Big Data?

Nach der klassischen Definition der Industrie gehören zu Big Data (nach IBM) die vier Vs: Volume (*scale of data*), Velocity (*analysis of streaming data*), Variety (*different forms of data*) und Veracity (*uncertainty of data*). Interessanter allerdings ist eine Definition aus den Sozialwissenschaften (Boyd & Crawford 2012) als „*cultural, technological, and scholarly phenomenon that rests on the interplay of Technology, Analysis and Mythology*", wobei hier insbesondere interessant ist, dass als entscheidender Faktor in die Begriffsbestimmung auch der Glauben an die Allmacht der Daten mit aufgenommen wurde, der Glaube daran, große Datenmengen ermöglichen „*a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy.*" Dieser Punkt spielt insbesondere für die Rhetorik in politischen Debatten um die angeblich unbestechlichen und neutralen Big-Data-Analysen eine große Rolle.

Über welche Datensätze reden wir aber eigentlich konkret, wenn wir von Big Data sprechen? Unterschieden werden können einerseits die Daten einer Person innerhalb ihres Alltags, etwa danach, wo sie angefallen sind: Die Daten, die aus den sozialen Medien über die Nutzer.innen gewonnen werden, und zwar hierbei die expliziten wie Kommentare, Fotos, Likes, ebenso wie auch die impliziten Daten, also die Spuren, die wir hinterlassen, wenn wir handeln (Ort, Zeit, Verweildauer, etc.). Andere Datensätze erfassen wiederum jegliche Formen von Transaktionsdaten, die orts- und zeitbezogenen (Meta-)Daten, Sensordaten oder Daten aus dem Internet der Dinge. Unterscheiden können wir die Daten andererseits auch etwa innerhalb der Wissenschaft, z. B. in Daten der Astronomie, der Physik, der Medizin, etc., und weiter differenziert schließlich innerhalb der Disziplinen – z. B. die medizinischen Daten in Daten aus Versuchsreihen, Daten aus elektronischen Patientenakten, in administrative Klinikdaten oder Daten des Personal Health Monitoring (aus Sensoren, Apps, Wearables, etc.). Im Kontext von Big Data ist noch eine dritte Gruppe an Daten relevant: Bürgerdaten, sog. Open Government Data, wobei diese jedoch nicht notwendigerweise offen sind. Hierzu zählen Daten aus dem Geburtsregister, Finanzdaten, Zensusdaten, usw.

Das Interessante an Big Data aber ist nicht, dass es all diese Daten gibt, sondern dass sie mit Hilfe der Datenanalyse vielfältig in Bezug zueinander gesetzt werden können. Erkenntnistheoretisch lässt sich dabei festhalten, dass bestimmte Unterscheidungen, die einst relevant waren, im Big-Data-Kontext zunehmend obsolet werden, wie etwa die Unterscheidung zwischen sensiblen persönlichen Daten und unverfänglichen sonstigen Daten. Ein Beispiel, an dem sich dies zeigt: Der eingangs genannte Fall der Zusendung von Werbung für Schwangerschaftsprodukte. Konsumdaten wie der Kauf einer parfümfreien Body Lotion oder von bestimmten Vitaminpräparaten sind zunächst nicht per se medizinische Daten. Sie werden jedoch genutzt für Prognosen über den medizinischen Zustand des oder der Käufer.in, in diesem Falle zur Prognose einer Schwangerschaft. Das Problem ist also, allgemeiner gesprochen: Je nach Nutzungskontext können scheinbar unverfängliche Daten sensibel werden. Dennoch sind diese (Proxy-)Daten weniger geschützt als herkömmliche Gesundheitsdaten, Finanzdaten, etc.

Eine zweite Differenzierung, die im Big-Data-Zusammenhang obsolet wird, ist die zwischen personenbezogenen und anonymen Daten. Durch Aggregation und Datenverarbeitung können anonyme Daten zunehmend leicht de-anonymisiert werden. Hier ein banales Beispiel: Ich wurde im Zusammenhang mit einem Forschungsprojekt in Österreich um eine Bewertung gebeten und musste hierfür einige Daten über mich angeben, wie meine wissenschaftliche Disziplin und mein Alter. Vier dieser Datenpunkte reichen jedoch aus, um mich eindeutig zu identifizieren. Zu einer Diskriminierung, die möglicherweise aus dieser Zuordnung folgt, reicht jedoch schon die Identifikation als Teil einer Gruppe aus, etwa die Zuordnung zu einer bestimmte Wohngegend, die bei Kreditinstituten schlechtere Konditionen erhält (vgl. Vortrag Corinna Bath: *Sozial gerechte Algorithmen?*).



Datenexplosion

Wer ist Teil von Big Data?

Wer ist nun aber involviert in diese Big-Data-Prozesse? Manovich (2011) unterscheidet hier in „*those who create data (both consciously and by leaving digital foot prints), those who have the means to collect it, and those who have expertise to analyze it*". Ersteres sind wir alle, die weiteren beiden Gruppen jedoch nicht, und dies wiederum führt zu Unterschieden bezüglich der – mitunter unsichtbaren und nicht uns allen verfügbaren – technischen Auswertungsfähigkeiten, was wieder eine Machtasymmetrie erzeugt zwischen denen, die die Daten bereitstellen und denen, die über sie verfügen.

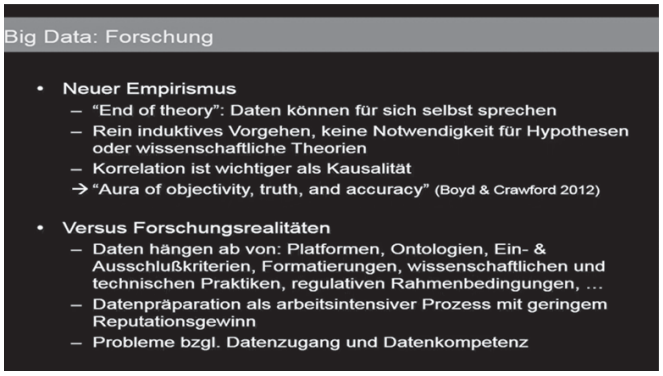
Wer sammelt also die (personenbezogenen) Daten? Schematisch können wir die Bereiche Wissenschaft, Staaten und Unternehmen unterscheiden sowie – eingeschränkt – auch die Nutzer.innen selbst, die bis zu einem gewissen Grad und in geringerem Ausmaß ebenfalls in der Lage sind, Daten zu sammeln und auszuwerten, etwa via Self-Tracking. Die Funktionen von Big Data für diese vier Gruppen sowie die Auswirkungen sind jedoch sehr verschieden. Daher ist es besonders wichtig, den jeweiligen Rahmen sehr genau zu formulieren, wenn von Big Data die Rede ist.

Big Data in der Industrie

Für Unternehmen geht es primär darum, Konsument.innen zu tracken und zu profilieren, um auf der Basis der Datenspuren, die sie hinterlassen, Rückschlüsse etwa für zielgenaue Werbung ziehen zu können. Hierzu zählen nicht nur die großen bekannten Datensammler Facebook und Google, sondern auch viele andere Unternehmen, die schon sehr lange Kompetenzen in der Datenanalyse haben, die uns mit dieser Praxis aber nicht unbedingt geläufig sind, etwa IBM, das sich inzwischen längst als Datenunternehmen versteht. Darüber hinaus gibt es viele Hintergrundakteure, die für Unternehmen arbeiten, deren Namen uns Nutzer.innen oft nicht bekannt sind, die jedoch trotzdem Daten aus diversen Kontexten über uns besitzen – ein geläufigeres Beispiel hier wäre Oracle.

Big Data in der Wissenschaft

Datensammlung und -analyse ist ein Grundbestandteil jeglicher wissenschaftlicher Forschung. Inzwischen wird sowohl aus philosophischer als auch aus wissenschaftlicher Perspektive allerdings diskutiert, ob es durch die neue Form der Datenanalyse zu einem Paradigmenwechsel kommt. Nach den Thesen des sogenannten *Neuen Empirismus* sprechen die Daten inzwischen für sich selbst, sodass es in der Wissenschaftspraxis keine Notwendigkeit mehr für Hypothesen gibt und Experimente oder Kausalitätszusammenhänge obsolet werden (*End of Theory*). Dem gegenüber stehen die Forschungsrealitäten, die zeigen, dass Daten keinesfalls aus sich selbst heraus neutral entstehen, sondern immer abhängig sind von verschiedenen Faktoren wie den Rahmenbedingungen, die für das Sammeln der Daten und für ihre Auswertung gesetzt werden. Beim Neuen Empirismus bleibt zudem u. a. das Problem aller Forschenden unberücksichtigt, stets nur einen limitierten oder kostenpflichtigen Zugang auf insbesondere kommerzielle Daten zu haben. Wissenschaftlich sind diese Thesen daher höchst umstritten, allerdings ist die Rhetorik dahinter für die Politik wiederum enorm verführerisch.



Big Data in der Politik

In der Politik wird auf Big Data große Hoffnungen (z. B. in der Verkehrs- oder Gesundheitspolitik) gesetzt, denn das Sammeln und Verarbeiten von Daten wie etwa das Führen von Geburts- und Sterberegistern (anfangs noch allein von der Kirche übernommen) war immer ein Grundbestandteil staatlicher Kontrolle. Seit dem 18. Jahrhundert bezeichnen wir diese systematische Sammlung demographischer und ökonomischer Daten speziell durch den Staat mit dem Terminus Statistik. Staatliche Verwaltung, die Konstruktion eines Staates und das Regieren als solches sind eng mit dem Erheben von Daten verbunden (Desrosières 1998), sodass sich die Geschichte von Nationalstaaten zugleich als Geschichte der Statistik und damit als eine Geschichte des Sammelns und Verarbeitens von Daten lesen lässt. Wissen und Macht gehören hier eng zusammen.

Big Data soll als sogenannte *evidenzbasierte Politik* zunehmend Anwendung finden. Ist dieses Vorgehen aber überhaupt epistemisch, politisch und ethisch gerechtfertigt? Die bereits angesprochenen ethischen Fragen um Privatsphäre, Datenschutz, Schutz vor Diskriminierung, Herstellung von Gleichheit, Autonomie, usw., sind beim Einsatz von Big Data in der Politik zwingend zu berücksichtigen. All diese Fragen sind bislang ungelöst. Die Rechtfertigung von Big Data in der Politik ist epistemisch jedoch bereits aufgrund des beschränkten Zugangs zu Daten (bzw. Algorithmen oder Software) und der mangelnden Kompetenz in kritischer Datenanalyse schwierig. Diejenigen, die auf der Basis von Datenanalyse politische Entscheidungen treffen, müssen in die Lage versetzt werden, sie zu verstehen, d. h. es muss zunächst einmal die Wissensgrundlage geschaffen sein, um einschätzen zu können: Wie ist die Qualität der Daten, der Berechnungen, der Algorithmen, der Systeme? Liefern sie tatsächlich zuverlässige Prognosen? Sind die Daten tatsächlich die argumentativ beste Grundlage, auf der ein politischer Entscheidungsprozess beruhen sollte? Auch die Rhetorik von Big Data als neutraler theorie- und verzerrungsfreier Wissenschaft erschwert die kritische Analyse, weil sie ermöglicht, dass Politiker.innen sich auf diese scheinbar unbestechlichen Zahlen berufen und damit die eigenen unliebsamen Entscheidungen begründen, sie so aber zugleich als nicht selbstgetroffen von sich weisen können.

Big Data: (Un)sichtbare Systeme?

Um die Schwierigkeit der epistemischen Rechtfertigung von Big Data zu verstehen, ist ein Blick auf die Intransparenz von Big-Data-Praktiken hilfreich. Unterscheiden lassen sich zwei Arten: Die funktionale und die epistemische Intransparenz. Die funktionale umfasst den eingeschränkten Zugang zu Systemen, Daten, Algorithmen, etc., insbesondere von proprietären Systemen, die nicht Open Source sind und als solche ein großes Problem darstellen, denn wie lässt sich funktionale Intransparenz auflösen, wenn Geschäftsgeheimnisse als Wettbewerbsvorteil gelten und daher ein Unternehmen nicht gezwungen werden kann, Daten und Algorithmen offenzulegen? Möglich wäre dies nur durch neue Geschäftsmodelle, die Big Data anders regulieren. Hierzu

gibt es derzeit drei Argumentationslinien: das Verteidigen des Status Quo in Berufung auf die Selbstregulierung des Marktes, die Forderung nach verbesserter Regulation durch effektivere Regulierungsmöglichkeiten großer Internetfirmen und drittens den Ansatz, dass sich die ökonomischen Grundlagen von Datenmärkten verändern müssen. Dieser Ansatz folgt u. a. aus der Erkenntnis, dass oft nicht mehr die Qualität der Algorithmen, sondern die Menge der Daten über die Qualität der Auswertung entscheidet und damit zu einem entscheidenden Wettbewerbsvorteil wird, der nicht durch bessere Algorithmen oder andere Maßnahmen ausgeglichen werden kann. Bereits allein aus ökonomischer Perspektive ist das höchst problematisch, denn so entsteht ein großes Ungleichgewicht zwischen den Unternehmen eines Marktes, sodass sich die Frage stellt, ob nicht längst eine Monopolbildung den freien Markt verunmöglicht hat. Auflösen lässt sich dies nur durch etwa alternative Infrastrukturen oder Konzepte, bei denen die Daten nicht mehr den Unternehmen gehören. Hier gibt es im Wesentlichen zwei Richtungen: Gehören Daten allein dem Nutzer oder sind sie als öffentliches Gut zu verstehen? Alexey Morosov etwa ist einer der Vertreter, die die Auffassung von Daten als Gemeingut vertreten, nach der Daten demnach gar nicht gehandelt werden können (was allerdings für den Schutz und die Sicherheit der Daten neue Herausforderungen mit sich bringt). Jaron Lanier nach sollten die Daten dem Nutzer gehören, der dann an Gewinnen auch direkt partizipieren kann.

Die zweite Art der Intransparenz nun, die epistemische, entsteht durch die Grenzen jedes Einzelnen, komplexe Systeme und Verfahren verstehen zu können. Sie ist damit relativ zur Kompetenz der Nutzer.innen: Je mehr ich über Datenanalyse weiß, desto mehr kann ich verstehen. Das Informed-consent-Verfahren ist in dieser Hinsicht ein für die meisten Nutzer.innen intransparentes Vorgehen, denn auch wenn offengelegt wird, was mit den eigenen Daten geschieht, d. h., wenn ich über die *Terms of Agreement* informiert werde, bevor ich sie unterschreibe, ist dies nur insofern transparent, als dass das Vorgehen nur bis zu einem gewissen Grad tatsächlich offengelegt wird. In den seltensten Fällen haben Nutzer als Nicht-Experten ausreichende Handlungskompetenz, um das Gelesene wirklich zu verstehen. Lösungsansätze hierzu sind Konzepte wie *Privacy* oder *Transparency by Design*, das heißt im Sinne des Vortrags von Leon Hempel werden die Dinge *transparent to use*: Wir schützen die Nutzer als Default. Für Expert.innen stellen sich in Bezug auf die epistemische Intransparenz zudem weitere Fragen: Wo sind Erkenntnisgrenzen mit welchen Auswirkungen, wenn ich verstehen will, wie komplexe Systeme im Kontext von z. B. Maschinenlernen oder neuronalen Netzen funktionieren? MacKenzie z. B. hat in *Mechanizing Proof* bereits 2001 danach gefragt, ob ein Beweis durch Computerberechnungen formal ein Beweis ist, wenn ihn keiner der Experten verstehen kann, denn im Mathematischen beruht ein Beweis darauf, dass er epistemisch nachvollziehbar ist. Auch im Vortrag von Corinna Bath ging es um die Frage, wo sich auf Expertenseite die Grenzen des Verständnisses verschieben lassen und inwiefern sich Verzerrungen und etwa daraus abgeleitete Diskriminierung durch Software nachweisen und visualisieren lassen.

Big Data: Was nun?

Das Problem der *Un.Sichtbarkeit* als einerseits funktionales, andererseits epistemisches System verlangt demzufolge nach sehr unterschiedlichen Lösungen – einerseits nach grundlegenden ökonomischen Veränderungen, andererseits nach dem Auflösen oder Verschieben der Grenzen der Verstehbarkeit von Big-Data-Praktiken für Nicht-Expert.innen wie für Expert.innen. Hierzu müssen wir uns von einem reinen Big Data for Governance hinwenden zur Notwendigkeit der Governance for Big Data. Es stellen sich Fragen wie: Wie erhöht man die Vertrauenswürdigkeit von Datenpraktiken? Durch welche technischen und legalen Verfahren lässt sich epistemische, politische und ethische Überprüfbarkeit unterstützen? Big Data Governance muss als eine Kombination gedacht werden aus rechtlichen Lösungen (Regeln der Hard Law), Selbstverpflichtungen (Soft Law), Governance by Design (die Bemühungen von Privacy by Design oder Transparency by Design) und auch einem Umdenken in der Bildung. Keine dieser Säulen wird allein ausreichen, um die bislang etablierte Praxis und derzeit größte Krux der In.Transparenz abzulösen: Die Bürde des Informiertseins auf die Schultern von Nutzer und Nutzerin zu legen.

Referenzen

Boyd, D./Crawford, K. (2012): Critical questions for big data – provocations for a cultural, technological, and scholarly phenomenon. In Information, Communication & Society 15 (5) 662–679

Manovich, L. (2011): Trending: the promises and the challenges of big social data. In M. K. Gold (ed.): Debates in the digital humanities. The University of Minnesota Press

Desrosières, A. (1998): The politics of large numbers – a history of statistical reasoning. Cambridge: Harvard University Press

Judith Simon

Judith Simon ist Associate Professorin für Wissenschaftstheorie und Technikphilosophie an der IT University of Copenhagen. Sie ist zudem Editorin der Journals *Philosophy & Technology* und *Big Data & Society* sowie Vorstandsmitglied in der *International Association of Computing and Philosophy* (IACAP) sowie der *International Society for Ethics and Information Technology* (INSEIT).

An den Enden der Informatik

Zusammenfassung des Vortrags von Wolfgang Coy

So wie die Physik vom Subatomaren bis zum Kosmischen forscht, spannt sich die Informatik von den beliebig unterteilten Dingen des Internet of Things *bis zu den weltumspannenden Netzen, die im letzten Jahrzehnt riesige Data Center als Knoten ausgebildet haben. Wir bewegen uns im digitalen Nebel der* Clouds *und im Dunstkreis unserer* Wearables *in immer engmaschigeren Datengeweben. Wolfgang Coys Vortrag will einen Überblick über die Informatik geben von ihren Anfängen bis heute und dabei die Enden der Informatik aufsammeln, die wir üblicherweise übersehen – bis sie uns schließlich auf die Füße fallen.*

Die Enden der Informatik erinnern an die der Physik, die nach Galilei und Newton zunächst ihren Kernbereich ausbaute und sich dann im 19. und frühen 20. Jahrhundert in zwei Richtungen entwickelte, die auf den ersten Blick sehr weit auseinander liegen: Die Quantenphysik und die subatomaren Prozesse einerseits, die Kosmologie andererseits. Auch die Informatik scheint sich derzeit auf dem Weg zu befinden, ihre eigenen „kosmologischen" Fragen zu entwickeln. In den letzten 15 bis 20 Jahren ist die Informatik jedoch – anders als die Physik – zudem ins Zentrum der politischen Diskussionen gerückt. Zwar hat die Physik mit der Entwicklung der Atombombe durchaus im 20. Jahrhundert Aufmerksamkeit erregt, ist aber doch im Alltag und in den alltäglichen Diskussionen eher entrückt geblieben. Die Fragen der Informatik hingegen gehen heute in vielerlei Hinsicht uns alle an.

Technische Entwicklung

Als Coy in den 60er-Jahren anfing, sich für Computer zu begeistern, waren die Rechenmaschinen noch um unendliches größer als heute und IBM begann gerade, sich für die Rechnerfamilie System 360 zu begeistern. Man trug blaue Anzüge und auch die raumfüllenden Maschinen konnten nicht anders als blau sein (wobei Coy als wissenschaftlicher Mitarbeiter ohne Kundenkontakt keine Anzüge tragen musste).

Computer Center Ende der 60er Jahre

Heute stehen wir ganz woanders: Noch immer gibt es Rechner, aber ein heutiges iPhone ist deutlich schneller als jedes Gerät aus der 360-Serie, und in seiner Leistung eher mit der etwas flotteren Cray-1 der 70er Jahre zu vergleichen, die natürlich nicht nur größer und schwerer (5,5 Tonnen), sondern auch wesentlich teurer war (mehrere Millionen US-Dollar) und damit bei weitem nicht für den Alltagsgebrauch jedem zugänglich.

Was die Informatik jedoch heute noch viel mehr ausmacht, ist die wirklich große Menge von Daten, die wir inzwischen speichern können. Hinter dem populär gewordenen und eher untechnischen Begriff *Big Data* stehen in erster Linie große digitale Datenmengen, die vor allem zunächst einmal gespeichert werden. 2014 standen im ZIB (Zuse-Institut Berlin) 20 Petabyte zur Verfügung – 3,7 davon online; das Klimaforschungszentrum in Hamburg verfügt inzwischen über 190 PB, davon 5 direkt über Festplatten; die Humboldt-Universität im Vergleich ebenfalls über 20 PB.

Inzwischen hat sich aber nicht nur die Menge der Daten, die anfallen, gespeichert und auch ausgewertet werden, enorm verändert, sondern auch der Ort des Speicherns hat sich verlagert, weg von einer lokalen Festplatte hin zu den sogenannten *Cloud Services*, die in unterschiedlichsten Formen angeboten werden: Speicherplatz in der Cloud, Software aus der Cloud – die Cloud als Plattform, um das komplette IT-Management aus dem Rechenzentrum weg zu verlagern. Hierfür gibt es eine Vielzahl Anbieter – darunter einige Überraschungen: Amazon speichert nicht nur Bücher, sondern auch Daten in großen Mengen; außerdem Microsoft, die sich so „neu erfunden haben", Google, Salesforce und einige eher kundenorientierte wie die Apple-Cloud, *Google Drive* oder *Microsoft OneDrive*. Mit den Clouds hat sich die Informatik stark verändert – abgesehen von den technisch Interessierten ist sie für die meisten Menschen damit ein Stück weit unsichtbar geworden; die Grenze des Verstehens beginnt bereits bei dem Namen *Cloud*, der Hoffnungen aller Art beflügelt. Auch andere Organisationen, wie die NSA, setzen *Data Center* (Rechenzentren) ein, die ihre Dienste unaufgefordert und für die Betroffenen völlig unkontrollierbar betreiben. In Bluffdale, Utah betreibt die NSA einen riesigen Bau mit mehreren hundert Metern Ausmaß, mit viel Speicher und selbständiger Energieversorgung. Auch in Berlin-Spandau gibt es ein großes Gelände, das am Eingang nicht näher bezeichnet ist und eine große Menge Speicher und Versorgungsanlagen beherbergt. Diese Art von Center – fensterlose Bauten – sind uns verborgen, *invisible*. Selbst wer weiß, wie sie aussehen und wo sie stehen, *invisible* bleiben dennoch die Innereien der Räume – ihre Speicher, Rechner und der Netzzugang.

Die Entwicklung der Netze

Die Idee des Netzes ist eine der großen tragenden Ideen der modernen Industriegesellschaft. Netze verschiedenster Art gibt es natürlich schon länger: Die Römer hatten Straßen- und Wagennetze rund ums Mittelmeer bis nach Schottland, im 19. Jahrhundert begann dann die moderne Vernetzung über das Ver-

kehrsnetz und neben den Verkehrswegen vernetzten sich auch immer stärker die Kommunikationswege. Insbesondere solche, die elektrisch sind und im Idealfall mit Lichtgeschwindigkeit Verbindungen herstellen können, prägen uns heute als Kommunikationsgesellschaft und bilden für uns Informatiker.innen das zentrale Element.

Lässt man den militärischen Bereich erst einmal außen vor, entstehen in den 60ern und 70ern dann die Datennetze. Technischer Vorläufer unserer digitalen Netze war das Forschungsnetz ARPA- bzw. DARPA- – *(Defense) Advanced Research Projects Agency – NET(work)*, das sowohl militärisch als auch von zivil orientierten Teilen der Universitäten genutzt wurde. Grundlage des ARPANET war SAGE *(Semi-Automatic Ground Environment)*, ein Luft-Abwehrsystem gegen die russischen atomar bewaffneten Langstreckenbomber. Als SAGE jedoch fertig war, spielten diese Bomber keine Rolle mehr, da die atomare Aufrüstung auf beiden Seiten zu Interkontinentalraketen gewechselt war.

Neben dem Glasfaser- und Kupfernetz haben wir heute noch ein zweites System, das immer wichtiger wird – den Mobilfunk. Dieses Netz ist überraschenderweise an einigen Orten in Deutschland noch recht unvollständig. Dieser unsichtbare Bereich der Informatik wird erst sichtbar, wenn man davon direkt betroffen ist – wenn man zum Beispiel von Berlin aus 20 Minuten mit dem Zug Richtung Norden fährt. Oder in Gumperda wohnt.

Neue Wege der Datenerfassung und ihre Utopien

Ein weiterer wenig sichtbarer Teil der Informatik ist der des Messens und der digitalen Sensoren, den wir in den letzten Jahrzehnten in die Informatik integriert haben. Menschen messen inzwischen ihr Elektrokardiogramm per Handy und umgeschnalltem Sensor, und Selfies werden inzwischen nicht mehr mit sichtbarem Licht, sondern mit Infrarot aufgenommen. Die Sensoren haben den Datenbereich enorm erweitert: Informatik berechnet nun nicht mehr nur Buchhaltung, sondern verarbeitetet Daten jeglicher Art.

Aus diesen Daten wiederum Nutzen zu ziehen, das ist das Gebiet der Aktorik. Ein Prototyp dessen ist die Robotik, die sich in den letzten Jahren rasant entwickelt hat: Die Anzahl und die Dichte der Roboter hat in den letzten Jahren enorm zugenommen und die Werkhallen der Autoindustrie sind weitestgehend menschenleer. Ein Ziel der Robotik sind insbesondere autonome Systeme, was insbesondere im KFZ-Bereich eine „Neurose“ ausgelöst hat. In Zukunft soll nach dem Diesel nun auch das Lenkrad verschwinden – woher die Kolleg.innen aus dem Automobilbereich die Hoffnung haben, dass dies so ganz bruchlos umsetzbar ist, erschließt sich nicht. Die Tatsache, dass man einzelne Fahrzeuge in Fabrikhallen autonom fahren lassen kann, ist nicht bestreitbar und als große Leistung hervorzuheben. Diese Systeme jedoch sicher auf die Straße zu bringen, das ist eine andere Sache, an der dennoch verbissen gearbeitet wird.

Hinter diesen Entwicklungen steht jedoch – auch – dieselbe treibende Kraft, die die Entwicklung der Datenspeicher und der Netze vorangetrieben hat. Es gibt eine *Future-of-Warfare*-Initiative, die allerlei Ideen zu autonomen Waffensystemen hat, die ähnlich wie autonome Autos funktionieren, nur anders ausgestattet sind, und auch Drohnen werden von Informatiker.innen freilich nicht nur für den zivilen Gebrauch gebaut. Solange solche Techniken klein und unbewaffnet als Modelle schönste Formationen fliegen, sind die Entwickler.innen davon begeistert – ob sie allerdings später glaubhaft verkünden können, dass sie mit der Verwendung als Kriegstechnik wenig zu tun hatten, ist fraglich.

Wolfgang Coy

Internet of Things

Auch aus dem Denken des Silicon Valley heraus sind Autos eher uninteressant. Vielmehr lautet hier die Frage, wie sich die Technik in die Wohnungen implementieren lässt. *Amazon Dash* (2016), das automatisiert Produkte bestellen kann, die zur Neige gehen, ist hier eines der jüngsten und sehr umfassend in unseren Alltag eingreifenden Systeme. Eine Ex-Entwicklerin von Apple fasste das sogenannte *Smart Home* in der Idee zusammen, „Mami“ zu automatisieren. Alles, was in der Kindheit Mami für dich erledigt hat, soll jetzt per Knopfdruck geregelt werden. Auch das Amazonprodukt *Amazon Echo* hätte sich die NSA nicht besser ausdenken können: Es bedarf keines Hackers mehr, der einen Lautsprecher in ein Mikrofon umfunktioniert, denn mit sechs Mikrofonen und vier Lautsprechern ist Echo in der Lage, ganze Räume akustisch zu überwachen, um den geneigten User überall in der Wohnung per Sprachsteuerung nicht nur mit Musik zu versorgen, sondern auch mit allen unendlichen Möglichkeiten des Internets zu verbinden. Die Abhörmöglichkeiten, früher umständlich über Wanzen in die Wohnung gebracht, sind heute kein Thema mehr, denn das ist inzwischen mit all den Dingen möglich, die wir ohnehin kaufen. Faszinierend daran auch: Wir bezahlen selbst für die Abhörtechnik.

Smarte Systeme wie diese – auch sie sind Teil der un- oder wenig sichtbaren Informatik, ebenso wie Badezimmerwaagen und Fitness-Armbänder mit Funkanschluss, die bei der Krankenkasse Rabatte ermöglichen. Das *Internet of Things* ist ein Riesenbereich mit im Grunde allen Geräten, die sich nur träumen lassen. Faktisch lassen sich diese technischen Neuerungen jedoch einer AMS-ix-Studie zufolge auf die Bereiche E-Health, Social Life, Shopping und News reduzieren, wobei unklar bleibt, was mit dem Begriff im Einzelfall tatsächlich gemeint ist – vermutlich

mehr als der Fernseher, der Laptop, das Smartphone und das Tablet, womit wir uns ohnehin schon täglich umgeben.

Methoden der Datenanalyse

Kern der Informatik ist das Berechnen, etwa nach einem Algorithmus (benannt übrigens nach dem Universalgelehrten Al-Chwarizmi). Ein Algorithmus ist eine endliche Vorschrift zur Berechnung eines Funktionswertes in endlich vielen Schritten und ein Begriff, der in den aktuellen Debatten um Datenanalyse oft sehr weit über seine technische Bedeutung hinaus gefasst wird. Datenbewertung, heute gerne Analysis genannt, ist im Zusammenhang mit Big Data derzeit in aller Munde (empfohlen sei hierzu der FIfFKon-Vortrag von Judith Simon), aber nur weil man riesige Datenbestände hat, heißt das leider nicht, dass man per se dadurch etwas besser versteht, denn die Daten müssen mit einer geeigneten Methode auch aufbereitet, d. h. ausgewertet werden. Das Sammeln der Big Data wird oft damit begründet, endlich nicht mehr programmieren zu müssen, nicht mehr zu berechnen und keine mathematischen Verfahren verstehen zu müssen. Einen mit Kundendaten vollen Speicher zu haben ergebe schon, was der nächste richtige Schritt ist. Insbesondere die Vorstandsetagen und die knapp darunter liegenden Ebenen hängen diesem Mythos an. Damit sich aus Big Data jedoch wirklich Erkenntnisse ableiten lassen, sind nicht Algorithmen, sondern Heuristiken nötig. Heuristiken wiederum gelten derzeit als eine Art goldene Lösung, wie sich Daten sinnvoll auswerten lassen, geben tatsächlich jedoch auch nur vage Vorhersagen.

Ein Beispiel hierfür und zugleich spannendes Maß für die Entwicklung der Datenauswertung ist die Wettervorhersage, die Wolfgang Coy seit seiner Studienzeit aus der Nähe mitverfolgt hat (an der TU Darmstadt gehörte die Meteorologie zum selben Fachbereich wie sein Institut, die Mathematik). Über Jahrzehnte hinweg konnte er beobachten, wie in beeindruckenden Dimensionen Rechner- und Sensornetze für die Wetterberechnungen zur Verfügung gestellt wurden, wobei zugleich dennoch immer mehr Rechenleistung gefordert wurde, weil mehr Sensoren (d. h. mehr Daten) und mehr Rechner (d. h. mehr Platz zur Speicherung und mehr Rechenleistung zur Auswertung) angeblich die Wettervorhersage um einen Faktor X verbessern würden. Die meisten Meteorolog.innen geben jedoch offen zu, dass das Wetter über mehr als 20 Tage nicht präzise vorhersagbar ist, und verfolgt man eine Wettervorhersage für den nächsten Tag, ändert sich auch diese stündlich mit jeder Aktualisierung der Daten. Eine stabile Vorhersage selbst für die kommenden Tage ist eher atypisch. Erst mit enormem Aufwand sind zuverlässigere Aussagen möglich, die wiederum auch noch lange nicht zu 100 Prozent richtig sind. Wettervorhersagen sind nun notgedrungen heuristisch – algorithmisch lässt sich hier kaum Sinnvolles berechnen – und wie vage demnach Heuristiken sind, zeigt sich sehr plastisch daran, wenn wir ohne Schirm im Regen stehen, weil Sonne berechnet war. Warum also Big Data für Kunden, für die Überwachung, in der Fabrik oder auf der Straße der goldene Weg sein soll, um bessere Ergebnisse zu erzielen, erschließt sich mit Blick auf die Meteorologie nicht direkt.

Ein ganz neues (im Grunde jedoch uraltes) Konzept ist das *Deep Learning* neuronaler Netze. In Wellen haben neuronale Netze immer wieder Triumphe gefeiert – dass bei komplexen Strategiespielen wie Schach oder dem alten chinesischen Go Künstliche Intelligenzen gegen Menschen gewinnen können, ist durchaus beeindruckend. Faszinierend ist auch, dass selbst die Entwickler.innen von Google sich nicht erklären können, warum ihr selbstlernender Translate-Dienst neuerdings so viel besser ist. Dass sich mit neuronalen Netzen jedoch auf Basis großer Datenbestände zuverlässige Vorhersagen treffen lassen und unsere Theorien (ganz im Sinne der Postmoderne) damit obsolet werden, erscheint stark übertrieben.

Technisierte Ethik?

Abgesehen von den bei Weitem noch nicht ausgereiften und mitunter zweifelhaften Konzepten des Datensammelns und -auswertens und der immer umfassenderen technischen Überwachung unseres Alltags gibt es einen weiteren, noch recht jungen Komplex, über den im Rahmen der Debatten um Informatik, Alltag und gesellschaftliche Prozesse dringend diskutiert werden muss: Im Kontext der autonomen Fahrzeuge wird inzwischen über eine algorithmische Ethik nachgedacht. Mit Entsetzen müssen wir beobachten, dass das Fernsehen dem breiten Publikum die Vorstellung nahebringen will, dass die Frage computergesteuerter Systeme derzeit lautet: Wollen wir lieber eine vollbesetzte Boeing abschießen oder wollen wir lieber riskieren, dass sie in einem vollbesetzten Stadion landet? Was da losgetreten wird, ist kurz gesagt furchtbar. Wie im Kontext des automatisierten Fahrens über Ethik gesprochen wird, als wäre Ethik algorithmisierbar, das ist nicht vertretbar. Völlig unverständlich ist auch der Kurzschluss, dass, weil über ethische Fragen im Zusammenhang mit „Entscheidungen“ technischer Geräte nachgedacht werden müsse (wir wollen die Geräte ja haben) und es deshalb konkrete Fragen zu lösen gibt, diese Lösungen (natürlich) algorithmisch zu sein haben. Denn selbst wenn Geräte für sich eine „ethische“ Lösung errechnen könn(t)en: Was passiert, wenn zwei Autos verschiedener Hersteller aus unterschiedlichen Teilen der Welt mit einer jeweils ganz unterschiedlichen Ethik dennoch zeitgleich auf einer Straße fahren? In diesen Autos möchten wir vermutlich nicht sitzen.

Wolfgang Coy

Wolfgang Coy ist Informatiker und gestaltete den Fachbereich *Informatik und Gesellschaft* in Deutschland wesentlich mit. Er leitete die Forschungsgruppe *Informatik in Bildung und Gesellschaft* an der Humboldt-Universität zu Berlin und arbeitet aktuell im Interdisziplinären Labor *Bild – Wissen – Gestaltung*. Er ist im Beirat des FIfF.

Andrea Knaut

Sie haben den Nutzen der Technik noch nicht rational erkannt!

Biometrie verstehen und akzeptieren

„Du hast verdammt nochmal Gemüse zu essen, solange du deine Füße unter meinen Tisch stellst." – So manche Eltern erhoffen sich durch die Erklärung des funktionalen Sinns bestimmter Regeln, die Kinder auf etwas sanftere Weise zu erziehen als mit solchen Befehlen. Sie erhoffen sich allerdings seltener, dass ihr Kind dies als Neunmalklug zum Anlass nimmt, einen differenzierten Disput über den Sinn und Unsinn des Gemüseessens zu beginnen. Mit der Offenlegung aller Details und Hintergründe einer Regel wird nicht ihre Infragestellung bezweckt, sondern die Herbeiführung einer Einsicht in ihre Befolgung.

Die breite Einführung IT-gestützter Überwachungssysteme wird nicht selten in vergleichbarer Weise transparent gestaltet. Im Folgenden wird dies speziell am Beispiel biometrischer Systeme erläutert. Wir kennen sie inzwischen zur Genüge aus dem Alltag, seien es der TouchID-Sensor am iPhone, das Fingerabdrucklesegerät beim Meldeamt oder bei einer Grenzkontrolle, die biometrischen Passbilder für eine automatische Gesichtserkennung usf. Ein biometrisches System dient dem Mustervergleich digitalisierter individueller physiologischer Merkmale, um anhand dieser Menschen automatisch wiederzuerkennen. Manche werden diese Prozeduren nicht allzu sehr mögen und vielleicht soweit wie möglich auf sie verzichten.

Die Marketing-Strateg.innen der Unternehmen oder Politiker.innen, die biometrische Kontrollsysteme in Staaten mit halbwegs funktionierenden Grund- und Freiheitsrechten einführen wollen, sind im Idealfall stärker argumentativ in der Herbeiführung einer breiten gesellschaftlichen Einsicht in den Sinn der Technik gefordert. Eine gesellschaftliche Erziehungsaufgabe muss bewältigt werden.

> *„Fears about a global Big Brother will be* dismissed if end users are educated *about the workings and purpose of the biometric system."*[1]

Erziehungsziele sind, neben der Einsicht in Funktionsweise und Nutzen der Systeme, das Verhindern von Benutzungsproblemen und die Beruhigung der Ängste über einen ungenügenden Umgang mit persönlichen Daten. Statt Angst wird Akzeptanz benötigt. Diese lässt sich nicht nur durch begleitende Aufklärungskampagnen befördern, sondern auch durch ein entsprechendes Systemdesign. Akzeptanz ist hierbei nur ein Baustein eines komplizierten Puzzles. Kontextabhängig gilt es, diesen sinnvoll gegen die Kosten, die möglichen Angriffe auf ein solches System oder gar die Feinde einer biometrischen Anwendung abzuwägen.[2] Eine Leitfrage ist dann, ob es unter Berücksichtigung all dieser Kriterien überhaupt möglich ist, ein passendes System zu finden.

Obwohl biometrische Verifikation – wie die Anmeldung mit TouchID am iPhone –, insofern sie die Passworteingabe obsolet macht, als eine besonders gebrauchstaugliche Authentifizierungstechnologie (*usable security*) gilt, ist die Akzeptanzproblematik noch lange nicht vom Tisch. Selbst grundlegende Anforderungen nach herrschenden Maßstäben von IT-Sicherheit und Datenschutz sind bisher gar nicht oder nur teilweise in der freiwillig nutzbaren Alltagsbiometrie und der hoheitlichen erfüllt. Dazu gehören etwa rückrufbare und verschlüsselte Templates, die Einbettung des Gesamtsystems in eine PKI, eine möglichst lokale Speicherung und Verarbeitung oder die Verknüpfung mit Multi-Faktor-Authentifizierung.[3] Eine bequeme Benutzbarkeit wird bei Erfüllung dieser Anforderungen auch schon schwieriger realisierbar.

Neben der verbrieften Einhaltung von IT-Sicherheitsstandards lässt sich Akzeptanz zusätzlich mit geeigneter Visualisierung biometrischer Prozesse, ihrer Eingaben und Resultate herstellen.

Andrea Knaut

Vor acht, neun Jahren gingen Bilder des Prototyps eines ePass mit flexiblem AMOLED-Display durch die Presse.[4] Die Bundesdruckerei und Samsung hatten ihn in Kooperation produziert und tingelten damit über internationale Computermessen. Inzwischen hat Samsung die Forschung an transparenten OLED-Displays zunächst auf Eis gelegt, da es an Nachfrage mangele.[5] Als wichtiges Argument für den Einsatz von Displays in Passdokumenten nannte Manfred Paeschke, damals Leiter der Innovationsabteilung der Bundesdruckerei GmbH, dass die Transparenz der Technologie auch die gesellschaftliche Akzeptanz von elektronischen Dokumenten steigere. [6]

Gegenwärtig bewirbt die Bundesdruckerei den Mitarbeiterausweis *Go ID!* mit integriertem alphanumerischem Display so:

> *„Ein integriertes Display erleichtert die Nutzung. Dort werden Statusmeldungen und Hinweise angezeigt. So weiß der Inhaber immer, welcher Prozessschritt gerade erfolgt und was er als nächstes tun muss."*[7]

Ebenso bedeutsam aber ist die diskursiv begleitende Aufklärung über den allgemeinen Nutzen der Technik: Biometrie gilt als das Mittel zur Verhinderung der schwerwiegenden Bedrohung durch Identitätsbetrug. Ein historisches Anwendungsfeld ist die negative Identifikation, bei der festgestellt wird, ob ein

und dieselbe Person zum Beispiel unter verschiedenen Namen in einem System registriert ist. Schon der britische Kolonialbeamte William J. Herschel nutzte Fingerabdrücke nach diesem System. Er begann um 1860 herum in der Britischen Ostindien-Kompanie in Bengalen, die an die indischen Angestellten ausgezahlten Pensionen mit einem Fingerabdruck quittieren zu lassen, um doppelten Pensionsbezug zu verhindern.

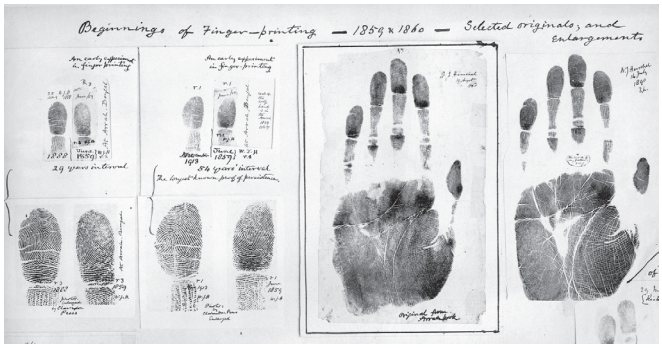


Abbildung 1: Die Anfänge der Daktyloskopie, Experimente mit Fingerabdrücken von William J. Herschel (1833–1917), die er in den Jahren 1859/1860 fertigte

Die koloniale Tradition setzt sich heute ironischerweise fort, wenn automatisierte Fingerabdruckidentifizierungssysteme europäischer Exportschlager für ehemalige Kolonialstaaten sind, wie zum Beispiel das Bank-Verifikations-Nummer-System in Nigeria. Es stammt von der deutschen Firma Dermalog, die auch in Deutschland der wichtigste Hersteller sämtlicher hoheitlicher Biometrie-Systeme ist. Im Auftrag der nigerianischen Regierung realisierte Dermalog das System im Rahmen der landesweiten „Kampagne gegen Korruption und Misswirtschaft [, die …] zur Streichung zahlreicher Stellen von Gehaltslisten des öffentlichen Dienstes [geführt hat]."[8]

Innerhalb der einstmaligen Kolonialmacht Großbritannien genügte der Öffentlichkeit das schwerwiegende Argument der Verhinderung des betrügerischen Mehrfachbezugs staatlicher Leistungen allerdings nicht als Grund für die Einführung einer *National Identity Card*. Die schon in die 1990er zurückreichende Idee wurde unter Blair mit dem *National Identity Card Act 2006*, mit dem auch ein zentrales *National Identity Register* geschaffen werden sollte, gesetzlich verankert. In dem Register sollten unter anderem biometrisch verwertbare Finger- und Gesichtsdaten abgelegt werden, die auch auf der Karte gespeichert würden. Als es 2007 einen Regierungswechsel zu der von den Konservativen geführten Koalition mit den Liberaldemokraten unter Premierminister Cameron gab, wurde das Gesetz in großen Teilen wieder einkassiert. Obwohl es in der Umbruchphase 2009 noch Versuche gab, das Projekt zu retten, gilt es heute als gescheitert.[9] Geblieben ist die im *UK Borders Act 2007* vorgesehene *Biometric Residence Permit* für Immigrant.innen, die nicht aus dem Europäischen Wirtschaftsraum kommen.[10] Prinzipiell bleibt die Karte damit infrastrukturell verankert, betrifft aber nur die, die sich ihr wohl am wenigsten widersetzen dürften.

Die National Identity Card gilt nichtsdestotrotz als eines der wenigen Beispiele, bei denen massiver öffentlicher Druck für das Scheitern eines nationalen biometrischen Ausweisprojekts entscheidend war. Hat hier also eine überwachungspolitische Lobbyarbeit mit angemessener „Transparenzrhetorik" versagt? Aaron K. Martin kam in einer diskursanalytischen Untersuchung des Falls zu dem Schluss, dass es das Fehlen einer sogenannten *organizing vision* war, die das Projekt zum Kippen brachte.[11] „Organizing visions function to mobilize actors for the purposes of materializing an innovation."[12] In diesem Fall fehlte es an einem Leitbild, das die Firmen, die dem Home Office helfen sollten, das *National Identity Scheme* zu bauen, die Einrichtungen des öffentlichen Dienstes, die die Technologie dann breit nutzen sollten, sowie die Öffentlichkeit unter einen Hut brachte. Martin benennt verschiedene politstrategische Verfehlungen in der Entwicklung. Dazu gehört, dass der fast einzige diskursive Fokus der Regierung auf dem logistischen Problem des massenhaften Enrolments und dem Bedarf an öffentlichen Ressourcen lag: Wie könne man doppelte Enrolments verhindern? Wie würde wirklich die gesamte Bevölkerung abgedeckt? Es gab dagegen kaum Verlautbarungen darüber, wie Organisationen die neue Karte nutzen würden und welche Probleme sie genau lösen würde. Außerdem kam es nie zu einem Large-Scale-Deployment. Nur 14.670 Briten hatten sich bis 2009 freiwillig erfassen lassen. Davon erhielten 3.000 auf Flughäfen kostenlose Karten und viele weitere waren mobilisierte Mitarbeiter des öffentlichen Dienstes. Die Politik versagte darin, möglichst viele Organisationen zu involvieren. Es formierte sich ein wirkungsvoller medialer Diskurs einer Opposition gegen die Karte. Dieser gelang es, auch im Appell an die national verankerten Gedanken von *citizenship, freedom and identity*[13] ausreichend Ängste zu schüren, dass die Regierung unschuldige Bürger.innen verfolgen und ihre Privatsphäre bedrohen würde. Eine wichtige Rolle in der öffentlichen Debatte spielten zudem an die Öffentlichkeit durchgesickerte Home-Office-Dokumente.

Auch in Deutschland ist der biometrische Teil des elektronischen Personalausweises bekanntermaßen bisher wenig erfolgreich, obwohl „die eingebaute Sicherheitstechnik gar nicht mal so schlecht" sei, schreibt Merkert 2016 in der c't. Verschlüsselungs- und Zertifizierungsarchitektur sind technisch gut überlegt, stattdessen aber habe das Bundesamt für Sicherheit in der Informationstechnik (BSI) „wirtschaftliche und gesellschaftliche Aspekte ignoriert."[14] So seien die Lesegeräte und die Zertifikate nach wie vor zu teuer, und die Software litt lange unter schlechter Wartung.

In bestimmten Anwendungsbereichen der Biometrie hat die Industrie weniger Überzeugungsarbeit nötig. Sind die von der biometrischen Erfassung betroffenen Personen sowieso schon weitestgehend rechtlos, wie es bei Asylbewerber.innen oder ohne gültige Papiere Aufgegriffenen der Fall ist, greift Biometrie am offensichtlichsten als autoritäres Instrument automatisierter Ressourcenverweigerung. Ein schon lange etabliertes Beispiel ist das automatische Fingerabdruckidentifizierungssystem Eurodac, das das Dubliner Übereinkommen umsetzen soll, nach dem der EU-Staat für einen Asylantrag zuständig ist, in den ein.e Asylbewerber.in zuerst einreist. In den verschiedenen Eurodac-Verordnungen wurden und werden zwar theoretisch im Rahmen der Datenschutzgesetzgebung der Europäischen Union Auskunftsrechte gewährt,[15] doch kaum eine.r nimmt sie in Anspruch. 2014 wurden bei 2,7 Mio. gespeicherten biometrischen Datensätzen lediglich 26 Abfragen im Sinne des Auskunftsrechts gestellt (2012: 111 bei 2,3 Mio. Datensätzen, 2013: 49 bei 2,4 Mio. Datensätzen).[16] Die Konsequenzen eines Eurodac-Treffers – Rückschiebung, menschenunwürdige Inhaftierung oder

Abschiebung – können lebensgefährlich sein. Doch greift der Schutz bürgerlicher Rechte nicht, ist die Akzeptanz der Technik nachrangig.

Als 2013 die neue Eurodac-Verordnung auch den Zugriff der Strafverfolgungsbehörden auf die Datenbank legalisierte, protestierten beispielsweise EU-Parlamentsabgeordnete der Grünen/Europäischen Freien Allianz gegen diesen schon frühzeitig von Kritiker.innen des Systems vorausgesagten Function Creep.[17]

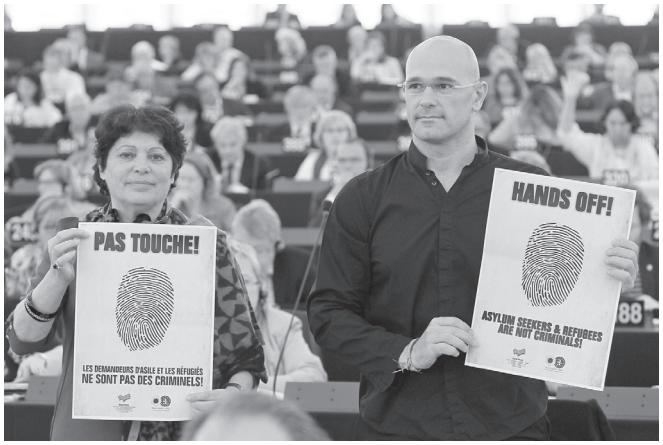


Abbildung 2: Finger weg! Asylbewerber.innen sind keine Kriminellen! – Proteste von EU-Parlamentsabgeordneten der Grünen/EFA gegen die Ausweitung der Zugriffs auf Eurodac für Strafverfolgungsbehörden, 12.6.2013

Die europäische Anti-Einwanderungspolitik bietet weiterhin das beste Testfeld für eine Überwachungsbiometrie, die kaum einer Rechtfertigung gegenüber ihren Usees bedarf und deren begleitende Auskunftsrechte nur noch in den Händen sehr standhafter Bürgerrechtler.innen zur Stärkung der Beweisfindung in einzelnen Rechtsverfahren von Nutzen sein dürften.

Bis hierher wurden beispielhaft verschiedene Strategien diskutiert, die Nutzer.innen Ängste vor einer vermeintlich falsch verstandenen Überwachungstechnik nehmen oder sie vor negativen Auswirkungen schützen sollen. Auf diese Weise können zwar durchaus transparentere Sicherheitssysteme entstehen, die allen Beteiligten mehr nutzen als schaden. Dies ist aber auch nur dann der Fall, wenn sie eben nicht allein als ein Instrument der Marktakzeptanz eines technischen Produkts dienen, sondern in Kauf genommen wird, dass es möglicherweise nie zu einer Markteinführung kommt. Denn ein sichtbar gemachtes Unrechtssystem bleibt ein Unrechtssystem. Informationelle Transparenz oder Sichtbarmachung erleichtert zwar erheblich die Wahrheitsfindung, ersetzt jedoch kein Urteil.

Anmerkungen

1 *Hervorhebung durch Autorin. Gary Roethenbaugh: »Truths and Myths« about biometric technologies. In: Biometrics explained. International Computer Security Association (ICSA), 1998, https://web.archive.org/web/19980529094811/http://www.icsa.net/services/consortia/cbdc/explained.htm (22.2.2017). Auf dem Text basieren große Teile des Biometrics Tutorial der ISO/IEC SC37 von 2007.*

2 *Ruud M. Bolle et al.: Guide to Biometrics. Springer: New York, 2004, p. 10.*

3 *Stefan G. Weber: Alltagstaugliche Biometrie: Entwicklungen, Herausforderungen und Chancen. iit perspektive Nr. 21, 2014.*

4 *Jens Ihlenfeld: ePass mit AMOLED-Display zeigt Bewegtbilder. golem.de, 21.5.2008, http://www.golem.de/0805/59848.html (23.2.17) und Detlef Borchers: Bundesdruckerei und Samsung kooperieren bei „3D"-Ausweisen. heise online, 11.12.2008, https://heise.de/-188949 (23.2.17).*

5 *Kim Young-won: Samsung Display stops producing transparent OLED. 26.8.2016, http://www.koreaherald.com/view.php?ud=20160826000325 (23.2.17).*

6 *omnisecure: Bundesdruckerei-Mitarbeiter für Innovationspreis Berlin-Brandenburg nominiert. 29.10.2007, https://www.omnisecure.berlin/de/news-pcb/unternehmen-pcb/1101-bundesdruckerei-mitarbeiter-fuer-innovationspreis-berlin-brandenburg-nominiert (23.2.17).*

7 *Bundesdruckerei GmbH: CeBIT: Bundesdruckerei zeigt Mitarbeiterausweis der Zukunft. 13.3.2015 https://www.bundesdruckerei.de/de/3865-cebit-bundesdruckerei-zeigt-mitarbeiterausweis-der-zukunft (22.02.17).*

8 *Dermalog: Bekämpfung von Identitätsbetrug. 8.3.2016, http://www.dermalog.com/de/news/de_Nigeria_2016.php (23.2.17).*

9 *Mit dem Identity Documents Act 2010 wurde die Gültigkeit der National Identity Card als offizielles Identitätsdokument außer Kraft gesetzt.*

10 *UK Visas and Immigration: Biometric residence permits: general information for applicants, employers and sponsors. July 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/539328/In-Country_information_leaflet_.-_July_2016.pdf (23.02.17).*

11 *Aaron K. Martin: National Identity Infrastructures. Lessons from the United Kingdom. In: ICT Critical Infrastructures and Society. Springer: Berlin, Heidelberg, 2012, pp. 44–55.*

12 *ebd., S. 51*

13 *ebd., S. 53*

14 *Johannes Merkert: Kontaktlos – nutzlos. Warum der neue Personalausweis auch nach fast sechs Jahren nicht durchstartet. In: c't 18/2016.*

15 *EU-VO 2725/2000, Art. 18 und EU-VO 603/13, Art. 29.*

16 *eu-LISA: Annual reports in the activities of the Central Unit of Eurodac, 2013, 2014, 2015.*

17 *Ska Keller: Neues europäisches Asylsystem. Stigmatisierung von Flüchtlingen als Kriminelle. 12.6.2013, http://www.gruene-europa.de/neues-europaeisches-asylsystem-10041.html (23.2.2017). Zum Function Creep siehe auch: Elif Mendos Kuşkonmaz: The Eurodac Debate: Is It Blurring the Line Between Asylum and Fight Against Terrorism? In: Annales de la Faculté de Droit d'Istanbul. 2013. S. 79–102, http://dergipark.gov.tr/download/article-file/7072 (23.2.2017).*

Andrea Knaut

Andrea Knaut ist Informatikerin und hat ihre Dissertation zum Thema *Fehler und Benutzungsprobleme von Fingerabdruckerkennungssystemen im gesellschaftlichen Kontext* geschrieben. Als wissenschaftliche Mitarbeiterin hat sie mehrere Jahre an der Humboldt-Universität zu Informatik und Gesellschaft und der Didaktik der Informatik geforscht und gelehrt. Sie ist aktiv in der Fachgruppe *Internet und Gesellschaft* der Gesellschaft für Informatik e. V. und Mitglied des FIfF e. V.

Informationen verstecken und Informationen herauskitzeln

Zusammenfassung des Vortrags von Gaby Weber

Wie kommen Bürger an staatliche Informationen? Da gibt es – grob gesehen – zwei Möglichkeiten: entweder man besorgt sie sich „irgendwie", indem man sich (physisch oder digital) dort „hineinschleicht" … aber das ist nicht immer legal. Oder aber man beschreitet den vorgesehenen Weg, der ist jedoch kompliziert, benötigt juristischen Sachverstand und verlangt einen langen Atem. Gut, und wie verhindern Regierungen den freien Informationszugang? Sie haben – grob gesehen – auch zwei Möglichkeiten, eine legale und eine illegale (aber tolerierte). Die legale Möglichkeit besteht darin, keine befriedigenden Zugangsgesetze zu erlassen, immer neue Ausnahmeregelungen zu schaffen, hohe Gebühren einzufordern und die Antragstellenden auf einen langen, kostspieligen Rechtsweg zu schicken. Die zweite Möglichkeit umfasst, dass Minister sensible Akten stehlen, diese mit nach Hause nehmen oder sie in einer privaten Stiftung ablegen. Das ist Diebstahl, wird aber toleriert; legaler Datendiebstahl sozusagen. Gaby Weber hat einige Fälle mitgebracht und Vorschläge präsentiert, was wir da tun können.

Souveräne Bürger.innen einer Demokratie haben die Aufgabe, sich zu informieren. Ein Rahmen dafür ist mit dem Informationsfreiheitsgesetz geschaffen, doch die Akten von Geheimdiensten bleiben dabei außen vor (was durchaus anzufechten wäre). Auch birgt das Gesetz noch immer diverse Probleme wie weitreichende Ausnahmeregelungen und deren noch weitreichendere Interpretationen durch die Behörden. Hindernisse wie Gebühren schüchtern Antragsteller.innen schon bei den ersten Schritten der Umsetzung ihrer Anfrage ein. Als Antragsteller.in muss ich zudem sehr konkret formulieren, welche Informationen erbeten werden, etwa um einer Interpretation meiner Anfrage möglichst wenig Spielraum zu geben – doch auf welcher Basis soll das möglich sein, wenn man bis Antragstellung noch keinen Einblick hatte und so das Wissen für die nötige spezifische Formulierung der Anfrage fehlt?

Gaby Weber

Für Demokratie und Antikorruption ist dennoch das Informationsfreiheitsgesetz (IFG) ein wichtiger Baustein, der die Bundes- und Landesarchivgesetze ergänzt, bei denen die Geheimdienste (noch) nicht ausgeschlossen sind. Nach derzeitiger Gesetzgebung sind aus diesen Behördenakten nach 30 Jahren angefragte Informationen freizugeben, solange keine Sperrerklärung der Dienstaufsicht vorliegt (z. B. des Kanzleramts für den BND).

Ein Beispiel für die langen und mühsamen Wege bei Informationsfreigabeforderungen sind die diversen Anfragen von Gaby Weber. 2008 erhob sie Klage zu den über 4000 Blättern zum Fall Adolf Eichmann, die der BND nicht herausgeben wollte. Durch das Archivgesetz konnten juristisch bis auf 100 schließlich alle freigegeben werden. Auch in Argentinien gab es eine Klage zur Freigabe der Regierungsabsprachen mit Israel. Solche zwischenstaatlichen Abmachungen sind nur schwer zu erhalten. Nicht unüblich ist zudem die Praxis der Dienststellenleiter, ihre Akten zu „privatisieren": sich zum Individuum statt als Amtsträger mit Staatsfunktion zu erklären und die – damit privaten – Akten einfach mit nach Hause zu nehmen. Nach dem Sterbefall landen sie dann z. B. bei der Konrad-Adenauer-Stiftung, welche wiederum ebenfalls privat ist und somit keine Verpflichtung hat, die Unterlagen zu veröffentlichen. In anderen Fällen gelangten Akten nicht ins Bundesarchiv, sondern stattdessen zum Historischen Institut der Deutschen Bank, in Privathäuser usw. Vorgänge wie diese sollten als Diebstahl gewertet werden und eine entsprechende Klage käme auch dem Sinn des Bundesarchivs gelegen, denn nur dort haben alle Forschenden gleichen Zugang, um Geschichte statt bloße Propaganda zu schreiben. Die Prozesskosten zu den Eichmann-Akten, über mehrere Instanzen laufend, belaufen sich inzwischen auf Tausende, doch durch solidarische Spendenaufrufe konnte bisher alles gedeckt werden. Im Verfassungsgericht wurden Gutachten verschiedener Institutionen zu den Machenschaften dieser umfassenden Geheimhaltung angefordert, doch Reaktionen blieben bislang eher aus.

Gaby Weber

Gaby Weber ist seit 1978 hauptberufliche Journalistin, arbeitete zuerst für den stern und ab 1981 für die ARD. Seit 1985 ist sie freiberuflich als Südamerika-Korrespondentin tätig. Für ihre Archivarbeit macht sie vom Recht auf Informationsfreigabe Gebrauch oder führt in diesen Angelegenheiten gerichtliche Verfahren gegen staatliche Institutionen zur Anerkennung dieses grundlegenden Rechts.

Die hiesigen Behörden wurden im Zusammenhang mit den Eichmann-Unterlagen auch zu Akten bezüglich der Militärdiktatur in Argentinien von 1975 bis 1983 angefragt, da in Deutschland sowohl Flüchtlinge als auch Solidaritätsgruppen in diesem Zeitraum überwacht wurden. Auch deutsche Firmen in Argentinien waren dabei nicht unbeteiligt und der BND hält stets durch Residenten in den Botschaften Kontakt zu befreundeten Geheimdiensten und -polizeien, so auch in diesem Fall. Doch lediglich 200 BND-Seiten wurden freigegeben, von denen manche jedoch einen Verweis auf den Verfassungsschutz als Mitempfänger enthielten. Der Zugang zu den für die Freigabe nötigen Findmitteln (Kataloge) wurde jedoch verwehrt – auch dagegen kann allerdings gerichtlich vorgegangen werden.

Um insgesamt mehr BND-Akten zugänglich zu machen und dennoch tatsächlich gerechtfertigte Geheimhaltung zu wahren, kann die Geheimhaltungsbedürftigkeit durch den Senat in einem In-Camera-Verfahren geprüft werden, bei dem via Gerichtsverfahren Urkunden oder Akten im Einzelfall geprüft werden. Der BND versucht jedoch, bei den von Gaby Weber angeforderten Akten eine generelle Sperrerklärung des Kanzleramtes zu erwirken. Begründet wird dies mit der Notwendigkeit, die Vertrauensbasis zu erhalten, auf welcher die Geheimdienste jeweils miteinander arbeiten. Am ungestörten Fortbestehen dieser geheimen Informationsflüsse habe auch die BRD ein Interesse. In Argentinien allerdings hat sich die Regierung für eine Deklassifizierung ausgesprochen, sodass es gut möglich ist, dass eine Sperrerklärung des Kanzleramtes ausbleibt. Die Akten des BND zur *Colonia Dignidad* in Chile wurden zwar angeblich notvernichtet und im Bundesarchiv seien nur noch wenige Blätter zu finden, doch Gaby Weber gibt die Hoffnung nicht auf. Vielmehr kritisiert sie, dass all dies unter der Verantwortung des Kanzleramtes geschieht.

Die so vehemente Geheimhaltung von Akten wurde in der sich Webers Vortrag anschließenden Fragerunde klar verneint und zu deren umfassender Freigabe ein Volksentscheid vorgeschlagen. Gabi Weber stellt den Nutzen von Geheimdiensten insbesondere deshalb auch generell in Frage, weil journalistische Korrespondent.innen vor Ort ihre Regierung oft besser informieren als deren eigene Geheimdienste mit ihren jeweiligen unsäglichen Verstrickungen, die das Freiklagen der Information überhaupt erst nötig machen. Hinzu kommt, dass Geheimdienste wie der BND sich großteils selbst vor allem aus öffentlichen Quellen informieren und das Geheimhalten von Informationen damit per se kaum begründbar ist. Drittens führt sie die Absurdität der auch internen Informationsfreigaben an: Etwa hat der Bundesrechnungshof keinen Zugang zu den Ausgaben der Dienste – eine adäquate Eigenkontrolle über Restaurantrechnungen und Bestechungsgelder für „Quellen" erscheint allerdings doch sehr fragwürdig.

Webers Fazit für den souveränen Bürger und die souveräne Bürgerin: Wer Informationen von Behörden erhalten will, sollte die Gesetze nutzen, eine Rechtsmittelbelehrung verlangen und gegebenenfalls dafür auch vor Gericht ziehen.

Sylvia Johnigk und Kai Nothdurft

We hate to say we told you so – IT-Sicherheit als Kriegshandwerk

IT-Sicherheit und Cyberwar stehen im Widerspruch zueinander, obwohl sich Militär und Geheimdienste Methoden und Wissen der IT-Sicherheit zunutze machen. Baut man Cyberwaffen und setzt sie ein, so schwächt man die Sicherheit der IT-Infrastruktur und daran angeschlossener Systeme. Für Cyberwaffen benötigt man geheim gehaltene Schwachstellen. Doch das Wissen um diese Schwachstellen bleibt nicht geheim, sondern gelangt irgendwann auch zu anderen nichtstaatlichen Kriminellen und gefährdet die IT-Sicherheit.

In unserem Vortrag auf der *FIfF-Konferenz 2016* am 27. November 2017 in Berlin haben wir exemplarisch gezeigt, wie Methoden und Werkzeuge der IT-Sicherheit zur (digitalen) Kriegsführung, dem Cyberwarfare verwendet werden. Dabei richteten wir den Blick sowohl zurück auf Prognosen, die wir in der Vergangenheit gestellt hatten, als auch in die Zukunft, mit neuen Prognosen, wie wir die weitere Entwicklung einschätzen. Wir zeigten anschließend Bezüge zwischen dem Tagungsthema *Un-*

sichtbare Systeme der FIfF-Konferenz 2016 und der digitalen Kriegsführung auf. Wir gaben Beispiele für teilweise Jahre zuvor von uns geäußerte Befürchtungen, die leider inzwischen eingetreten waren, bevor wir neue Prognosen stellten und einige bereits gestellte wiederholten. Schließlich erläuterten wir, warum Angriff im Cyberwarfare keineswegs die beste, sondern vielmehr eine schlechte Verteidigungsstrategie ist.

Schwachstellen

Unter Schwachstellen (engl. *vulnerabilities*) versteht man Eigenschaften eines IT-Systems, die Möglichkeiten bieten, in das System einzudringen oder eine ungewollte Veränderung vorzunehmen.

Wir sehen einige Ursachen für Schwachstellen in schlechtem Design und/oder mangelhafter Implementierung aufgrund von erheblichem Zeit- und Kostendruck. Dazu kommt Unwissenheit und mangelnde Qualifikation von Projektbeteiligten, insbeson-

dere von Entscheidern. Bei Kaufprodukten, Auftragsarbeiten und Outsourcing besteht in den seltensten Fällen eine Produkthaftung, was die Motivation schmälert, qualitativ ausgereifte Produkte zu liefern. Die Folgen von Sicherheitsmängeln tragen selten die Hersteller, manchmal sogar die Allgemeinheit.[1] Beispielsweise wurden einige von vielen Endanwendern genutzte Internet-Service-Dienstleister wie Twitter, Netflix, Spotify durch *Distributed-Denial-of-Service* (DDoS)-Attacken lahmgelegt, die durch unsichere Internet of Things (IoT)-Produkte anderer Hersteller möglich wurden.[2]

Kai Nothdurft und Sylvia Johnigk

Eine besonders gefährliche Quelle von Schwachstellen sind undokumentierte Funktionen oder versteckte Hintertüren in IT-Produkten.

Angriffe

Angriffe auf IT-Systeme können sehr unterschiedlichen Zielen dienen und unterschiedliche Schäden hervorrufen. Einige dienen der Spionage und Informationsgewinnung, bei gezielten Angriffen wird sogar kompromittierte IT in die Lieferkette eingeschleust.[3] Mit einem *Defacement*-Angriff werden die Inhalte und Darstellung von Webseiten verändert. Gegen die Verfügbarkeit richten sich *Denial-of-Service*-Attacken, aber auch weitergehende Sabotage-Angriffe, die bis zu physikalischen Schäden an der IT oder an von der IT gesteuerter Infrastruktur führen können.

Einige IT-Angriffe zielen auf Menschen selbst. Im *Information Warfare* werden *Social Bots* auch für Propaganda genutzt. Mit *Social-Engineering*-Attacken werden legitime Benutzer mit Trickbetrug dazu verleitet, dem Angreifer Zugriff auf das IT-System zu verschaffen.

IT-Angriffe gliedern sich typischerweise in mehrere Phasen: Sie beginnen mit der Informationsgewinnung, also dem Auskundschaften des anzugreifenden Systems. Neben einer Recherche von öffentlichen Quellen gehören dazu auch Port- und Schwachstellenscans. Danach erfolgt die Kompromittierung durch Ausnutzung einer Schwachstelle. Das System wird infiltriert, der Angreifer dringt ein. Hat sie oder er sich Zugang verschafft, ist das nächste Ziel, durch Privilegienerweiterung die vollständige Kontrolle zu erlangen und sich im System persistent festzusetzen. Ist der Zweck des Angriffs erreicht, werden zum Schluss noch die Spuren verwischt.

Verteidigung

Bei der Verteidigung gegen Angriffe gibt es präventive und detektive Methoden. Präventive Methoden greifen bereits vor dem Angriff und reduzieren die Angriffsfläche oder vermeiden Risiken. Dazu muss man seine IT-Systeme und die zu schützenden Informationen gut kennen, um sich auf die wichtigen Assets („Kronjuwelen“) konzentrieren zu können.

Die Ausfallsicherheit wird durch redundant ausgelegte Systeme erhöht. Segmentierung verringert die Vernetzung der Systeme untereinander und senkt die Querabhängigkeiten. Dadurch verringert sich die Komplexität (Fehleranfälligkeit) und die Größe der Angriffsfläche.

Eine sehr erfolgreiche Methode der Verteidigung ist die mehrschichtige Sicherheit (*security in depth*), bei der mehrere Sicherheitsmaßnahmen hintereinander greifen. Dies führt dazu, dass ein Angreifer mehrere Schutzmaßnahmen überwinden muss.

Häufig vernachlässigt wird ein effizientes, aktuelles und strukturiertes Identitäts- und Rechtemanagement. Nicht sauber gepflegte Zugriffsrechte bilden ein hohes Risiko.

Technische Maßnahmen wie die sichere Konfiguration von IT-Systemen (*Hardening*) oder das regelmäßige und zeitnahe Schließen von bekannt gewordenen Schwachstellen (*Patching*) müssen vollständig und mit der nötigen Sorgfalt durchgeführt werden. Regelmäßige Qualitätskontrollen wie Testen, Audits, Codereviews, Penetrationstests etc. ergänzen die obigen Maßnahmen.

Die wichtigsten Maßnahmen zur Detektierung von Angriffen, von deren Vorbereitung oder (zunächst) erfolglosen Versuchen bestehen im Aufzeichnen von sicherheitsrelevanten Ereignissen (*Logging*) wie Logon/Logoff, Veränderung von Zugriffsrechten und anderen Sicherheitsparametern. Diese „Spurensicherung“ muss aber durch regelmäßige Analyse dieser Log-Daten, durch Kontrolle und Überwachung (*Monitoring*) ergänzt werden. Der dafür nötige personelle Aufwand und die Reaktionszeiten können durch den Einsatz eines *Security Information and Event Management* (SIEM)-Systems reduziert werden. Ein SIEM-System analysiert Logfiles automatisch und reagiert regelbasiert auf Häufigkeit oder Kombination bestimmter Events durch Alarmierung. (Nur) auf bekannte Malware oder *Exploit*-Signaturen reagieren *Intrusion-Detection-Systeme* (IDS) mit Alarmen, *Intrusion-Prevention-Systeme* (IPS) blocken diese aktiv ab.

Eine besondere Form von Detektierungsmaßnahmen sind sogenannte *Honeypots*. Dabei handelt es sich um Systeme in größeren Netzwerken, die bewusst mit Schwachstellen versehen sind und Angreifern als leichte Beute erscheinen. Werden diese angegriffen, wird ein Alarm ausgelöst und die Aufmerksamkeit auf den Angreifer und seine Aktivitäten gelenkt.

Findet bereits ein Angriff statt, muss dieser abgewehrt werden; wenn er bereits erfolgreich war, sind Gegenmaßnahmen einzuleiten. Eine wichtige Basis dafür bilden klare Prozesse und Zuständigkeiten für das *Incident Handling* mit qualifiziertem Personal. Auch Krisenübungen dienen der Vorbereitung auf erfolgreiche Angriffe. Technisch kann mittels IPS oder Firewalls durch das gezielte Blocken der IP-Adressen, Geräte oder kompromittierter Accounts auf Angriffe reagiert werden.

Es gibt zudem Methoden, vermeintliche oder als tatsächliche Bedrohung identifizierte Systeme oder Benutzer zu bremsen. Gegen das automatisierte Durchprobieren von Passwörtern oder Denial-of-Service-Angriffe durch Logon-Versuche können *Captchas* eingesetzt werden, bei denen ein Rätsel gelöst werden muss, bevor der Logon erlaubt wird; nach Falscheingabe eines Passworts kann ein erneuter Eingabeversuch verzögert werden oder bestimmte Netzwerkverbindungen werden mit der Teergrubentechnik nur verzögert beantwortet.[4]

Von einigen im IT-Sicherheitsbereich arbeitenden Personen wird auch die Ansicht vertreten, dass das Angreifen eines identifizierten Angreifers zu den Verteidigungsmaßnahmen gehört. Durch Exploiten und Ausschalten greift man selbst das IT-System des vermeintlichen Angreifers mit einem Gegenangriff an und nennt dies Verteidigung. *Diese Ansicht wird von uns jedoch nicht geteilt.* Wir halten dies schon deshalb für extrem problematisch, weil insbesondere kurzfristig bei einer zeitnahen Gegenreaktion die tatsächliche Quelle eines Angriffs nicht zuverlässig identifiziert werden kann und die Wahrscheinlichkeit sehr hoch ist, dass nicht der eigentliche Angreifer, sondern ein von ihm als Angriffsbasis benutztes Opfersystem Ziel der Gegenmaßnahme wird. Dass Hacking-Angriffe nur schwer eindeutig einem Verursacher zugeordnet werden können, wird als *Attributierungsproblem* bezeichnet.

Häufig sind Verteidigungsmaßnahmen leider ineffizient. Dies liegt zum Teil daran, dass Maßnahmen falsch kombiniert oder mit einer inkonsequenten Strategie umgesetzt werden. Es gibt zahlreiche Standards und Prüfvorschriften, an denen sich Verantwortliche in Behörden und Unternehmen orientieren und die für offizielle Zertifizierungen verwendet werden. Problematisch wird dies, wenn ausschließlich auf die Einhaltung der Vorschriften geachtet wird, dabei aber wichtige Aspekte, die nicht explizit oder spezifisch gefordert sind, übersehen oder nicht berücksichtigt werden (*Security by Compliance (only)*). Ein plakatives Beispiel dafür war die Anschaffung einer Firewall, die dann aber gar nicht in Betrieb genommen wurde.

Ein weiteres Problem ist die Strategie, immer neue und teurere Security-Tools anzuschaffen, ohne gleichzeitig ausreichend viele qualifizierte Fachleute zu bezahlen, die diese auch bedienen können.

Außerdem existieren zahlreiche Produkte, die keine oder nur eine sehr eingeschränkte Schutzwirkung besitzen (*Snake-Oil*-Produkte), wie „Virenscanner" oder IDS-/IPS-Produkte, die ausschließlich signaturbasierte Malware-Erkennung verwenden und deshalb nur einen Bruchteil der Malware erkennen. Es existiert zudem eine Reihe von *Closed-Source*-Produkten, die mit herstellerabhängiger Beratung angeschafft oder implementiert werden, deren Schutzwirkung nicht überprüft werden kann. Dies ist insbesondere problematisch, wenn die Hersteller aus Staaten stammen, die nachweislich Wirtschaftsspionage oder Cyberwarfare betreiben, und damit von potenziellen Angreifern zur Kooperation genötigt werden können oder die Hersteller sogar deren strategische Partner sind.

NSA Strategic Partnerships, Folie aus den Dokumenten von Edward Snowden

Nebel des Krieges – unsichtbare Systeme

Die digitale Kriegsführung weist mehrere Bezüge zum Tagungsthema *Unsichtbare Systeme* auf: Schwachstellen werden geheim gehalten, um Exploits dafür in Cyberwaffen oder Staatstrojanern zu verwenden, infiltrierte Systeme dienen als stille Reserve von Angriffs-Bots, Überwachung und Spionage fanden lange unbemerkt und vor allem nicht offensichtlich und schwer wahrnehmbar statt. Die militärische Nutzung behindert eine freie IT-Sicherheitsforschung wegen der ihr zugrunde liegenden Geheimhaltungsinteressen. Die NSA hat heimlich offizielle Verschlüsselungsstandards geschwächt, indem mit Dual_EC_DRBG ein schwacher Zufallszahlen-Generator promotet wurde.[5]

Wie bereits erwähnt, werden häufig intransparente Sicherheitsmechanismen in Hardware und Closed-Source-Software eingesetzt oder absichtlich *Backdoors* in Hard- und Software zu Spionagezwecken oder *Lawful Interception* eingebaut. Mit der zunehmenden Verbreitung von IoT-Geräten können Schwachstellen in Haushaltsgeräten für DDoS-Angriffe genutzt werden, wobei die IoT-Geräte kaum als IT-Systeme wahrgenommen werden.

We hate to say, we told you so

Folgende unserer Befürchtungen (in kursiv) sind inzwischen leider eingetreten:

- *Jeder kann Opfer werden, auch Informatiker.innen und Administrator.innen (SIGINT 2012).* Admins der Belgacom wurden durch den GCHQ gezielt angegriffen.

- *Risiken steigen, kritische Infrastrukturen werden angegriffen:* Cyberwaffen gelten als nicht letal, die Einsatzschwelle ist niedriger, ein Cyberangriff gilt inzwischen als Bündnisfall

nach Art. 5 des NATO-Vertrags, *der Trend zum asymmetrischen Krieg wird verstärkt, besonders die industrialisierten Staaten sind durch Cyberwar bedroht*: Beispiel TV5-Hack.

- *Angriffe auf kritische Infrastrukturen:* fehlende, wegfallende Redundanz bei VoIP.

- *Attributierungsprobleme: Cyberattacken können* remote *aus großer Distanz, durch Anonymisierung oder indirekten Missbrauch von bereits kompromittierten Zwischensystemen Dritter ausgeführt werden, Spurenverwischung z. B. durch* Onion Routing *oder* Mixe*, keine physikalischen Spuren, nur Indizien, kein manipulationssicherer Nachweis möglich,* Information Warfare *beinhaltet auch Desinformation und Propaganda – das schließt ein, als Täter jemand anderen als den Angreifer zu diffamieren.* Nordkorea wird für den Angriff auf Sony verantwortlich gemacht, Russland für diverse Angriffe ohne handfeste Belege.

- *Risiken steigen, kritische Infrastrukturen:* In der *Shodan*-Suchmaschine für verwundbare Systeme tauchen französische Atomkraftwerke auf.[6]

- *IT-Insecurity: Informationssicherheit ist schwach verglichen mit steigenden Gesamtrisiken der IT:* Kein vertrauenswürdiges System, keine vertrauenswürdigen Komponenten, da (fast) alles kompromittiert und angreifbar ist, Hardware, Betriebssysteme, Lieferketten, Software.

- *Netzwerke sind verletzlich – durch falsche Bedienung oder Missbrauch.*

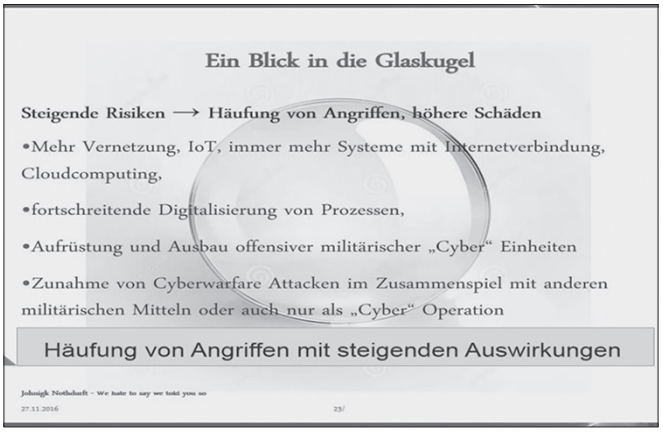
- *Ältere Internet-Protokolle oder -Dienste, die Angriffsfläche ist groß, Hardware und Software sind oft von außen angreifbar, IT-Projekte folgen der Zielsetzung in Budget, in Time, in Function, Verhinderung von unerwünschten Effekten (Absicherung gegen Angriffe) ist, wenn überhaupt, nur ein indirektes Ziel, das in Konkurrenz zu den anderen Projektzielen steht (Sigint 2012).* Der DDoS-Angriff auf Internet-Service-Dienstleister mittels IoT nutzte veraltete Protokolle und unsicher designte IoT-Geräte (siehe 2).

- *Vermischung von Cybercrime und Cyberwar, Kriminalität/Strafverfolgung und Cyberwarfare haben unterschiedliche Motivationen und unterschiedlich geeignete Gegenmaßnahmen (SIGINT 2012 Cyberpeace).* Es wird diskutiert, die Bundeswehr im Inneren zur Abwehr von Cyberangriffen einzusetzen und IT-Sicherheitsexperten aus der Wirtschaft zur Unterstützung zu verpflichten.

- *Illegales wird nachträglich legalisiert (INDECT Vortrag 2011).* Beispielsweise legalisiert das neue BND-Gesetz vormals illegale Praktiken.

Wir erwarten für die Zukunft folgende Entwicklungen:

1. *Das Gesamtrisiko steigt, da sich Angriffe häufen und jeweils höhere Schäden verursachen werden.*
   Ursachen dafür sind: eine immer stärkere Vernetzung bisher isoliert betriebener Systeme; Anschluss von schlecht gesicherten Haushaltsgeräten an das Internet (IoT), wodurch immer mehr Systeme mit Internetverbindung, aber ohne Security-Support existieren; Cloud-Computing-Lösungen als *Single Point of Failure* (SPOF) und attraktive Angriffsziele; fortschreitende Digitalisierung von Prozessen; Aufrüstung und Ausbau offensiver militärischer „Cyber"-Einheiten; Zunahme von Cyberwarfare-Attacken im Zusammenspiel mit anderen militärischen Mitteln oder auch nur als „Cyber"-Operation.



2. Es wird einen Trend zur Einschränkung freier Sicherheitsforschung geben. Das IT-Sicherheitsgesetz fordert akkreditierte IT-Sicherheitsunternehmen für die Beratung von KRITIS-Unternehmen (Betreiber kritischer Infrastrukturen). Nicht akkreditierte „Hackerbuden" oder unabhängige Untersuchungen werden dadurch benachteiligt. Anti-Hacking-Gesetze werden auf nationaler und internationaler Ebene ständig verschärft. Dies führt zu stärkerer Reglementierung (Erlaubnisvorbehalt für Sicherheitsüberprüfungen, Erhöhung des Strafmaßes, Absenkung der Strafbarkeitsschwelle). Dadurch wird eine unabhängige Sicherheitsanalyse und -forschung kriminalisiert.

3. Die aktuelle „Cyber"-Sicherheitspolitik der Bundesregierung und anderer Staaten gefährdet die IT-Sicherheit mehr als sie sie stärkt. Staatliche Stellen (BKA, Geheimdienste) kaufen weiterhin Schwachstellen für Staatstrojaner und Cyberwaffen. In vielen Staaten gibt es Einschränkungen in der Nutzung starker Kryptografie oder eine Pflicht zur Herausgabe von Schlüsseln (z. B. Frankreich, Großbritannien). Die Ausbildung von „Cyberkriegern" an den Bundeswehrhochschulen und das Verpflichten von Reservisten aus zivilen Bereichen für militärische Operationen führen dazu, dass diese Fachkräfte zur Verteidigung fehlen.

Risiken durch Geheimhaltung von Schwachstellen

Im letzten Teil des Vortrags erläuterten wir, warum wir die offensive Nutzung von Schwachstellen und Exploits für extrem gefährlich halten. Grundsätzlich erfordern *Zero-Day-Exploits* für Cyberwaffen geheim gehaltene Schwachstellen, um in offensiven Szenarios effektiv zu wirken. Geheimhaltung von Schwachstellen bedeutet aber gleichzeitig, dass nicht nur der Gegner, sondern auch die eigene Infrastruktur des offensiv agierenden Militärs sowie die Wirtschaft und Zivilgesellschaft des eigenen Landes gegenüber der Schwachstelle verwundbar bleiben (*Dual-Use-Dilemma*).

Geheim gehaltene Schwachstellen sind besonders gefährlich,

- da keine Gegenmaßnahmen ergriffen werden können, die Schäden vermeiden oder begrenzen,
- weil sie sehr lange existieren können,
- da sie sich dadurch in viele Implementierungen ausbreiten,
- da sie in Basiskomponenten eingebettet werden,
- da sie selbst bei Entdeckung dann nicht mehr kurzfristig beseitigt werden können, weil zu viele Abhängigkeiten bestehen und erheblicher Aufwand benötigt würde.

Ein weiteres Risiko besteht darin, dass behördliche Geheimnisträger die geheim gehaltenen Schwachstellen für „private" Zwecke verwerten können. Ihr „Marktwert" und die Replizierbarkeit stellen eine große Versuchung dar, sie weiter zu verkaufen. Wir wiesen bereits 2015 darauf hin, dass von staatlichen Stellen geheim gehaltenes Wissen um Schwachstellen nicht dauerhaft exklusiv und ausschließlich auf den Staat beschränkt bleibt (Conference Troopers, 19. März 2015). Im Oktober 2016 wurde bekannt, dass nach Snowden erneut ein NSA-Mitarbeiter Dienstgeheimnisse aus einem Zeitraum von 16 Jahren zu Hause gelagert hatte.[7] Ebenso erwähnten wir bereits 2010 das Risiko, dass Technologien auch an repressive Staaten geliefert werden könnten (SIGINT 2010 Indect, SIGINT 2012 Cyberpeace). 2015 wurde bekannt, dass die Firma *Hacking Team* über Jahre Spionagesoftware an autoritäre Staaten geliefert hatte.[8]

Angriff oder Verteidigung?

Schwachstellen veröffentlichen

Wir fordern deshalb, Schwachstellen zu veröffentlichen statt sie geheim zu halten. Es sollte sogar eine gesetzliche Pflicht zur Offenlegung bestehen. Dabei soll einer *Responsible Disclosure Policy* gefolgt werden, bei der den Verantwortlichen eine kurze Frist für die Behebung der Schwachstelle vor der Veröffentlichung eingeräumt wird, damit diese Patches bereitstellen und verteilen können. Das Melden von Schwachstellen an Behörden ist dabei nicht mit der geforderten Veröffentlichung zu vergleichen, solange die Behörden statt der Veröffentlichung auch die Geheimhaltung praktizieren.

Angriff ist nicht die beste, sondern schlechte Verteidigung

Wir kamen zu dem Schluss, dass Angriff im Cyberwarfare eine schlechte Verteidigung bedeutet:

- Krypto-Standards werden geschwächt (Dual_EC_DRBG in NIST),
- zahlreiche Systeme kompromittiert,
- um sie als Angriffs-Bot zu missbrauchen,
- oder um deren Informationen auszuspähen,
- Ressourcen und Knowhow werden für Angriffe statt für Verteidigung eingesetzt,
- freie Sicherheitsforschung wird behindert,
- Geheimhaltung von Schwachstellen verhindert das Patchen der eigenen Infrastruktur und den Schutz der Zivilgesellschaft des eigenen Landes,
- eine offensive Politik führt zu Eskalation und in eine Rüstungsspirale,
- und nationale Egoismen widersprechen globalem Handeln und internationaler Kooperation.

Rererenzen

1 *https://www.heise.de/security/meldung/DDoS-Untersuchung-Angriffe-werden-zum-Problem-fuer-die-Allgemeinheit-3631903.html*
2 *https://www.heise.de/newsticker/meldung/DDoS-Attacke-legt-Twitter-Netflix-Paypal-Spotify-und-andere-Dienste-lahm-3357289.html*
3 *Glen Greenwald: No Place to hide, S. 149, https://nsa.imirhil.fr/documents/no-place-to-hide.pdf*
4 *https://de.wikipedia.org/wiki/Teergrube_(Informationstechnik)*
5 *https://de.wikipedia.org/wiki/Dual_EC_DRBG*
6 *http://www.golem.de/news/it-security-atomkraftwerke-oft-ungeschuetzt-am-netz-1510-116694.html*
7 *https://www.heise.de/security/meldung/Juengster-NSA-Leak-16-Jahre-Geheimnisse-mitgenommen-3355278.html*
8 *https://netzpolitik.org/2015/hacking-team-wird-zu-hacked-team-400-gb-interne-daten-von-ueberwachungssoftware-hersteller-veroeffentlicht/*

Sylvia Johnigk und Kai Nothdurft

Sylvia Johnigk forscht und arbeitet seit über 25 Jahren im Bereich IT-Sicherheit, seit 2009 ist sie selbständige Beraterin in Großkonzernen. Ebenfalls seit 2009 ist sie im Vorstand des FIfF e. V.

Kai Nothdurft arbeitet als *Information Security Officer* in einer großen deutschen Versicherung. Seit 2009 ist Kai Nothdurft im Vorstand des FIfF e. V. aktiv. Seit Jahren hält er Vorträge und schreibt Artikel, die sich kritisch mit seinem Fachgebiet IT-Sicherheit beschäftigen.

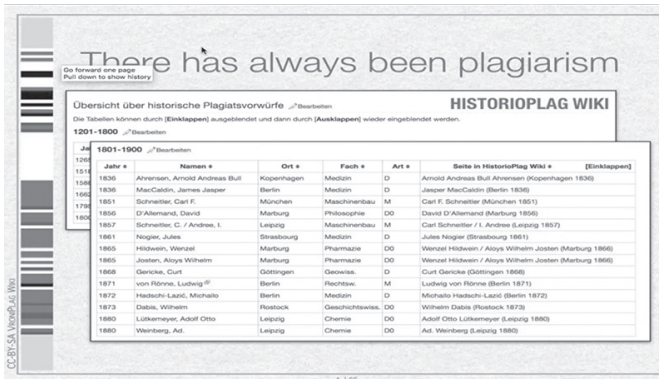
Viel Licht und noch mehr Schatten: Plagiat in Dissertationen

Zusammenfassung des Vortrags von Debora Weber-Wulff

Seit 2011 werden bei VroniPlag Wiki *Plagiate in Dissertationen dokumentiert, aktuell sind 177 Fälle publiziert worden. Obwohl diese Fälle nur die Spitze des Eisbergs sind, reagieren die Hochschulen teilweise sehr träge auf Plagiatsanzeigen, obwohl es durchaus Lichtblicke gibt. Interessanterweise sind die Dissertationen alle veröffentlicht, also eigentlich sichtbar für jeden. Nur, wie macht man Plagiate sichtbar?*

Kurzer Rückblick auf die Plagiatsskandale

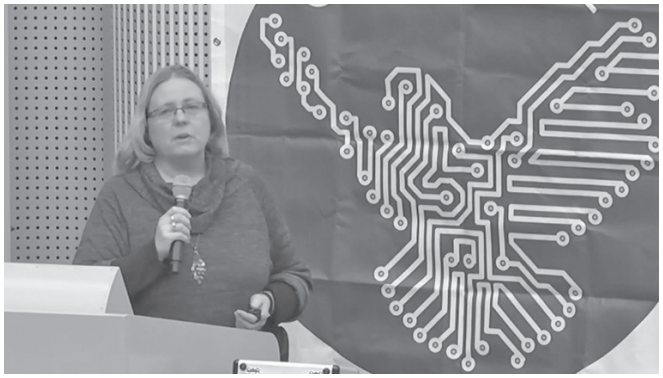
Dass es Plagiate gibt, ist nicht neu: Schon aus dem Jahre 1265 ist uns ein Vorfall überliefert; in den letzten Jahren sorgten Plagiate jedoch auch politisch für Aufmerksamkeit. Die Berichterstattung erzeugte dabei den Eindruck, allein die Technik habe ihr Aufdecken ermöglicht. Dies ist allerdings ein Missverständnis, ebenso wie die Annahme, dass es bei der großen Welle der Plagiatsvorwürfe nur um Dissertationen von Politikern gehe. Viel erschreckender ist die lange Liste der aktiven Dozent.innen und Forscher.innen, deren Arbeiten in den vergangenen Jahren als Plagiate enttarnt wurden. Von den insgesamt 177 Vorfällen auf *VroniPlag Wiki* sind der größte Teil Dissertationen, aber auch Habilitationsschriften und andere wissenschaftliche Arbeiten und Veröffentlichungen sind darunter. Betroffene Universitäten weisen die Verantwortung von sich oder spielen die Fälle herunter mit Hinweisen auf die „Fachkultur", verfallen jedoch dann in Aktionismus, wenn es um prominente Fälle geht. Auf der anderen Seite stehen die positiven Nachwirkungen: gezielte Plagiatsprävention wie Seminare zu wissenschaftlichem Arbeiten oder das *ReFAIRenz*-Programm der Uni Konstanz.



Übersicht über historische Plagiatsvorwürfe

Methoden zur Aufdeckung

Wie aber nun können Plagiate sichtbar gemacht werden? Hochschullehrer.innen wünschen sich am liebsten eine einfache und zuverlässige Software, die Plagiate „errechnet". Dadurch ist ein Markt entstanden, auf dem Softwarelösungen mit großen Versprechungen angepriesen werden; am Ende eines so automatisierten Prüfdurchlaufs steht dann eine Zahl, die in Einzelfällen bei Journals sogar schon als Ausschlusskriterium für Textzulassungen verwendet wird. Allein: Ob eine Originalität vorliegt oder nicht, darüber lässt sich nicht so einfach eine zweifelsfreie Aussage treffen, auch ist nicht jede mögliche Quelle der Texte zugänglich – es können höchstens Hinweise auf eventuelle Plagiate geliefert werden. Die Zahlen, die diese Programme



Debora Weber-Wulff

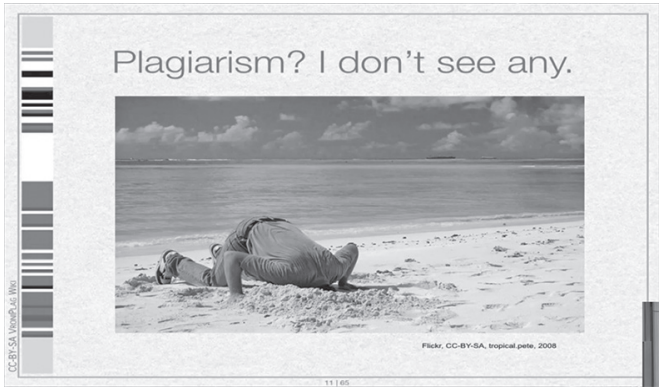
gewissermaßen als Quotienten einer Plagiathaftigkeit auswerfen, sind oft eher bedeutungslos und ändern sich auch nicht nachvollziehbar, sobald die Heuristik zufallsbasiert ist. Wenn darauf Abzüge in der Benotung basieren, ist das ein Problem, das alle wissenschaftliche Arbeiten betrifft. Falsch-positive Ergebnisse müssen die Grundannahme sein und gründlich überprüft werden. Dabei bleibt wie in den meisten Fällen computergestützter Entscheidungsfindung die Software nur ein Werkzeug, welches das kritische Lesen der Arbeit nicht ersetzt. Neben Auffälligkeiten wie unterschiedlichen Anführungszeichen oder Links innerhalb der Texte, die durch Kopiervorgänge entstanden sein können, sind Unregelmäßigkeiten in Formulierungen, Grammatik oder Zitierstilen Indizien für Plagiate, die eine genauere inhaltliche Untersuchung nahelegen.

VroniPlag Wiki (http://de.vroniplag.wikia.com/) nun verbindet beide Ansätze: Hinter dem Namen verbirgt sich eine Gruppe, die zwar auch Software nutzt, aber hauptsächlich selber liest, Gefundenes dokumentiert und darüber diskutiert. Ausgangspunkt kann dabei der Hinweis eines Whistleblowers mit manchmal nützlichen Zeugenberichten aus den unterschiedlichsten Motiven sein. Aber auch reine Neugier, Spielerei beim Durchforsten und Bauchgefühl können in Zufallsfunden von Plagiaten enden. Darüber hinaus können die algorithmenbasierten Analysen des *Textmining* als Methode hilfreich sein, um dementsprechende Quellen aufzuspüren. Wenn die Quelle jedoch nicht zu finden ist, kann auch kein Plagiat nachgewiesen werden.

Ein großer Vorteil in Deutschland ist, dass alle Dissertationen publiziert werden müssen. Als ein leichter Einstieg in die Plagiatsaufdeckung stellte sich die Medizin heraus, weil dort verhältnismäßig kurze Texte schnell und oft frei zugänglich publiziert werden. Während die Fakultäten selbst, in denen die betroffenen Texte erschienen sind, leicht auszumachen sind, ist das automatisierte Durchsuchen ihrer Websites (sog. *Crawlen*) kompli-

zierter. Besonders aufwändig ist die Vorarbeit zum eigentlichen Plagiats-Scan: die Daten aus etwa via Texterkennung nicht ganz fehlerfrei ausgelesenen PDF-Dokumenten zu bereinigen. Erst danach kann z. B. der Sim-Algorithmus von Dick Grune den Abgleich verschiedener Publikationen innerhalb einer Uni, zwischen verschiedenen Hochschulen und auch mit Wikipediaeinträgen gewinnbringend durchführen. Die große Anzahl an Kombinationen von Vergleichstexten stellt sich für die Prüfung dabei immer wieder als erhebliche Herausforderung heraus. Insbesondere gilt es abzuwägen zwischen einer mitunter langen Suchlaufzeit und der Qualität der Ergebnisse bzw. der Anzahl der in die Suche einbezogenen Texte. Plagiatsprüfungssoftware kann dabei freilich nicht nur exakte Übernahmen ganzer Sätze oder Abschnitte erkennen, sondern auch in der Arbeit umsortierte Teilsätze oder -abschnitte. Hilfreich für den Prüfer ist dabei auch die Darstellung: Beim Vergleich zweier Texte markieren farbige Unterlegungen jeweils gleiche Passagen visuell und machen so auf den ersten Blick Plagiate und auch die Plagiatsdichte sichtbar.

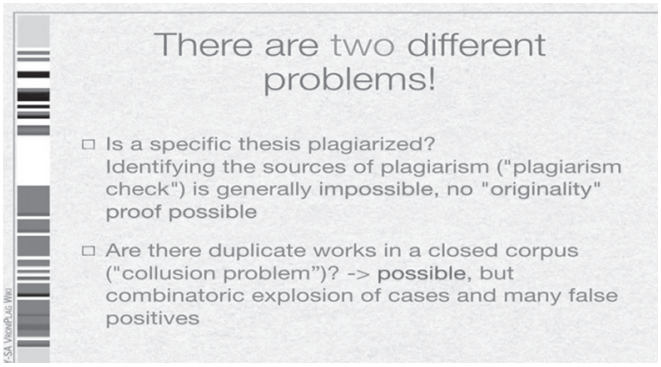
Ein hoher Prozentsatz an Übereinstimmung allein sagt jedoch wenig aus, so ist z. B. Zusammenarbeit kein Plagiat oder natürlich ist es möglich, die gleiche Arbeit selbst auch mehrfach an verschiedenen Stellen zu veröffentlichen. Auf der anderen Seite können auch Übersetzungen Plagiate sein, was weitaus schwieriger automatisiert zu erkennen ist. Der aufwändigste Schritt bei der Plagiatsprüfung ist jedoch die sich den Ergebnissen der computergestützten Prüfung anschließende manuelle Auswertung und Dokumentation, die durch mindestens zwei Personen gemeinsam geschieht und in einem Bericht mit Quellencluster und ggf. Plagiatsketten mündet.



Ergebnisse der Plagiatsprüfungsverfahren

Eine Erkenntnis der bisherigen Prüfungen ergibt, dass in vielen Fällen tatsächlich seitenlang Wikipediainhalte übernommen werden: Mindestens 58 Doktorarbeiten sind überführt worden. Es zeigt sich zudem, dass Plagiate ein universelles Problem sind, das in jedem Fach und an jeder Hochschule auftritt. Entsteht am Ende der Prüfungen aber nun mehr Licht oder mehr Dunkelheit?

Die sich aus den Plagiatsfeststellungen ableitenden und zu erwartenden Entscheidungen der Unis über die betroffenen Texte bzw. Autor.innen lassen oft unbestimmt lange auf sich warten. Sie bedeuten dann entweder den Entzug des Doktortitels oder enden in dem Beschluss, dass der Titel nicht (ausreichend) beeinträchtigt ist. Bedauerlicherweise versuchen Universitäten selbst nach Entzug des Doktortitels oft, die Einstufung der betroffenen Texte als Plagiate möglichst geheim zu halten. Da unter Beachtung der Persönlichkeitsrechte etwas wie ein entsprechender Google-Eintrag über eine Aberkennung durchaus diffizil ist, bietet sich als diskreter Mindestvorgang jedoch etwa an, bei den Bibliotheken, die die Texte führen, einen Zusatzvermerk zur Arbeit im Katalog anzulegen, der z. B. auf den Entzug des Doktorgrades für die Dissertation hinweist. Einen fragwürdigen Umgang mit den Texten pflegen darüber hinaus manche Universitäten, die das Einreichen einer korrigierten Version erlauben, in denen die im *VroniPlag*-Bericht nachgewiesenen Mängel behoben sind.



Was zu tun bleibt

Natürlich ist jedoch nicht das klassische Plagiat – die exakte Übernahme von Textpassagen – ein Problem, sondern auch das Verwenden der immer gleichen Ideen stellt keine gute wissenschaftliche Praxis dar. Hinsichtlich der Aufklärung und auch zukünftiger Plagiatsvorbeugung bleibt also noch viel zu tun. Ein weiterer Punkt ist dabei von großer Bedeutung: Maschinell können immer nur Textübereinstimmungen gefunden werden, letztendlich kann aber nur ein Mensch entscheiden, ob tatsächlich ein Plagiat vorliegt, am besten sogar vor Veröffentlichung des Textes. Dafür brauchen Doktorarbeitsbetreuer jedoch auch genügend Zeit, damit ihre ggf. aus der (Zeit-)Not entstandene Fahrlässigkeit nicht auch für sie ein Karriereende bedeutet. Plagiate müssen nicht nur als isoliertes Phänomen, sondern als Symptom eines kranken Systems gesehen werden, das auf schnelles Studium und einen hohen jährlichen Paper-Output statt auf tatsächliche Textqualität setzt. Statt nur die Auswirkungen zu behandeln, müssen auch die tatsächlichen Gründe für die Praxis des Plagiierens angegangen werden – auch mit soziologischer Forschung und mehr Aufklärung zum Thema wissenschaftliches Arbeiten.

Debora Weber-Wulff

Debora Weber-Wulff hat eine Professur für Medieninformatik an der Hochschule für Technik und Wirtschaft Berlin und arbeitet zu den Themen Plagiatsforschung, Medieninformatik, E-Learning, Softwaretechnik, Usability, Gender & Informatik und Ethik. Sie schreibt unter dem Namen *WiseWoman* an der Wikipedia und dem *VroniPlag Wiki* mit.

10 Jahre Informationsfreiheitsgesetz – Wie wir den Staat zu mehr Transparenz zwingen – Ein Stück in 3 Akten

Zusammenfassung des Vortrags von Arne Semsrott

Das Informationsfreiheitsgesetz feiert dieses Jahr seinen zehnten Geburtstag – und niemand feiert mit. Zwar ist der Zugang zu staatlichen Informationen längst als Teil der Menschenrechtskonvention und der Jahrhundertziele der Vereinten Nationen anerkannt. In Deutschland bleibt das Thema aufgrund mangelnden Engagements und schlechten Gesetzen aber meist unter dem Radar. Wie können wir das ändern? Und welche Mittel haben wir, um den Staat zu mehr Transparenz zu zwingen?

Akt 1 – Die Revolution

Das Informationsfreiheitsgesetz (IFG) ist im Kern ein revolutionäres Gesetz, denn es hat den *Default* der Informationspolitik in der deutschen Verwaltung grundlegend geändert. Es ist immer die Tradition des preußischen Obrigkeitsstaates gewesen, dass alle Informationen bei staatlichen Behörden liegen und als solche waren sie grundsätzlich erst einmal unzugänglich, es sei denn, Antragsteller.innen hatten ein berechtigtes Interesse daran. Staatliche Informationen waren damit Herrschaftswissen, das nur einer kleinen Elite aus Politik und Verwaltung vorbehalten war – ein enormer Wissensschatz. Dieses Herrschaftswissen ist jetzt durch das IFG der gesamten Öffentlichkeit, der gesamten Gesellschaft zugänglich. Damit änderte das IFG den Default-Zustand grundlegend: Alle Informationen, die bei staatlichen Stellen liegen, müssen nun prinzipiell herausgegeben werden, es sei denn, es gibt berechtigte Einwände, diese Informationen tatsächlich geheim zu halten. Die Grundprämisse – und das ist das Revolutionäre daran – hat sich damit vollkommen verkehrt.

Das IFG bezieht sich dabei zudem grundsätzlich auf alle Arten staatlicher Informationen; zudem haben alle Personen, ob juristische oder natürliche, das Recht – und in der Tat dasselbe Recht –, Anfragen zu stellen und die angeforderten Informationen zu erhalten. Egal ist dabei, ob man volljährig ist oder nicht, welchen Pass man hat, wo man wohnt. Zudem muss wirklich jede Behörde (mit wenigen Einschränkungen, s.u.) Auskunft darüber erteilen, wie sie Informationen speichert, und diese herausgeben. Dabei gibt es zudem keine Begrenzungen auf die Art der Informationen: Hierunter fallen ganz klassische Informationen wie schriftliche Vermerke und Gutachten, die bei den zuständigen Behörden liegen. Eingeschlossen sind aber auch Fotos und Videos, die etwa Polizeibeamte auf Demonstrationen aufnehmen. Ebenso müssen Briefwechsel oder SMS herausgegeben werden. *Informationen* ist also unabhängig von Speicherort und Form zu verstehen. Das bedeutet demnach auch, wir sind berechtigt zu erfragen, welche Nachrichten die Bundeskanzlerin (in ihrer staatlichen Funktion) sendet, welche Informationen der Innensenator an andere Referate oder Ministerien schickt und auch, was er erhält, z. B. von Lobbyisten. Wir können so viel detaillierter nachvollziehen, wie ein Gesetz zustande kommt und welche Korrespondenzen es dazu gibt (sofern sie schriftlich festgehalten wurden oder reproduzierbar sind). Auch Karten und Pläne oder Stiftungssatzungen und Verträge dürfen wir einsehen. Das heißt, nicht nur Informationen, die von Behörden selbst erstellt wurden, sind anfragbar, sondern grundsätzlich alle Informationen, die bei Behörden liegen, was auch z. B. die Satzungen privater Stiftungen wie der *Friede-Springer-Stiftung* betrifft. Denn genau wie alle anderen Stiftungen muss deren Satzung bei der Stiftungsaufsicht, also einer staatlichen Behörde, vorgelegt werden, um als gemeinnützig anerkannt zu werden.

Die Satzung der *Friede-Springer-Stiftung* wurde in der Tat von *FragDenStaat* etwa vor einem Jahr angefragt und nach Freigabe genauer studiert. Demnach erhalten alle Personen, die Mitglied des Kuratoriums sind, jeweils 10.000 € im Jahr für ihren Dienst. In diesem Kuratorium sitzen zum Beispiel Horst Köhler, der ehemalige Bundespräsident, und auch Joachim Sauer, der Ehemann von Angela Merkel. Er bekommt also jedes Jahr 10.000 € von Deutschlands mächtigster Verlegerin.

Aufklärungen dank IFG

Ein paar weitere Beispiele zeigen, was uns Bürger.innen die neue Informationsfreiheit konkret bringen kann:

- 2015 fragte *FragDenStaat* die Bundeswehr zu ihren PR-Kampagnen an: Die Plakate mit dem Slogan *Mach, was wirklich zählt* zur Gewinnung digitaler Kräfte sind vermutlich vielen bekannt. Die Bundeswehr versucht mit solchen Ansprachen derzeit, besonders junge Leute zu rekrutieren, weil ihnen Wehrdienstleistende fehlen. *FragDenStaat* wollte wissen, wo genau in Berlin die Bundeswehr plakatiert. Auf die Anfrage wurden sechzig Seiten mit den jeweiligen Adressdaten herausgegeben. Diese Adressen hat *FragDenStaat* in eine Karte übertragen, und so wurde sichtbar, dass es vor allem drei Bereiche gibt, in denen die Bundeswehr plakatiert: Das sind zum einen Schulen, vor allem weiterführende Schulen wie Gymnasien, zweitens Hochschulen, drittens *McFit*-Fitnessstudios. Das heißt im Umkehrschluss auch, wenn man in Berlin ein solches Plakat sieht, befindet man sich mit großer Wahrscheinlichkeit in der Nähe einer Schule, einer Hochschule oder eines McFit.

- Ein weiteres Beispiel sind Ausweise von Lobbyisten im Bundestag: Bis vor kurzem konnten sich Lobbyisten bei den Fraktionen registrieren, und diese durften dann Hausausweise frei vergeben. So ein Ausweis ermöglicht es, ohne sich zu registrieren (die übliche Praxis, um sich mit Abgeordneten zu treffen), den Bundestag frei zu betreten und wieder zu verlassen. Die Organisation *Abgeordnetenwatch* wollte vom Bundestag wissen, wer konkret einen solchen Ausweis erhalten hat. Vor allem die CDU/CSU-Fraktion, aber auch die SPD, haben sich lange geweigert, die Namen der betreffenden Personen bzw.

Organisationen herauszugeben. *Abgeordnetenwatch* hat allerdings geklagt, und sowohl das Verwaltungsgericht als auch später das Oberverwaltungsgericht haben klar angeordnet, diese Namen herauszugeben. Das hat nicht nur dazu geführt, dass der Bundestag letztlich die Namen von 3.000 Organisationen freigeben musste, sondern vor allem auch dazu, dass er diese Praxis eingestellt hat. Hier zeigt sich der weitreichende Nutzen des IFG: Erst dadurch, dass die Namen der Ausweisträger.innen öffentlich bekannt wurden, war es überhaupt möglich, eine Diskussion über die Zweifelhaftigkeit dieser Praxis zu führen, durch die einzelnen Personen ein privilegierter Zugang zum Bundestag möglich war – eine Diskussion, die dann schließlich sogar große Veränderungen nach sich gezogen hat. Dieser Fall ist damit einerseits ein ziemlich guter Beweis dafür, welche Macht es bedeutet, Informationen zu besitzen, und andererseits zeigt er, welche Machtverlagerung das konsequente Beharren auf das IFG bedeuten kann.

- Eines der bekanntesten Beispiele für Informationsfreiheit in Deutschland ist das Abendessen von Josef Ackermann im Bundeskanzleramt im Jahr 2008. Damals noch in seiner Position als Chef der Deutschen Bank hatte er seinen 60. Geburtstag im Bundeskanzleramt gefeiert; geladen waren u. a. Angela Merkel und diverse Firmenbosse, Verleger usw. Foodwatch-Chef Thilo Bode hat daraufhin Gästeliste und Rechnung angefragt. Schließlich war Veranstaltungsort das Kanzleramt und damit müssten beides staatliche Informationen sein. Das Kanzleramt hat sich jedoch gewehrt, Thilo Bode daraufhin über zwei Instanzen geklagt und schließlich wurde auch hier die Herausgabe entschieden. Das Wochenmagazin *Der Freitag* hat aus der freigegebenen Sitzliste, die zeigt, wer dabei war und wer wo saß, ein kleines Gesellschaftsspiel gemacht, was vor allem retrospektiv mit Blick darauf interessant war, wer von den Gästen während der fünf Jahre des Freigabeprozesses inzwischen wegen Korruption gerichtlich verurteilt worden war.

- Ein anderes Beispiel zeigt, dass sich mithilfe des IFG auch sehr gut herausfinden lässt, wie genau für Leistungen gezahlt wird, die für den Bund erbracht werden, z. B. von privaten Unternehmen – etwa wieviel das Logo für den in Deutschland abgehaltenen G7-Gipfel im Jahr 2015 gekostet hat.

Die Grafik zeigt eine Auflistung der gezahlten Gelder; demnach hat das Logo insgesamt fast 80.000 € gekostet. Es war ursprünglich wesentlich günstiger, aber dann kam die Krimkrise und Russland wurde aus der G8 verbannt. Als G7 musste das Logo geändert werden, was mehr als 20.000 Euro zusätzlich gekostet hat (wobei ein genauer Blick auf das Logo eine Lücke der 7 Stränge zeigt, in der einst Russland platziert gewesen sein mag).

- Ein dramatisches historisches Beispiel zur Aufklärung dank des IFG ist der Hauptbericht über die Evaluation der deutschen Entwicklungszusammenarbeit mit Ruanda, die 1998 abgeschlossen und erst in diesem Jahr durch *FragDenStaat* veröffentlicht wurde. Der Bericht kommt zu dem Schluss, dass Deutschland sich am ruandischen Völkermord, bei dem vor 22 Jahren knapp 800.000 Menschen umgebracht wurden, im Prinzip mitschuldig gemacht hat. Über viele Jahrzehnte hat Deutschland für Ruanda im Rahmen der Entwicklungszusammenarbeit eine wichtige Rolle gespielt, ist jedoch weder während der Gräueltaten noch danach wesentlich eingeschritten, obwohl es nachweislich viele Berichte von GIZ-Mitarbeiter.innen (Deutsche Gesellschaft für Internationale Zusammenarbeit, ehemals GTZ) an die Botschaft gegeben hat: zu einzelnen Massakern, zur politisch aufgeheizten Stimmung bis hin zu dem Aufruf, es müsse gehandelt werden. Die Evaluation deckt auf: Alle Informationen lagen vor, der politische Wille, aktiv gegen diesen Völkermord vorzugehen, war offenbar jedoch nicht da; kurz: Die Botschaft hat aktiv weggeschaut.

Warum jedoch werden diese Verfehlungen jetzt erst veröffentlicht? Die GIZ und das Bundesministerium für wirtschaftliche Zusammenarbeit hatten natürlich selbst kein Interesse daran; relativ früh aber haben auch Journalisten dieses 150-seitige Gutachten bekommen, es jedoch nicht publiziert, höchstens daraus zitiert oder darüber geschrieben. Hier wird ein riesiges anderes Problem offenbar: dass das IFG zwar genutzt wird, auch von immer mehr Journalisten, dass aber die Originale nicht veröffentlicht werden. Es hätte viel gebracht, wenn wir schon vor 20 Jahren diesen Bericht gehabt hätten, damit sich auch die Öffentlichkeit ein besseres Bild davon hätte machen können. Erst viele Jahre später können es nun alle nachlesen.

Akt 2 – Die Ernüchterung

Ausnahmeregelungen

Am Anfang stand die Revolution: das IFG. Dann jedoch wurden Schritt für Schritt Ausnahmen eingeführt, wie die Möglichkeit zum Ausnahmetatbestand, bei dem Informationen nicht herausgegeben werden müssen, wenn sie als nachteilig für die innere und öffentliche Sicherheit eingestuft werden. Wenn man sich in der Praxis ansieht, wie Behörden das interpretieren, dann kann das wirklich alles betreffen, und plötzlich gefährdet auch die Herausgabe des Namens einer Sachbearbeiterin schon die innere Sicherheit. Eine andere Ausnahme: die VS-Anordnung, die Anordnung zu Verschlusssachen. Was als *Verschlusssache* (VS) klassifiziert ist, muss nicht herausgegeben werden, aber die Vergabepraxis ist mitunter fragwürdig: Bearbeiter.innen erklären ihre Dokumente offenbar äußerst gerne als VS, manchmal auch erst dann, wenn sie zur Freigabe angefragt werden. Tatsächlich müssen sie diese dann nicht mehr herausgeben.

Gebühren

Ein zweiter großer Kritikpunkt an der Umsetzung der IFG-Anfragen sind die Gebühren: Deutschen Behörden ist es grundsätzlich möglich, für umfangreichere Anfragen Gebühren zu nehmen. Das ist international ein ziemliches Unikum: Deutschland ist das

Arne Semsrott

einzige Land in Europa, in dem regelmäßig Gebühren für IFG-Anfragen verlangt werden, teilweise in kuriosem Ausmaß. Ein Beispiel: Auf eine Anfrage an die Berliner Polizei gab es folgende Antwort: „Die erbetene Aktenauskunft würde bei dem mit dieser Amtshandlung betrauten Beamten einen Verwaltungsaufwand zur Vorbereitung dieser Auskunft von 0,25 h verursachen. Hierfür würde eine Verwaltungsgebühr von 13,94 Euro erhoben werden. Für die Übermittlung per E-Mail würde voraussichtlich 1,- Euro erhoben werden." Tatsächlich ist diese Praxis legal. Laut IFG von 1998 können für die Übermittlung von Anfragen per Post keine Gebühren erhoben werden, per E-Mail jedoch 1–2 €, es sei denn, es werden Dateien mitgeschickt, die zuvor bearbeitet werden mussten, dann kann eine Anfrage bis zu 13 € kosten. Diese Regelung führt dazu, dass, wenn die Berliner Polizei etwas schickt, bei dem z. B. die PDF im Anhang gelöscht werden muss, so werden auf Grund der „Veränderung" 13 € fällig. Im Bundes-IFG steht jedoch – wie auch im Berliner IFG –, dass Gebühren nicht abschrecken dürfen, weil private Bürger.innen damit vom Informationszugang ausgeschlossen werden könnten. In der Praxis zeigt sich allerdings, dass mehr als 80% der Anfragen, die über *FragDenStaat* an die Behörden gestellt werden und bei denen Gebühren angekündigt werden, nach dem Hinweis auf die Kosten zurückgezogen werden. Faktisch passiert also genau das, was laut Gesetz zu verhindern ist: Menschen werden vom Informationszugang abgeschreckt und sogar, wenn sie wenig Geld zur Verfügung haben, ausgeschlossen. Viele Schülerinnen und Schüler, die über *FragDenStaat* Anfragen an ihre Schulen stellen, fragen, nachdem sie von den Gebühren wissen, nie wieder nach.

Nichteinhaltung der Fristen

Die Revolution wurde durch einen dritten Aspekt noch ein bisschen kleiner: durch nicht eingehaltene Fristen der Behörden. Im IFG ist festgehalten, dass Behörden innerhalb eines Monats oder sogar unverzüglich zu antworten haben. Das Problem ist jedoch, dass, falls sie dem nicht nachkommen, dies keine Konsequenzen hat. *FragDenStaat* hat eine Statistik darüber erstellt, wie lange Bundesministerien im Schnitt brauchen, um auf Anfragen zu antworten. Von 14 Bundesministerien brauchen nur zwei im Schnitt einen Monat oder weniger, d. h. fast alle überziehen diese Frist, ohne dass Sanktionen erfolgen würden. Folglich gibt es offensichtlich auch keine Motivation, die Frist einzuhalten. Inzwischen haben sich die Datenschutzbeauftragten eingeschaltet, die leider aber weder auf Bundes- noch auf Landesebene Sanktionsmacht haben. Ihre Aufgabe ist zwar die Kontrolle, aber effektiv können sie nicht viel tun, weil sie lediglich beanstanden dürfen. In den meisten anderen Ländern mit vergleichbarem Gesetz wie dem IFG ist auch das anders geregelt.

Ausnahme: Geheimdienste

Ausnahmen gibt es auch für die Geheimdienste, d. h. es sind faktisch nicht alle Behörden verpflichtet, Anfragen zu beantworten: Der MAD, der BND und der Verfassungsschutz sind vom IFG ausgenommen. Der BND hat sich mit dem neuen Bundesarchivgesetz, beschlossen im Dezember 2016, nun auch vom Bundesarchivgesetz ausnehmen lassen. Alle Archivakten des BND, die nach Ablauf der 30-Jahres-Frist dem Bundesarchiv übergeben werden müssten, dürfen in Zukunft zurückgehalten werden, sofern der BND Einwände auf Grundlage des Quellen- und Methodenschutzes sowie des Schutzes der Identität von Geheimdienstmitarbeiter.innen bekundet *(Anm. d. Red.: nachträgliche Aktualisierung zum Gesetzesstand)*. Angesichts der bisher bekannten Verstrickungen in der Geschichte des BND lässt sich erahnen, was das zukünftig für die Aufklärung von Skandalen bedeutet wie dem zum Oktoberfestattentat, die Spiegelaffäre oder Geheimdienst-Affären.

Einschränkungen durch andere Gesetze

Auch andere Gesetze werden herangezogen, um Informationsfreigaben zu verhindern. Hindernis ist etwa oft das Urheberrecht, ebenso die Bedingung eines Identitätsnachweises als Antragsteller.in in Bremen und Rheinland-Pfalz: Hier kann man keine anonymen Anfragen mehr stellen, was für den Einzelnen durchaus abschreckend wirken kann.

Das Bundesgesetz legt weiterhin fest, dass Informationen aus Dokumenten, die Betriebs- und Geschäftsgeheimnisse betreffen, nicht herausgegeben werden müssen. In der Praxis bedeutet das, dass wann immer Unternehmen sich bei Informationen etwa zu Verträgen auf Betriebs- und Geschäftsgeheimnisse berufen, es keine Möglichkeit gibt, diesen Einwand abzuschmettern, denn zu beweisen, dass Informationen keine Betriebs- und Geschäftsgeheimnisse betreffen, ist nicht so leicht. In Konse-

Arne Semsrott

Arne Semsrott arbeitet für die *Open Knowledge Foundation Deutschland* und betreut dort das Portal zur Informationsfreiheit *FragDenStaat.de*. Außerdem leitet er bei *Transparency Deutschland* die AG *Wissenschaft* und ist Mitglied im Beirat des Whistleblower-Netzwerks.

quenz führt dieser Schutz mitunter zu massenweiser Schwärzung in Dokumenten, wie etwa bei der Anfrage der Deutschen Umwelthilfe nach dem Volkswagenskandal, bei der unter den 600 Seiten ein Blatt mit auch nur einzelnen lesbaren Zeilen eher die Ausnahme war. *FragDenStaat* ging es bei einer Anfrage zum selben Thema an das Wirtschaftsministerium nicht anders. Konkret bedeutet das, dass selbst bei einem Unternehmen wie VW, das mutmaßlich systematisch über viele Jahre hinweg betrogen hat, Betriebs- und Geschäftsgeheimnisse (im Klartext: die sich aus freigegebenen Informationen ggf. ergebenden wirtschaftlichen Nachteile) über das öffentliche Interesse gestellt werden.

FragDenStaat hat aus den zensierten Dokumentseiten etwas Neues gemacht: Kunstdrucke unter dem Titel *Limitierte Volkswagenedition* – für jedes neue Fördermitglied eine Seite.

FragDenStaat 2016. Limitierte Volkswagen-Edition. Giclée-Druck, mattes Papier, 20x30cm. Gerahmt, handgefaltet und handgelocht. Quelle: http://000000.limited/edition

IFG: nicht in allen Bundesländern

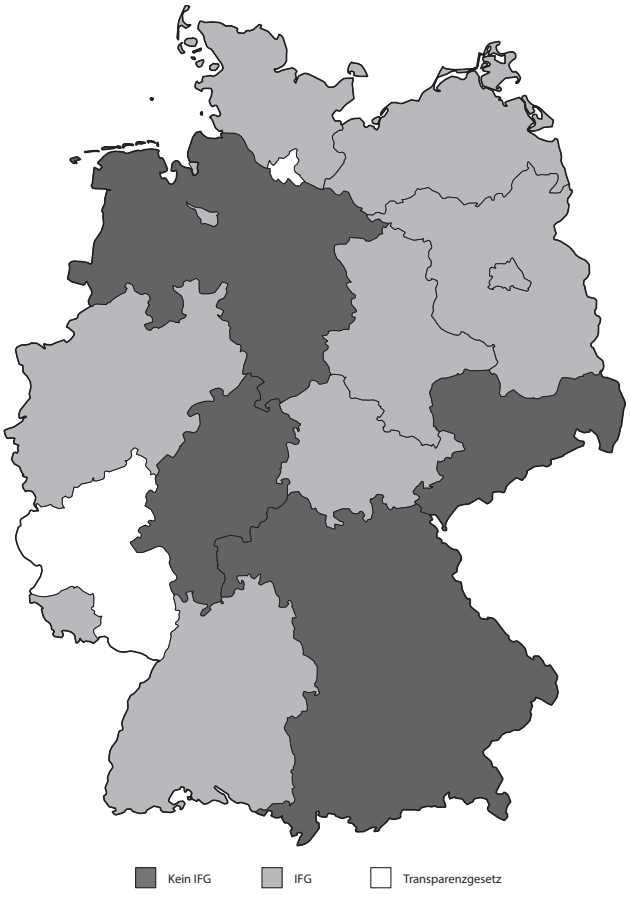
Zum Abschluss noch eine territoriale Ernüchterung: Deutschland hat noch vier große dunkelgraue IFG-Flecken: In Niedersachsen, Hessen, Sachsen und Bayern gibt es kein eigenes IFG (siehe Karte rechts). Das bedeutet: Alle Bundesbehörden müssen nach dem IFG Auskunft geben, alle Behörden in zwölf Bundesländern müssen Auskunft geben – nur diese vier Bundesländer folgen diesem Recht nicht – ein Recht, das übrigens als Recht auf Zugang zu staatlichen Informationen von den Vereinten Nationen inzwischen als Jahrhundertziel formuliert wurde.

Akt 3 – Recht und Ordnung

Gesetz ist Gesetz (?)

Im Diskurs um das IFG wird oft davon gesprochen, dass wir einen Kulturwandel in Politik und Verwaltung brauchen. Die Bundesdatenschutzbeauftragte Andrea Voßhoff hat dieses Jahr bei einem Symposium gesagt, das IFG sei in der Verwaltung angekommen. Das mag stimmen, das mag auch wichtig sein, aber was wir brauchen, ist, dass sich Politik und Verwaltung auch an die Gesetze halten. Das IFG existiert seit zehn Jahren und viele Behörden halten sich seit zehn Jahren nicht an seine – bindenden – Vorgaben. Wie es dazu kommen kann und warum das eines Kulturwandels bedarf, das ist absolut unverständlich. Wenn es eine Steuerreform gibt, dann fordert niemand einen Kulturwandel in der Bevölkerung oder schlägt vor, nach zehn Jahren einfach mal zu schauen, ob alle richtig ihre Steuern zahlen. Wir haben ein Gesetz und das muss befolgt werden, aber momentan wird es einfach nicht gut befolgt. Die Einstellung lautet: „*Not in my Backyard*" (NIMBY), das heißt, alle finden Informationsfreiheit und Transparenz wunderbar, es sei denn, es tangiert sie selbst.

Das betrifft ebenso die Landtage wie den Bundestag, der sich über Jahre dagegen gewehrt hat, dass seine Wissenschaftlichen Dienste alle Gutachten, die er von ihnen erstellen lässt, herausgeben müssen. Der Bundestag hat sehr lange nicht publiziert, zu welchen Themen er gearbeitet hat – über die Jahre handelt es sich dabei um tausende Gutachten, denn alle Abgeordneten des Bundestages können Ausarbeitungen anordnen, etwa zur Menschenrechtssituation in China, der Finanzpolitik in Berlin seit den 80ern oder der Verfassungspolitik in den USA (ein Gutachten von Herrn zu Guttenberg). Seit das Bundesverwaltungsgericht 2015 entschieden hat, dass all diese Gutachten auf Einzelantrag hin herausgegeben werden müssen, erfolgt dies nun nach und nach auch tatsächlich – wie etwa das sogenannte Ufo-Gutachten, das ein paar Exopolitiker angefordert hatten und das auf 10 Seiten darlegt, wie die Bundesregierung mit Ufos umgeht. Sie sind mit ihrer Anfrage über drei Instanzen gezogen und letztlich



Landkarte der Informationsfreiheit in Deutschland

musste es herausgegeben werden. Ein zweites Beispiel: die Gutachten, die Karl-Theodor zu Guttenberg bei den wissenschaftlichen Diensten in Auftrag gegeben hatte und die dann als Plagiate in seiner Doktorarbeit auftauchten. Manuel Bewarder (*Die Welt*), der diesen Antrag gestellt hatte, ist dafür vor das Bundesverwaltungsgericht gezogen. Auch hier wurde für die Herausgabe entschieden.

Freigabe der Bundestags-Gutachten

Durch diese zwei Beispiele wusste *FragDenStaat*, dass einzelne Gutachten herausgegeben werden können. Dem Bundestag haben sie daraufhin vorgeschlagen, dass, wenn all diese Tausende Gutachten nun herausgegeben werden müssen, es doch einfacher und logisch wäre, diese aktiv selbst zu publizieren. *FragDenStaat* bot dafür seine Hilfe über eigene vorhandene Tools an. Der Bundestag lehnte dankend ab. Um die komplette Herausgabe der Gutachten dennoch zu bewirken, startete *FragDenStaat* zusammen mit *Abgeordnetenwatch* eine Aktion: Auf Basis einer Liste mit 5.000 Gutachten wurden die Titel in eine gemeinsame Datenbank eingespeist. Mit einem Klick konnten Interessierte die Datenbank nach einem Thema durchsuchen, z. B. Drogenpolitik, und dann gezielt eine Anfrage nach dem zugehörigen Gutachten stellen. Das hat dazu geführt, dass innerhalb von zwei Wochen knapp 3.000 verschiedene Anfragen beim Bundestag eingegangen sind, was für den Bundestag eine große Herausforderung war. Für jede dieser 3.000 Anfragen hätte das bedeutet, beim Bundestag eine Anfrage auszudrucken, die Anfrage mit Aktenzeichen zu versehen, eine Eingangsbestätigung per Post an den/die Antragsteller.in zu senden (es wird alles per Post, nicht per E-Mail gesendet), zu prüfen, ob das Gutachten vorliegt, es auszudrucken, zu schwärzen, dem Vorgesetzten zur Freigabe zu schicken usw. Alternativ konnte der Bundestag entscheiden, dass alle Gutachten wie von *FragDenStaat* vorgeschlagen, einfach aktiv veröffentlicht werden sollen. Drei Wochen nach Beginn der Kampagne verkündete Bundestagspräsident Lammert die Entscheidung, alle Gutachten, die der Bundestag in der Vergangenheit angeordnet hat und alle Gutachten, die in Zukunft erstellt werden, aktiv auf der Bundestags-Website zu veröffentlichen.

Nachdem die vollständige Herausgabe erwirkt war, stellte sich allerdings die Frage, wie dieser Zugang überhaupt sinnvoll genutzt werden kann, insbesondere da die Suchfunktion dieser Website nicht besonders gut war. *FragDenStaat* hat daraufhin ein eigenes Projekt gestartet: Alle Gutachten wurden *gescraped* (automatisiert zusammengesucht) und auf sehrgutachten.de veröffentlicht. Dort stehen nun alle Gutachten nicht nur als PDF zur Verfügung, sondern auch als TXT- und JSON-Dateien, wodurch eine Volltextsuche möglich ist.

Mit dieser Aktion hat *FragDenStaat* jedoch noch mehr bewirkt: Es gibt nun diese technische Infrastruktur, mit der sich Listen einfügen lassen und massenhaft Anfragen an Behörden gestellt werden können. Das stärkt die Verhandlungsposition enorm, denn bei zukünftigen Anfragen zu umfassenden (Einzel-)Veröffentlichungen interessanter Dokumente können nun, falls die zuständigen Behörden eine allgemeine Herausgabe wie im Falle der Bundestags-Gutachten ablehnen, alle interessierten Menschen die einzelnen Anfragen schnell und einfach in großem Umfang stellen.

Freigabe von Dokumenten der Jobcenter

Auch das Jobcenter verfügt über besonders interessante Dokumente, die nach dem IFG uns allen zugänglich herausgegeben werden müssen. Dazu zählen etwa die internen Weisungen, die in Zusammenhang mit dem großen Ermessensspielraum z. B. über Sanktionen stehen. Es macht in der Tat einen großen Unterschied, ob das Jobcenter in Hamburg, München oder Sindelfingen über einen Fall entscheidet, denn jedes Jobcenter kann ziemlich autonom darüber entscheiden, ob es Sanktionen von 0 % oder von 20 % verhängt. Willkür ist damit Tür und Tor geöffnet. *FragDenStaat* will all die Zielvereinbarungen der Metaebene und die entsprechenden Weisungen aller Jobcenter in Deutschland veröffentlichen. Dazu wurde die Kampagne *FragDasJobcenter* ins Leben gerufen (*fragdenstaat.de/jobcenter*). Mit vorformulierten Anfragen lassen sich hierüber beim Jobcenter der Wahl ganz einfach Weisungen oder Zielvereinbarungen anfordern. So wird schließlich bei ausreichend Anfragen vergleichbar, wo besonders viel sanktioniert wird und wo nicht; außerdem können auf diese Weise ggf. rechtswidrige Weisungen oder Praktiken aufgedeckt werden, die gegen Grundrechte verstoßen.

Verweigerte Freigaben der Polizei

Problematisch ist es, wenn Behörden trotz IFG und keinen heranzuziehenden Ausnahmeregelungen oder Korrelationen mit anderen Gesetzen angefragte Informationen nicht herauszugeben bereit sind. Ein gutes Beispiel ist hier die Hamburger Polizei: 2014 gab es eine Anfrage über *FragDenStaat* an die Polizei dazu, ob es eine Datei zu Sportgewalt gebe. Die meisten Polizeibehörden oder Landeskriminalämter führen Dokumente, in denen registriert ist, wer z. B. ein potenzieller Hooligan ist oder in Verbindung stehen könnte mit radikalen Organisationen der Fußballvereine. Solche Listen sind schon bürgerrechtlich sehr problematisch, weil nur Verdachtsfälle gespeichert werden, niemand weiß genau, wer sie unter welchen Kriterien anlegt. Darüber hinaus wissen die Betroffenen nicht, dass sie in einer solchen Datei geführt werden; niemand weiß, was für Sanktionen möglicherweise folgen und vor allem wie Personen hieraus wieder gelöscht werden können. Die Anfrage an die Hamburger Polizei hat nach anderthalb Monaten ergeben, dass es nach eigener Aussage so eine Datei nicht gebe. Ein Jahr später fragte eine Abgeordnete der Linken ebenfalls nach einer Datei zu Sportgewalt. Die Antwort des Innensenats lautete, ja, es gebe sie seit neun Jahren.

Die große Frage ist: Wie kann das sein? Der erste Antragsteller fragte in Bezugnahme auf diese Datei erneut nach. Der Pressesprecher der Polizei antwortete ihm, es habe offensichtlich ein Missverständnis gegeben, er entschuldige sich sehr dafür, aber es gebe in Hamburg keine Sportgewaltdatei, sondern nur eine Datei „zur Szenen- und Gruppengewalt im Sport". *FragDenStaat* hat daraufhin die interne Kommunikation zu dieser Anfrage angefordert, alle E-Mails bekommen, die intern zur ersten Anfrage hin- und hergeschickt wurden. Es zeigte sich, dass das eine Referat dem anderen schrieb: „Hier geht es um die Datei Szenen- und Gruppengewalt, beantwortet ihr das." Daraufhin hat die Hamburger Polizei den Antragsteller schließlich belogen. In solchen Fällen gibt es auch nach IFG keine Hand-

habe gegen die Behörden, und für die Herausgabe der internen E-Mails berechnete die Hamburger Polizei *FragDenStaat* zudem 120 €.

Auf eine andere Weise unkooperativ zeigt sich derzeit die Berliner Polizei: Rainer Rehak vom FIfF hat angefragt, welche kriminalitätsbelasteten Orte es in Berlin gibt, und ein paar detaillierte Fragen zur Einstufung der Rigaer Straße und den durchgeführten Maßnahmen gestellt. Wie so oft hat die Berliner Polizei klar geantwortet, dass sie all diese Informationen auf Grund der Gefährdung der inneren Sicherheit nicht herausgeben könne. Es wird argumentiert, dass „staatliches Handeln, insbesondere polizeiliches Handeln nicht kalkulierbar oder voraussehbar sein [darf], da sonst die gesetzliche übertragene Aufgabe der Polizei zur Gefahrenabwehr und der vorbeugenden Strafverfolgung nicht mehr erfüllt werden kann". Wir haben also eine Polizei, die demokratisch überprüfbar sein soll, aber argumentiert wie ein Geheimdienst. Natürlich muss staatliches Handeln kalkulierbar sein, natürlich muss staatliches Handeln in einer Demokratie voraussehbar sein, denn wir müssen es ja – ganz im Sinne des IFG – überprüfen können. Diese wirklich obskure Argumentation darf so nicht stehenbleiben. Darum hat Rainer Rehak gemeinsam mit dem FIfF vor dem Verwaltungsgericht Klage gegen den Bescheid eingereicht und bisher zunächst zumindest teilweise Freigaben der Informationen erwirken können.

Das Recht erklagen

Mit Blick auf all die genannten Beispiele ist der richtige und einzige Schritt, um Behörden zu Recht und Ordnung zu verhelfen, offenbar, Freigaben anzufordern und ggf. auch zu erklagen. Immer mehr Interessierte stellen Anfragen über *FragDenStaat*, auch immer mehr Journalist.innen. Die anfallenden Gebühren können sich Antragsteller.innen inzwischen dank einer Initiative von *FragDenStaat* und Wikimedia von einem dafür geschaffenen Fonds erstatten lassen. Inzwischen ist es aber ein Modus Vivendi geworden, eine Ablehnung zu bekommen. Um diesen Kreislauf zu durchbrechen, müssen wir klagen, was an sich ziemlich einfach ist: Man stellt eine Anfrage, bekommt einen Bescheid, reicht Widerspruch ein, bekommt einen Bescheid – und klagt. Dabei hilft die Seite *VerklagDenStaat*. Leider kostet aber auch das Klagen nicht wenig. Wir müssen jedoch viel mehr fragen und viel mehr klagen, denn wenn wir das konsequent tun, kommen wir auch wieder zum ursprünglichen Sinn des IFG zurück – der Revolution.

Referenzen

https://fragdenstaat.de/
http://www.abgeordnetenwatch.de/
https://verklagdenstaat.de/

FIfF-Konferenz 2016

Social Media in Südkorea: Staatliches Machtinstrument vs. „fünfte Gewalt" in einer defekten Demokratie

Zusammenfassung des Vortrags von Ok-Hee Jeong

Seit der Gründung der Republik 1948 herrschten jahrzehntelang Diktatoren über Südkorea. Erst Ende 1980 gelang es den Bürgern, sich die Demokratie zu erkämpfen. Dennoch ist das Erbe der Diktaturzeit immer noch nicht überwunden. Mittlerweile nennt sich Südkorea stolz eine „digitale Supermacht". Nirgendwo sonst ist die Infrastruktur des Internets so fortgeschritten wie in Südkorea, sind die Internetverbindungen so schnell und die sozialen Netzwerke so unentbehrlich. Der Geheimdienst und eine Cybereinheit des Militärs machten sich bei der Präsidentschaftswahl 2012 genau das zunutze und führten mithilfe der Social Media für den Wahlsieg der jetzigen Präsidentin Park Geun-hye verdeckt Wahlkampf. Wie der Staat mithilfe der Social Media die Bürger manipuliert und lenkt, aber gleichzeitig wie unentbehrlich die Rolle der Social Media als „fünfte Gewalt" in dieser defekten Demokratie ist, soll in diesem Beitrag anhand einiger Beispiele beleuchtet werden.

Die *digitale Supermacht* Südkorea

Als *digitale Supermacht*, so bezeichnet Südkorea sich stolz selbst – und in der Tat ist in keinem anderen Land die Internet-Infrastruktur so ausgebaut wie hier, sind die Internetverbindungen so schnell und die sozialen Online-Netzwerke so unentbehrlich: 94 % der südkoreanischen Bevölkerung nutzen das Internet – weit mehr als 41 Mio. Menschen; 88 % der erwachsenen Südkoreaner benutzen heute ein Smartphone (Zahlen des Meinungsforschungsinstituts *Pew Research Center*, 2016), laut KISA (*Korean Internet and Security Agency*) nutzten 2014 60,7 % Social Media, Tendenz steigend, die beliebtesten sind dabei mit 73 % *Facebook* (wobei der Anteil der Teenager und jungen Erwachsenen bis 30 um 90 % liegt), gefolgt von dem koreanischen Social Network *Kakaostory* (51 %) und *Naver Band* (40,1 %). Die durchschnittliche tägliche Smartphone-Nutzungsdauer lag 2014 bei 2 Stunden 51 Minuten, was gegenüber dem

1.2 Aktuelle Daten und Statistiken: Internet in Südkorea

Internet (PC und Smartphone)

- 94 % der südkoreanischen Bevölkerung nutzen das Internet (mehr als 41 Mio. Menschen)
- 88 % der erwachsenen Südkoreaner benutzen ein Smartphone (2012: 65%)
- Beliebte soziale Netzwerke: 73% Facebook, 51% Kakaostory, 40,1% Naver Band etc.

Vorjahr eine Steigerung von 38 Minuten bedeutete. Anzunehmen ist, dass die Zahlen inzwischen weit höher liegen. Das Bild der permanent auf ihre Smartphones starrenden Südkoreaner ist damit kein Klischee, sondern entspricht unübertrieben der Realität.

Ok-Hee Jeong

Da der Begriff *Social Media* oft sehr schwammig verwendet wird, an dieser Stelle eine kurze Definition: Im Folgenden wird *Social Media* verwendet als Überbegriff für Medien, in denen Internetnutzer.innen ihre Meinungen, Eindrücke, Erfahrungen oder Informationen austauschen und Wissen sammeln. Social Networks, Weblogs, Microblogs, Wikipedia und Foto- und Videoplattformen gelten ebenso als typische Vertreter sozialer Medien wie Chats und Diskussionsforen, virtuelle Kontakt- und Tauschbörsen und bestimmte Apps zur Kommunikation und Bewertung.

Wie werden diese sozialen Medien in Südkorea nun hauptsächlich genutzt? Zentrale Aspekte sind Informationsbeschaffung (99 %) und Kommunikation (97,5 %), einschließlich das Sich-Informieren über die online verknüpften Freundeskreise sowie das Reagieren aufeinander. 63,6 % der Südkoreaner halten Informationen, die sie aus den Social Media haben, für glaubwürdig; ebenfalls 63 % haben das Gefühl, über die sozialen Netzwerke frei ihre Meinung äußern zu können, was die Social Media zugleich über ihren Informations- und Vernetzungsaspekt hinaus zu einem wichtigen Instrument des demokratischen Grundsatzes der Redefreiheit macht.

Warum aber hat ausgerechnet Südkorea eine so enorme Technikaffinität? Wer die rasante IT-Entwicklung und große Liebe zur Technik verstehen will, muss einen Blick zurück auf die Asienkrise 1997/98 werfen. Deren Überwindung ist in Südkorea eng damit verknüpft, dass die demokratische Regierung von Kim Dae-jung (1998-2003) ihr einen neuen wirtschaftspolitischen Schwerpunkt entgegensetzte: die IT-Technologie. Hohe staatliche Förderung von Existenzgründungen im IT-Bereich, genauer für Informations- und Kommunikationstechnologien, sowie in der Medienindustrie, vergünstigte Tarife für Telekommunikation, kostenlose Computerkurse für Frauen waren Teil eines umfassenden Maßnahmenkatalogs. Der Kauf und damit die Nutzung von Computern wurde intensiv gefördert, alle Schulen erhielten Breitbandzugang zum Internet und alle Klassenräume und Lehrerzimmer wurden mit Computern ausgestattet. Diese neuen Ansätze der Wirtschaftspolitik Südkoreas waren in der Tat ein voller Erfolg und führten zur digitalen Revolution des gesamten Landes, wie sich etwa an den steigenden Zahlen der Internetnutzung zwischen 1998 (14.000) und 2002 (über 10 Mio.) ablesen lässt.

Social Media als willkommenes Korrektiv und Instrument der Öffentlichkeit

Um die große und auch zwiespältige Rolle der Social Media in Südkorea zu verstehen, ist es hilfreich, sich die Bedeutung der herkömmlichen Medien im Land vor Augen zu führen. Es gibt im Wesentlichen drei große Zeitungen: die *Chosun Ilbo*, die *JoongAng Ilbo* und die *Dong-A Ilbo*. Zusammen haben sie einen Marktanteil von 70 %, zudem folgen sie derselben politischen Ausrichtung (rechtskonservativ). Damit haben sie einen enormen Einfluss auf Politik und Öffentlichkeit: Sie definieren politische Belange und die öffentliche Themensetzung nahezu allein. Problematisch jedoch ist insbesondere ihre extreme Nähe zur Regierung: Sie gelten zu Recht als die mächtigsten Instrumente südkoreanischer Politik und sind damit keine Kontrollinstanz des Staates im Sinne einer notwendigen „vierten Gewalt", sondern Verbündete der konservativen Kräfte.

Cyber-Wahlskandal 2012

- Astroturfing (Vortäuschen von Grassroots-Bewegung bzw. Basisbewegung) durch die sogenannten Internettrolle.
- Die Internettrolle bei diesem Skandal:
  - Abteilung für psychologische Kriegsführung des südkor. Geheimdienstes: Rund 70 Agenten unter der Leitung des Geheimdienstchefs Won Sei-Hoon
  - Einheit 530 der militärischen Cyberabteilung: 120 Soldaten unter dem Kommando von Yeon Jae-Wool und Ok Do-Gyoung
  - Organsiation „Shibaldan" (Kreuzzugs-Trolle) unter der Leitung vom Pastor Yoon Jung-Hoon
  - Vom Geheimdienst angeheuerte Internettroll-Jobber

Der Korruptionsskandal um die südkoreanische Präsidentin Park Geun-hye (jahrzehntelang soll Choi Soon-sil, eine Freundin der Präsidentin, Einfluss auf die Regierungsarbeit genommen haben, ohne offiziell ein Amt zu bekleiden, was zahlreiche Proteste der Bevölkerung und die Forderung nach dem Rücktritt Parks sowie schließlich ein Amtsenthebungsverfahren zur Folge hatte) macht die Manipulation und Einflussnahme der drei Großen auf die Öffentlichkeit besonders deutlich: Die Vorwürfe gegen Park waren bereits Mitte September 2016 bekannt; in besagten Zeitungen gab es dennoch einen Monat lang zunächst keine Berichterstattung, dann nur zu weitaus geringeren Anteilen als in den kleineren, unabhängigen Medien. Dass nur regierungskonforme Nachrichten an die Öffentlichkeit gelangen, wird in „öffentlich-rechtlichen" Einrichtungen, wie etwa auch dem Fernsehsender *KBS (Korean Broadcasting System*, die größte Rundfunkanstalt Südkoreas) u. a. mit unrechtmäßigen Praktiken wie gezielten Fragen nach Regierungsloyalität und politischer Gesinnung der Journalist.innen in ihren Einstellungstests erreicht (etwa „Was denken Sie über die Linken?", „Stehen Sie zu der in der vierten Strophe der südkoreanischen Hymne besungenen Loyalität?" „Werden Sie in die Gewerkschaft eintreten?").

Angesichts dieser deutlich einseitig agierenden Medienlandschaft Südkoreas lässt sich plausibel erklären, warum sich Ende der 90er-Jahre mit dem Zugang zum Internet rasch eine alternative Öffentlichkeit herauszubilden begann, mit der sich auch alternative Informationskanäle langfristig etablieren konnten, wie die Erfolgsgeschichte der Bürgerzeitung *OhmyNews* zeigt: In den letzten Tagen vor der Wahl 2012 wurde sie täglich über 10 Millionen Mal aufgerufen.

Ein zweiter Faktor, der die tragende Rolle der sozialen Medien in Südkorea maßgeblich vorangetrieben hat, ist das 2009 von der rechtskonservativen Regierung erlassene neue Mediengesetz, das u. a. den großen Zeitungshäusern den Einstieg in den Fernsehmarkt ermöglichte und daher zu großem Protest von Öffentlichkeit und Opposition geführt hatte. Kritiker befürchteten, die drei großen, ohnehin bereits sehr einflussreichen Zeitungen könnten den Medienmarkt so völlig entdemokratisieren. In der Tat ist seither ein Rechtsruck sowohl in der Medienlandschaft als auch in der Bevölkerung festzustellen. Man verurteilt zunehmend Demokratiebewegungen als „nordkoreanische Machenschaft" und schürt gezielt Ängste vor einem Angriff durch den Nachbarstaat. Nie zuvor wurde so viel über Nordkorea als Aggressor berichtet, gegen den es sich zu wappnen gilt – ebenso wie im Übrigen gegen die linken (und damit pronordkoreanischen) Kräfte im eigenen Land. Gezielt verschwiegen werden dagegen etwa Korruptionsfälle der Großunternehmen südkoreanischer Politiker.innen oder weitreichende Fälle von Machtmissbrauch durch die Regierung wie die Auflösung und das Verbot der linken Partei UPP ohne Abstimmungsverfahren oder der inzwischen aufgedeckte Fall von Dokumentenfälschungen zu einem angeblich nordkoreanischen Geheimagenten durch den südkoreanischen Geheimdienst. Ganz klar muss den (Staats-)Medien damit ein Machtkartell des Schweigens vorgeworfen werden; die Pressefreiheit, wesentlicher Bestandteil einer intakten Demokratie, ist insbesondere unter Präsidentin Park Geun-hye massiv untergraben worden, wie auch die aktuelle Rangliste der *Reporter ohne Grenzen* aufzeigt, laut der Südkorea im Laufe ihrer Amtszeit auf den 70. Rang (von 180) zurückgefallen ist.

Fokus Kerzenscheindemonstration, Wahlkampf und das Schiffsunglück der *Sewol*

Dieser Einblick in die traditionelle Medienlandschaft Südkoreas macht die gestörte Demokratie des Landes deutlich und erklärt, warum die sozialen Netzwerke hier so rasant eine so große Bedeutung einnehmen konnten und auch, welche Rolle sie heute spielen. Wie der Staat mithilfe der Social Media die Bürger manipuliert und lenkt, wie unentbehrlich anderseits jedoch die Rolle der Social Media als eine „fünfte Gewalt" in dieser defekten Demokratie ist, soll anhand einiger Beispiele beleuchtet werden.

Ein wichtiges Ereignis für die heute bedeutende Rolle der sozialen Medien als Instrument der Bevölkerung zur (auch) politischen Vernetzung war die sogenannte Kerzenscheindemonstration, die erstmals am 17. April 2008 stattfand und sich gegen die neuen, weniger strengen Importregelungen von Fleisch aus den USA und hiervon ausgehend generell gegen das geplante Freihandelsabkommen mit den USA richtete. Zehntausende Koreaner protestierten mehrere Monate von April an landesweit, noch heute gibt es Demonstrationszüge, deren politische Botschaften sich inzwischen erweitert haben und die aktuell den Rücktritt der Präsidentin aufgrund des bereits erwähnten Korruptionsskandals fordern. Hinter den Protesten standen von Anfang an keine führenden Organisationen, sondern die Demonstrant.innen hatten sich über die sozialen Medien, v. a. das Netzwerk *Agora*, zusammengefunden, d. h. es hatte sich erstmals eine große Öffentlichkeit online formiert, die sich dann physisch, offline, in Kundgebungen zeigte.

Kerzenscheindemonstration 2008

Ähnlich bemerkenswert war die Rolle der sozialen Medien im Wahlskandal von 2012: Schon während des Wahlkampfes wurde bekannt, dass der südkoreanische Geheimdienst *NIS* und die Cybereinheit der südkoreanischen Armee illegal und verdeckt Wahlkampf für Parks Sieg betrieben. Rund 70 Agent.innen der Abteilung für psychologische Kriegsführung und rund 120 Soldaten der militärischen Cybereinheiten hatten Millionen Tweets und Kommentare verfasst, um den Gegenkandidaten zu diskreditieren. Brisant ist dies auch angesichts der Tatsache, dass der Wahlsieg von Park mit 51,5 % der Stimmen sehr knapp ausfiel. Kleine unabhängige Medien enthüllten den Skandal, der sich wiederum über die sozialen Netzwerke rasch verbreitete. Erst durch den so entstehenden öffentlichen Druck kam es zu einem Ermittlungsverfahren (welches jedoch auf Grund des angeordneten Rücktritts des Generalstaatsanwalts zum Erliegen kam).

Als wichtigste Zäsur des Wandels der südkoreanischen Gesellschaft gilt jedoch das Schiffsunglück der *Sewol* am 16. April 2014, bei dem 304 Menschen vor der südkoreanischen Küste ums Leben kamen, darunter 250 Schüler.innen. Am Unfalltag

Ok-Hee Jeong

Ok-Hee Jeong arbeitet als freie Journalistin in Berlin. Ihre Themenschwerpunkte sind Politik und Gesellschaft Südkoreas. Ihr erster Dokumentarfilm SEWOL wurde 2015 fertiggestellt und hatte Ende 2016 Premiere in Deutschland. Zurzeit arbeitet sie an ihrem zweiten Dokumentarfilm über Liebe im Alter bei gleichgeschlechtlichen Paaren.

berichteten die großen Medien zunächst geschlossen über die Rettung aller Passagiere; als schließlich die Zahlen der mit dem Schiff Gesunkenen bekannt wurde, war in den folgenden Tagen propagandahaft von einem großen Ausmaß an Rettungsaktionen die Rede, von zahlreichen Rettungskräften, die rund um die Uhr im Einsatz seien, von zahlreichen Helikoptern und Schiffen. Als die Eltern selbst an den Unfallort fuhren, stellte sich jedoch heraus, dass es keine Rettungsaktionen gab. Über die sozialen Medien kämpften die Eltern um Verbreitung der Wahrheit, gaben aus Protest ausschließlich ausländischen Reportern Interviews und über *Facebook* ließ sich weltweit die Situation auf der Insel Jindo verfolgen, wo die Angehörigen auf die Rettung der Verunglückten warteten, wie sie am 20. April mit einem Protestmarsch Richtung Seoul gegen die Untätigkeit der Regierung demonstrierten, durch die südkoreanische Polizei blockiert wurden und teilweise in Hungerstreik traten. Beeindruckend war, wie rasch sich eine solidarische Öffentlichkeit über die sozialen Medien bildete, was u. a. Solidarkundgebungen und kritische Berichterstattungen im Ausland zur Folge hatte, die wiederum über die sozialen Netzwerke auch in Korea Verbreitung fanden. Deutlich zeigt sich an diesem Beispiel einerseits, wie sich die Social Media spätestens jetzt als Alternative zu den einflussreichen staatsnahen Medien etablierten und sich andererseits auf diesem Wege auch eine noch heute bestehende Solidargemeinschaft herausbilden konnte, wie sie sich bei anderen Themen etwa auch vermehrt in Online-Petitionen niederschlagen. In Reaktion auf die umfassende eigenmächtige Verbreitung der Informationen durch die Betroffenen und ihre Unterstützer begann jedoch auch die Regierung um die Präsidentin, die sozialen Medien zu ihren Zwecken zu nutzen, verbreitete gefälschte Fotos der Angehörigen oder Falschmeldungen, etwa um einen hungerstreikenden Vater gezielt zu diskreditieren. Die sozialen Medien werden so also gleichermaßen zu einem Machtinstrument des Volkes wie der Regierung. Erst vor wenigen Monaten ist ein expliziter Plan der Regierung bekannt geworden, wie die sozialen Medien für die öffentliche Meinungsbildung zu nutzen seien.

Social Media zwischen „fünfter Gewalt“ und staatlichem Machtinstrument

Diese Beispiele zeigen einerseits eindrücklich, wie das Internet immer mehr an Bedeutung gewinnt – für die Informationsbeschaffung und Kommunikation der südkoreanischen Bevölkerung ebenso wie als essenzielle Grundlage für eine alternative Medienlandschaft ist es nicht mehr wegzudenken, genauso wenig wie für das Verbreiten gezielter politischer Propaganda durch die Regierung. Damit einher geht andererseits aber auch eine Informationsflut – schnell ist im Netz eine Behauptung aufgestellt und genauso schnell ist sie verbreitet. Was diese Beispiele nämlich auch zeigen, ist, wie schnell über soziale Medien eine Welle losgetreten werden kann, die im schlimmsten Falle sogar in *Shit Storms* mündet. Ein Kommentar kann Leben zerstören, genauso wie er weltberühmt machen kann, wie etwa der südkoreanische Sänger Psy mit dem Lied *Gangnam Style* bewiesen hat. Wenn wir optimistisch glauben, das Internet würde eine neue Objektivität widerspiegeln, dürfen wir dabei jedoch nicht außer Acht lassen, dass seine Algorithmen sich gleichermaßen manipulieren lassen wie die Nachrichten selbst – inzwischen ist nicht nur in Südkorea eine eigene Branche entstanden, die diese Manipulationen als Dienstleistung anbietet. Besonders im Online-Marketing werden mit angeheuerten Internet-Trollen in Südkorea Grenzen in einem Ausmaß überschritten, von dem wir in Deutschland kaum eine Vorstellung haben. Umfassende Manipulation der sozialen Medien – etwa bei *YouTube* sich die Anzahl der Klicks erkaufen zu können – ist längst Realität. Südkoreanische Suchportale wie *Naver* oder *Daum.net* werden scharf kritisiert auf Grund der Manipulation ihrer Algorithmen, die gezielt beeinflussen können, welche Nachrichten in den Hitlisten landen und welche in der Fülle der Information untergehen, und die damit eine nie dagewesene Informationshoheit innehaben. Wie die letzten beiden der drei ausgeführten Beispiele zeigen, weiß sich längst auch die südkoreanische Politik der Macht des Internets und der Social Media zu bedienen.

Dass Südkorea jedoch hier kein Einzelfall ist, zeigen Beispiele aus China (Ghostwriter der *Internet Water Army*), Russland (Putins Internet-Trolle) ebenso wie aus Deutschland (der Manipulationsversuch der Öffentlichkeit durch die Deutsche Bahn vor ihrem Börsengang im Jahr 2009, in den über eine Million Euro investiert worden war). Das sogenannte *Astroturfing* – das künstliche Nachbilden von Graswurzelbewegungen mithilfe eingekaufter Kommentare, Likes und eigener Texte zur Beeinflussung der öffentlichen Meinung oder zu kommerziellen Zwecken – hat sich längst so weit verbreitet wie das Internet selbst. Je intensiver man sich mit dem Thema Social Media und ihrer gesellschaftlichen und politischen Rolle beschäftigt, desto mehr wird der anfängliche Mythos der Netzoptimisten entzaubert. Ob Social Media als „fünfte Gewalt“ Staatskorrektiv oder staatliches Machtinstrument ist, lässt sich freilich nicht pauschal beantworten – beides ist jederzeit möglich und liegt in den Händen aller, die Social Media nutzen und sie auch kritisch nutzen müssen. Erinnern sollten wir uns daher immer wieder neu an Evgeny Morozovs Feststellung, Informationstechnik sei weder als Technik der Freiheit noch als Technik der Tyrannei zu betrachten, sondern in erster Linie als Technik der Macht, die sich in bestehende oder entstehende Machttechniken einschaltet.

Der Fall Südkorea ist dennoch ein hoffnungsvoller, wie die beeindruckenden Kerzenscheindemonstrationen zeigen (*https://www.youtube.com/watch?v=cwlSuNm4ODE)*, denn einerseits sind zwar die alten Kräfte der Diktatur noch immer im Verborgenen und mit großer Macht aktiv, was ganz fundamental Südkoreas Demokratie untergräbt – insbesondere die junge Generation macht sich jedoch die Möglichkeiten der Vernetzung und Kommunikation über das Internet im ganz demokratischen Sinne zunutze, um sich umfassender zu informieren und gemeinsam für das Recht auf Meinungsfreiheit und Demokratie sowie gegen Korruption und Informationshoheit durch den Staat aufzustehen. Wenn der entstehende öffentliche Druck groß genug wird, um die an der Korruption um Präsidentin Park Beteiligten abzustrafen, wird eine echte Demokratie das defekte System Südkoreas ablösen können. Den aktuellen Umfragewerten zufolge liegt die Akzeptanz Parks unter den jungen Leuten derzeit bei 0 %, was noch einmal auf eine andere, eindrückliche Weise die Rolle der Social Media als Korrektiv in einer aufgeklärten und sich gegenseitig aufklärenden Gesellschaft besonders deutlich macht.

Fortsetzung des Schwerpunkts:

Zukunft der Arbeit – Arbeit der Zukunft: Wer steuert wen?

Nadine Müller

Das Ringen um Gute Arbeit in Zeiten *smarter* Technik

Die Gestaltung von Arbeit mit Software

Unter dem Schlagwort Digitalisierung *wird derzeit eine Reihe umfassender Veränderungen in der Arbeitswelt gefasst, die uns vor (teils) neue Herausforderungen für die Arbeitsgestaltung stellen. Diese als Digitalisierung oder auch als* Computerisierung *bezeichnete Entwicklung erfasst nahezu alle Arbeitsplätze, direkt oder indirekt. Der Prozess ist vor allem dadurch gekennzeichnet, dass die Arbeitsmittel* digital *ausgestattet sind: über 90 % der Arbeitsplätze in der Medien- und Kulturbranche, über 80 % in den Energieunternehmen und rund 70 % im Handel. Präziser wäre: nur noch wenige Arbeitsplätze – und in Zukunft wird dieser Anteil weiter abnehmen – kommen heute ohne Software aus, ob in Scannern, Robotern, Personal-Computern, Laptops oder Smartphones.*

Damit ergeben sich große Herausforderungen an die Arbeitsgestaltung: Einige Tätigkeiten werden hinfällig, andere entstehen neu; so auch Berufe und Qualifikationen. Arbeit in Betrieben und Verwaltungen wird umorganisiert, Out- und Crowdsourcing sowie globale Arbeitskooperationen stehen auf der Tagesordnung. Dies stellt auch unsere Gewerkschaft vor große Anforderungen. So hat sich ver.di auf dem 4. Bundeskongress die soziale, demokratische und humane Gestaltung des digitalen Umbruchs *zum Ziel gesetzt. Nur so werden aus den Risiken der Digitalisierung Chancen. Dazu bedarf es politischer, demokratisch legitimierter* Initiativen und Interventionen.

Beschäftigungs- und Zukunftsperspektiven

Eine Studie der Bank *ING-DiBa* kommt zum Ergebnis, dass der Anteil der gefährdeten Arbeitsplätze in Deutschland höher ist als in den USA: Die Berechnung der Volkswirte basiert auf der Untersuchung von Carl Frey und Michael Osborne aus dem Jahr 2013:

> *„Während die Originalstudie davon ausgeht, dass in den USA 47 Prozent aller Stellen gefährdet sind, schießt der Wert in der Untersuchung für Deutschland auf 59 Prozent. Die Autoren glauben, dass das größere Gewicht der Industrie in Deutschland für den Unterschied verantwortlich ist."*[1]

Die Potenziale von zukunftsorientierten Wirtschaftszweigen wie Gesundheit, Software oder IKT sind dagegen laut dem Leiter des Deutschen Instituts für Wirtschaftsforschung (DIW) Marcel Fratzscher noch nicht wirklich ausgeschöpft:

> *„Wir müssen die jungen Branchen, die jungen Unternehmen fördern. Und wir sollten viel ambitionierter sein, was Forschung und Entwicklung angeht."*[2]

Es gibt inzwischen diverse Studien mit verschiedenen Prognosen, die sich auf unterschiedliche Annahmen, Zeithorizonte etc. beziehen. Unbestritten ist jedoch das Rationalisierungspotenzial in den Branchen. Eine kürzlich veröffentlichte Untersuchung kommt zu dem Ergebnis, dass 300 000 neue Arbeitsplätze in den Branchen Gesundheit und Pharma bis 2030 benötigt werden, während bis dahin 940 000 Verkaufskräfte nicht mehr nachgefragt werden. In Teilen bedeutet dies eine Fortschreibung des Trends: Auch aufgrund des demografischen Wandels sind 1,3 Millionen Arbeitsplätze von 2001 bis 2014 im Gesundheits- und Sozialbereich entstanden, während 300 000 Stellen in der Industrie abgebaut wurden – so eine Studie des Instituts für deutsche Wirtschaft (Stiens 2015)[3]. Bezüglich des zukünftig benötigten Arbeitsvolumens nach Berufshauptfeldern weist das Institut für Arbeitsmarkt- und Berufsforschung (IAB) in einer Prognose darauf hin, dass auch im Jahr 2030 die meisten Arbeitsstunden in Büro- und kaufmännischen Dienstleistungsberufen (7,9 Mrd. Stunden) aufgewendet werden, aber dann nicht mehr gefolgt von den be- und verarbeitenden und instandsetzenden Berufen (7,5 Mrd. Stunden), sondern von den Gesundheits- und Sozialberufen sowie Körperpflege (7,8 Mrd. Stunden; IAB 2012)[4].

Auf der Auftaktveranstaltung des Bundesarbeitsministeriums (BMAS) zum Dialog „Arbeiten 4.0" hat der damalige VW-Vorstand Horst Neumann prognostiziert, dass vor allem durch die Robotisierung bei VW mittelfristig taktgebundene Arbeit wegfällt, die etwa die Hälfte in der Produktion ausmacht, – und mehr Wissensarbeit sowie Arbeit am Menschen entstehen wird (BMAS, 20.4.2015)[5]. 70 % der Beschäftigung finden in Deutschland bereits im Dienstleistungssektor statt. Interaktive Arbeit beziehungsweise Arbeit an und mit Menschen nimmt

an Bedeutung zu. Diese Bedeutung spiegelt sich jedoch noch nicht im Investitions- und Innovationsgeschehen wider – wie Marcel Fratzscher vom DIW richtig feststellt – auch nicht in der Entlohnung. Allzu einseitig wird Industriepolitik betrieben und mit neuen Schlagwörtern wie *Industrie 4.0* auf 20 % der Wertschöpfung fokussiert.

Weil jedoch laut den Beschäftigten Gute Arbeit zuvörderst in beruflicher Zukunftssicherheit besteht, ist es vorrangiges Ziel von ver.di, eine möglichst positive Beschäftigungsentwicklung im Zuge des digitalen Umbruchs zu erreichen. Dazu eignet sich insbesondere, neue gute Arbeitsplätze in gesellschaftlich notwendigen und sozialen Dienstleistungsbereichen aufzubauen. Zu den gesellschaftlich notwendigen Dienstleistungen – also Diensten, die das Funktionieren der Gesellschaft garantieren – gehören neben Gesundheit auch Bildung und Mobilität etc. Dazu ist die gezielte Erforschung, Identifikation und Unterstützung von sozialen Innovationen nötig, die geeignet sind, nachhaltige Beschäftigung zu schaffen. Soziale Innovationen meint, dass – durchaus im Sinne von *Open Innovation* – Bürger.innen, Patient.innen, Kund.innen wie auch die Erwerbstätigen an der Erstellung neuer Dienste beteiligt werden. Dahinter steht also ein partizipativer Innovationsprozess, denn Partizipation wie auch gute Arbeitsbedingungen fördern (Er-)Neuerungen (Müller 2012, Müller/Roth 2013/2016)[6].

Für die Beschäftigungsförderung ist es unerlässlich, in eine hochwertige, flächendeckende und allen Bürger.innen gleichermaßen zugängliche digitale Infrastruktur zu investieren. Es genügt jedoch nicht, die technischen Grundlagen bereitzustellen. Genauso wichtig ist die Investition in eine entsprechende Qualifizierung. Damit einhergehen müssen intensivere Anstrengungen zur Vermittlung digitaler Kompetenzen auf allen Ebenen des Bildungswesens, die Verbesserung der finanziellen, rechtlichen und zeitlichen Rahmenbedingungen für berufsbegleitende Weiterbildung und die Entwicklung neuer Berufsbilder für eine digital vernetzte Arbeitswelt. So spricht sich die Mehrheit der Deutschen für den Vorschlag aus, dass Kinder in der Schule Programmieren lernen sollten – wie aus einer von der Hamburger Körber-Stiftung veröffentlichten Forsa-Umfrage hervorgeht.[7] Fortschritt wird aber auch dabei nur herauskommen, wenn Kinder zugleich eine Ausbildung in sozialen, v. a. demokratischen Belangen erhalten. Dazu gehört das Wissen, was es mit der *informationellen Selbstbestimmung* und den Persönlichkeitsrechten auf sich hat. Technische Kompetenzen und Fähigkeiten allein garantieren noch keine Innovationsfähigkeit. Das bestätigt unsere regelmäßige Befragung von ver.di-Aufsichts-, Betriebs- und Personalräten. Sie sehen mehr Weiterbildungsbedarf in sozialen Kompetenzen[8]. Wie Technisches und Soziales in der Informatik im Bereich der Hochschulausbildung verknüpft werden können, zeigt das „Mikropolis-Modell“[9].

Aber es geht eben nicht nur um das Wie, sondern um die erforderlichen Ressourcen für das im Prozess der Computerisierung erforderliche permanente Lernen (Müller 2010, 150)[10]. Dafür, und um die Effekte der Rationalisierung abzumildern, eignet sich eine Reduktion der Arbeitszeit – Zeit, die auch für Weiterbildung aufgewendet werden kann. Eine öffentlich geförderte Weiterbildungsteilzeit sollte das unterstützen (ver.di 2015a, Schröder 2016/2017)[11].

Crowdwork

Mit der Computerisierung und ihren technischen Möglichkeiten, insbesondere dem Internet, hat sich der Grad der Globalisierung von Arbeit erhöht (vgl. Müller 2010: Kap. 2.2). Diese Möglichkeiten hat eine Bewegung für die Erstellung von Software genutzt, die eine *freie* Kooperation bzw. einen möglichst freien Wissensaustausch sicherstellen will, um damit die Qualität ihres Codes zu verbessern (ebd., 74). Um die Vorteile freier Software zu nutzen, haben die Unternehmen diverse Strategien verfolgt. Eine besteht darin, mit der daran anschließenden Open-Source-Bewegung zu kooperieren und neue Lizenzmodelle zu schaffen, die eine Kommerzialisierung der Software erlauben – auch wenn darin nicht entlohnte Arbeit steckt (ebd.). Ein weiterer Versuch, sich die Vorteile einer erweiterten Kooperation anzueignen, die über die im *eigenen* Unternehmen hinausgeht, ist *Crowdwork* (vgl. Boes et al. 2014)[12]. Das ist jedoch nur eines von mehreren Zielen, die mit der Auftragsvergabe auf Plattformen wie *freelancer.com* verfolgt werden: die Einbindung nicht im Unternehmen angestellter Freelancer bzw. Solo-Selbständiger und damit auch des Know-how, über das sie verfügen. Ein weiteres Ziel besteht schlicht in der Reduktion von Kosten, auch durch das Unterlaufen von Arbeitsrechten. Denn den Freelancern muss kein Urlaubsgeld gezahlt werden, keine Lohnfortzahlung im Krankheitsfall und keine Weiterbildungskosten. Sie sind für ihren Arbeits- und Gesundheitsschutz selbst verantwortlich, für die Ergonomie ihres Arbeitsplatzes – das Arbeitsschutzgesetz greift hier nicht. Zudem müssen die Crowdworker.innen auch allein für ihre Sozialversicherungsbeiträge aufkommen.

Um in Erfahrung zu bringen, was die Crowdworker umtreibt, hat ver.di Studien in Auftrag gegeben. So wurden auf der Plattform *jovoto* sowie auf einer IT-Plattform 165 Crowdworker zu ihrer Lebenssituation, ihrer Motivation und ihren Erwartungen an Gewerkschaften im Herbst 2015 befragt. Die Befragten sind hoch qualifiziert, die Mehrheit hat einen Hochschulabschluss (Al-Ani/Stumpp 2015, 19)[13]. Der Zeitaufwand für Crowdwork variiert. Während die *Kreativ-Crowd* (jovoto) in der Mehrheit bis zu 10 Stunden im Monat für Arbeitsaufträge von Plattformen verwendet, sind es bei der *IT-Crowd* 11 bis 40 Stunden. Eine knappe Mehrheit (ca. 51 %) würden in eine Festanstellung mit tariflicher Bezahlung und ähnlichen Tätigkeiten wechseln, wenn sie die Möglichkeit dazu hätten (Leimeister et al. 2016)[14]. Von den Kreativen (jovoto) arbeiten die meisten freiberuflich, während über 40 % der IT-Crowd angestellt sind (Al-Ani/Stumpp 2015, 19). Weitere Studien bestätigen, dass auf Design-Plattformen über 50 % freiberuflich tätig sind. Sie weisen jedoch insgesamt darauf hin, dass die Mehrheit nur *nebenberuflich* Aufträge von Plattformen ausführen. So ist das Ergebnis der – nicht repräsentativen – Studie von Leimeister et al. (2016), dass für nur 22 % von den 248 befragten Crowdworkern Plattformaufträge Haupteinnahmequelle sind.

Während eine knappe Mehrheit der Crowdworker in dieser Studie eher keine Erwartungen an die Gewerkschaften haben (über 50 % der Kreativ-Crowd wünscht sich jedoch Beratung und fast 50 % eine Zertifizierung von Plattformen), so erachten nach einer Untersuchung der Universität Kassel über 50 % der Befragten eine gewerkschaftliche Interessenvertretung als sinnvoll (Leimeister et al. 2016). ver.di setzt sich für Gute Digitale Arbeit

in der Crowd ein und bietet seit April 2015 eine spezielle Beratung für Crowdworker an: *www.cloudworker-beratung.de*. Darüber hinaus betreibt ver.di Öffentlichkeitsarbeit und engagiert sich politisch wie beispielsweise im Dialogprozess „Arbeiten 4.0" des Bundesministeriums für Arbeit und Soziales. ver.di fordert ein Minimum an ganzheitlichen Arbeitsinhalten, adäquate Mitbestimmungsmöglichkeiten und eine soziale Regulierung der Arbeitsverhältnisse mit Mindestbedingungen sowie den Schutz der Persönlichkeitsrechte. Solo-Selbständige sind in die gesetzliche Sozialversicherung aufzunehmen sowie die Auftraggeber und Plattformbetreiber zu verpflichten, ebenfalls ihren Beitrag hierfür zu leisten. Diese Forderungen hat ver.di auch in die Debatte um den Code of Conduct einiger Plattformbetreiber – initiiert von *testbird* – im Juli 2015 eingebracht.

Humane und gesunde Arbeit

Um die Potenziale der Digitalisierung für gutes, humanes und gesundes Arbeiten zu nutzen, sollte entsprechend das Arbeits-, Sozial- und Datenschutzrecht modernisiert werden. Die Ansprüche abhängig Erwerbstätiger auf *Nicht-Erreichbarkeit* und *Nicht-Reaktion* sind zu verankern. Das ist ein Beitrag neben anderen, um Rechte auf Zeit- und Ortssouveränität der Beschäftigten zu gewährleisten. Weitere wichtige Schritte sind die Verankerung wirksamer Arbeits- und Sozialstandards mit Mindestbedingungen für Werkvertragsnehmer.innen, Solo-Selbständige und Crowdworker.innen hinsichtlich Vertragsinhalten und Honorarhöhe. Zudem ist es notwendig geworden, die sozialen Sicherungssysteme an die neuen Größenordnungen und Herausforderungen abhängiger Erwerbstätigkeit außerhalb klassischer Normalarbeitsverhältnisse – unter anderem durch die Einbeziehung von Solo-Selbständigen und Crowdworker.innen – anzupassen und eine Ko-Finanzierung durch deren Auftraggeber sicherzustellen. Dabei ist zudem darauf hinzuwirken, dass die auf Risikoausgleich ausgerichteten Solidarsysteme in Zeiten erhalten werden, in denen sich automatisiert persönliche Daten über individuelle Risikofaktoren einer Person auswerten lassen (Stichwort: *Scoring*). Digitalisierung soll helfen, eine solidarische Gesellschaft zu stärken.

Auf die Herausforderungen der Digitalisierung müssen auch im Arbeits- und Gesundheitsschutz kreative und innovative Antworten gefunden werden. Bislang vorwiegend an ortsfesten Tätigkeiten ausgerichtete Normen sind mit Blick auf ortsflexible Arbeit zu modernisieren. Zudem ist es längst an der Zeit, hochwertige ergonomische Hard- und Softwarestandards für mobile digitale Arbeitsmittel zu entwickeln und zu fördern. Gefördert werden sollten zudem Initiativen zur Humanisierung digitaler Arbeitsprozesse, die die Gewährleistung von möglichst sinnvollen und ganzheitlichen Arbeitsinhalten zum Ziel haben müssen. Unabdingbar ist außerdem die Intensivierung der öffentlichen Förderung von Modell- und Forschungsprojekten zur Klärung der spezifischen Belastungen und Beanspruchungen wie auch der positiven Potenziale und erforderlichen Ressourcen digital mobiler Arbeit, zu deren menschengerechter Gestaltung und eben zu Konzepten einer *Mobilisierung* des Arbeits- und Gesundheitsschutzes. Die Ergebnisse solcher Projekte müssen umgesetzt werden, sie dürfen nicht in der Schublade verschwinden wie bisher oft.

Gute Arbeit: Mehr Beteiligung und mehr Mitbestimmung

Ein zentraler Punkt, um im Zeitalter *smarter* Technik Demokratisierung voranzutreiben, ist die Verbesserung der Beteiligung der Erwerbstätigen und der Mitbestimmungsrechte von Betriebs- und Personalräten in verschiedenen Feldern wie im Arbeits- und Gesundheitsschutz, bei Auftragsvergaben, Out- und Crowdsourcing und bei Wertschöpfungsprozessen in vernetzten *virtuellen* Strukturen. ver.di setzt sich dafür ein, dass im Betriebsverfassungs- und im Personalvertretungsrecht das sofortige Hinzuziehen unabhängiger externer Sachverständiger in allen Fragen vor Einführung neuer Arbeitsverfahren, neuer Arbeitsmittel und Software als eindeutiger Rechtsanspruch festgeschrieben wird. Die Verabschiedung eines eigenständigen Beschäftigtendatenschutz-Gesetzes, das den spezifischen Bedingungen und Abhängigkeiten in Arbeitsverhältnissen Rechnung trägt, ist längst überfällig. Auch tritt ver.di für die Schaffung von Rechtssicherheit für die Kommunikation von Arbeitnehmer.innen in sozialen Netzwerken ein.

Um die Ziele zu erreichen, wird sich ver.di intensiv an den Diskussionen um die Weiterentwicklung und Umsetzung der Digitalen Agenden von Bundesregierung und Europäischer Kommission sowie an weiteren Debatten von Parteien und Parlamenten beteiligen. So hat ver.di jüngst Stellung zum Grünbuch „Arbeiten 4.0" des Bundesministeriums für Arbeit und Soziales genommen. Es sollen die zu erwartenden Konsequenzen des digitalen Umbruchs für die Beschäftigung und für Geschäfts-, Produktions- und Arbeitsmodelle in Branchenanalysen untersucht und prognostiziert werden. Kerngeschäft wird es sein, kollektive Vereinbarungen zur Durchsetzung Guter Arbeit abzuschließen sowie Mustervereinbarungen für die und mit den Kolleg.innen in Betrieben und Verwaltungen zu entwickeln. Aufbauend auf den langjährigen Erfahrungen der Selbständigenarbeit wird ver.di sich verstärkt auch den Anliegen von Crowdworker.innen zuwenden und für sie und mit ihnen gewerkschaftliche Unterstützungs- und Beteiligungsangebote entwickeln. Kurz, ver.di hat

Nadine Müller

Nadine Müller ist Referentin im Bereich Innovation und Gute Arbeit beim ver.di-Bundesvorstand in Berlin.

die Durchsetzung Guter Arbeit in den Zeiten des digitalen Umbruchs zu einem Schwerpunkt ihrer Aktivitäten gemacht. Davon zeugt auch der 3. ver.di-Digitalisierungskongress (*http://www.verdi.de/themen/digitalisierungskongresse/kongress-2016*).

Weiterlesen

Mehr Informationen: *http://innovation-gute-arbeit.verdi.de/themen/digitale-arbeit*

Referenzen

1 *Kaiser, T.: Maschinen könnten 18 Millionen Arbeitnehmer verdrängen, in: Die Welt vom 2.5.2015, www.welt.de/wirtschaft/article140401411/Maschinen-koennten-18-Millionen-Arbeitnehmer-verdraengen.html; Brzeski/Burk, Die Roboter kommen, Economic Research, 2015*

2 *Sievers, M., Interview mit M. Fratzscher: „Ich glaube, dass Berlin goldene Jahrzehnte vor sich hat", in: Berliner Zeitung vom 18./19.4.2015, S. 10*

3 *Stiens, T. (2015): Mehr Jobs, weniger Gehalt, in: SZ vom 16.4.2015*

4 *IAB (2012): Qualifikations- und Berufsfeldprojektion bis 2030, Kurzbericht 18/2012, http://doku.iab.de/kurzber/2012/kb1812.pdf*

5 *BMAS (20.4.2015), Arbeiten 4.0, http://www.arbeitenviernull.de/aktuelles/videos/arbeiten-40-auftaktveranstaltung-diskussionspanel-1.html; siehe dazu auch: Industrie 4.0 und Arbeit 4.0 prallen aufeinander, in: CuA 5/2015, 3*

6 *Müller, N./Roth, I. (2013): Innovationsfähigkeit durch Partizipation – Ergebnisse des Innovationsbarometers 2011, in: Schröder/Urban: Jahrbuch Gute Arbeit, Frankfurt/M. und Müller, N./Roth, I. (2016): Digitalisierung und Innovation, in: Schröder/Urban: Jahrbuch Gute Arbeit, Frankfurt/M.*

7 *dpa, Umfrage: Mehrheit fordert Programmieren als Schulfach, in: Berliner Zeitung vom 22./23.10.2016, B11*

8 *ver.di-Bereich Innovation und Gute Arbeit (2015): ver.di-Innovationsbarometer 2015. Ausgewählte Ergebnisse, Berlin, http://innovation-gute-arbeit.verdi.de/innovation/innovationsbarometer*

9 *Christ, M./Krause, D./Rolf, A./Simon, E. (2006): Wissen, wie alles zusammenhängt. Das Mikropolis-Modell als Orientierungswerkzeug für die Gestaltung von Informationstechnik in Organisationen und Gesellschaft, in: Informatik-Spektrum, 29. Jg., Heft 4, S. 263–73*

10 *Müller, N. (2010): Reglementierte Kreativität, Arbeitsteilung und Eigentum im computerisierten Kapitalismus, Berlin*

11 *ver.di (2015a): Stellungnahme zum „Grünbuch Arbeiten 4.0" der Bundesregierung, http://innovation-gute-arbeit.verdi.de/themen/digitale-arbeit; Schröder, L. (2016): Die Digitalisierung der Arbeitswelt – ein Blick zurück nach vorn, in: Schröder/Urban: Jahrbuch Gute Arbeit, Frankfurt/M., 46–60; Schröder, L. (2017): Die digitale Treppe, Frankfurt/M.*

12 *Boes et al. (2014): Cloudworking und die Zukunft der Arbeit, hrsg. von der Beratungsstelle für Technologiefolgen und Qualifizierung (BTQ) im Bildungswerk der ver.di im Lande Hessen e. V./Input Consulting GmbH Stuttgart*

13 *Al-Ani, A./Stumpp, S./Schildhauer, T. (2015): Motivationen und Durchsetzung von Interessen auf kommerziellen Plattformen. Ergebnisse einer Umfrage unter IT- und Kreativ-Crowdworkern. HIIG Working Paper 5/2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2699065*

14 *Leimeister, J. M./Durward, D./Zogaj, S. (2016): Crowd Worker in Deutschland. Eine empirische Studie zum Arbeitsumfeld auf externen Crowdsourcing-Plattformen. Study Nr. 323, Hans-Böckler-Stiftung, Düsseldorf, http://www.boeckler.de/pdf/p_study_hbs_323.pdf*

Eva von Buch

Gesundheit in Zeiten von *Arbeit 4.0*

Mit der großflächigen Umsetzung von Industrie 4.0- *und* Digitalisierungs*vorhaben verändern sich die Anforderungen an die Gestaltung von Arbeit. Damit stellen sich auch neue Fragen hinsichtlich der Gesundheit von Beschäftigten. Es scheint immer wichtiger zu werden, dass Beschäftigte selbst mehr Verantwortung übernehmen für die eigene Gesundheit. Denn die Möglichkeiten zur Regulierung von Unternehmensseite sind rückläufig. Deren Verantwortung wird zukünftig darin liegen, in enger Abstimmung mit den Beschäftigten immer individuellere Lösungen zur Vereinbarung von Beruf und Privatleben und auch generell zur Bewältigung von Anforderungen im Beruf zu entwickeln. Die Prävention berufsbedingter Erkrankungen sollte dabei mehr Bedeutung erlangen. Politik und Gewerkschaften müssen sich neu positionieren.*

Was ist Gesundheit – und was *Arbeit 4.0*?

Aaron Antonovsky, der Wissenschaftler, der in den 70er-Jahren das Konzept der *Salutogenese* entwickelte, sprach von einem *Kontinuum*, auf dem sich unsere Gesundheit ein ganzes Leben lang hin und her bewegt. Dabei könne ein sehr kranker Mensch sich aufgrund unterschiedlicher Ressourcen trotzdem als verhältnismäßig gesund empfinden, ein objektiv kerngesunder Mensch hingegen sich aufgrund fehlender Ressourcen als sehr krank wahrnehmen. Es sei grundsätzlich möglich, dass Beschäftigte sich *gesund* oder *wohl* fühlen, trotz Einschränkung beispielsweise durch ein erhöhtes Stressaufkommen in Veränderungsprozessen.

Antonovsky warf in seiner Forschung die Frage auf: „Was hält den Menschen gesund?" Auf die heutige Arbeitswelt bezogen stellt sich die Frage, was Beschäftigte brauchen, um die Veränderungen, die in den Organisationen mit der Einführung von *Industrie 4.0*/Digitalisierung einhergehen, verstehen, annehmen und bewältigen zu können. Welche Ressourcen kann und muss eine Organisation generell zur Verfügung stellen, damit sich ihre Beschäftigten wohl fühlen? Müssten diese Ressourcen andere sein als noch vor zehn oder fünfzehn Jahren? Und schließlich: Wie viel Verantwortung kann und muss eine Organisation für die Gesundheit ihrer Beschäftigten überhaupt übernehmen?

Das Bundesministerium für Arbeit und Soziales definiert den Begriff der *Arbeit 4.0* wie folgt:

> *„Arbeiten 4.0 wird vernetzter, digitaler, flexibler sein. Wie genau die zukünftige Arbeitswelt aussehen wird, ist offen. Seit Beginn des 21. Jahrhundert stehen wir vor einem erneuten grundlegenden Wandel der Produktionsweise. Die wachsende Vernetzung und zunehmende Kooperation von Mensch und Maschine ändert nicht nur die Art, wie wir produzieren, sondern schafft auch ganz neue Produkte und Dienstleistungen. Durch den kulturellen und gesellschaftlichen Wandel entstehen neue Ansprüche an Arbeit, auch die Nachfrage nach Produkten und Dienstleistungen verändert sich. Welche Auswirkungen diese Entwicklungen auf die Organisation von Arbeit und sozialer Sicherung haben, ist offen. Wir stehen am Beginn neuer Aushandlungsprozesse zwischen Individuen, Sozialpartnern und dem Staat.*
>
> *Es reicht zukünftig nicht, an den Rändern des Arbeitsmarktes auf unerwünschte Entwicklungen zu reagieren, auch wenn dies weiter notwendig sein wird. Der Gestaltungsbedarf von Arbeiten 4.0 geht darüber hinaus.“*[1]

Veränderte Belastungen

Über die Annahme, dass die Belastung von Beschäftigten durch Auswirkungen von Digitalisierung und *Industrie 4.0* zugenommen hat, streiten sich die Gelehrten. Aus dem Arbeitgeberlager heißt es, es habe immer schon Phasen höheren Belastungsaufkommens gegeben und der sich seit Jahren abzeichnende Anstieg von Fällen und Dauer psychischer Erkrankungen sei nicht zwingend auf die Veränderungen im Berufsalltag zurückzuführen. Arbeitnehmernahe Organisationen wie beispielsweise der DGB hingegen propagieren sehr deutlich, dass die veränderten Arbeits- und Vereinbarungsanforderungen der letzten Jahre ihren Tribut von den Beschäftigten fordern. Sie rufen anlässlich der aktuellen Veröffentlichung von Krankheitsdaten der DAK[2] nach einer wirksamen *Anti-Stress-Politik*[3].

Eine im September 2016 veröffentlichte Studie von BARMER GEK und Universität St. Gallen bestätigt einen signifikanten Einfluss, den die Nutzung moderner Informations- und Kommunikationstechnologie (IuK) auf die Gesundheit der Beschäftigten hat. Danach seien „signifikante Zusammenhänge mit emotionaler Erschöpfung (Burnout) und Konflikten zwischen Arbeit und Familie zu verzeichnen. 23 % der Befragten fühlten sich durch ihre Arbeit emotional erschöpft.“[4] Diesem Ergebnis geht die These voraus, dass durch die Digitalisierung in vielen Branchen der Druck entsteht, schneller zu arbeiten und sich ständig fortzubilden. Überdurchschnittlich betroffen seien Führungskräfte, jüngere Berufstätige, Männer – und natürlich IT- und naturwissenschaftliche Berufe.[5] Eine weitere These ist aber auch, dass die Digitalisierung *kaum* den Krankenstand erhöhe; zwischen der Anzahl der Krankentage und dem Grad der Digitalisierung von Unternehmen bestehe lediglich ein geringer Zusammenhang.

Die *Große Freiheit:* Flexibilisierung

Schon Albert Camus hat gesagt: „Es gibt keine Freiheit ohne gegenseitiges Verständnis.“ So ist es! Die zunehmenden Freiheiten, die Beschäftigte heute zur Ausgestaltung ihrer Arbeit haben, müssen auch vereinbar sein mit ihrem Belastungsprofil. Ein Zugewinn an Freiheit für Beschäftigte ist häufig mit einem Mehr an Arbeit verbunden. Nur selten wird dabei überprüft, ob die Arbeitsmenge tatsächlich auch zu dem Freiraum passt, der gewährt wurde. Weil Mitarbeitende sich durch den Vertrauensbeweis ihres Arbeitsgebers *gebauchpinselt* fühlen, mögen sie dann oft nicht reklamieren, dass die Arbeitsmenge doch zu hoch sei – und erledigen die Arbeit in den späten Abendstunden oder am Wochenende, vielleicht sogar im Urlaub. Es sollte also einen offenen Dialog zwischen Beschäftigten und ihren Vorgesetzten geben, um die Interessen beider Parteien ins Gleichgewicht zu bekommen. Dazu braucht es eine gesundheitsbewusste Unternehmensphilosophie, verantwortungsbewusste Führungskräfte und reflektierte Beschäftigte.

Umstrukturierung

In den vergangenen Jahren haben sich die Veränderungszyklen in den Organisationen um ein Vielfaches beschleunigt. Nicht selten können Beschäftigte mit der Geschwindigkeit und Häufigkeit der Veränderungen nicht mehr mithalten, weil klare Informationen und gute Beteiligungsstrukturen fehlen. Die daraus resultierende latente Überforderung schlägt sich auf die Gesundheit der Beschäftigten nieder. Das trifft nicht nur IT- und Produktionsbetriebe, sondern inzwischen auch die öffentlichen Verwaltungen.

Die Veränderungs- und Umstrukturierungsmaßnahmen müssen in vielen Organisationen von einer alternden Belegschaft bewältigt werden – der *demografische Wandel* ist in vollem Gange, ohne hörbar thematisiert zu werden.

Eva von Buch

Eva von Buch ist Beraterin bei der Technologieberatungsstelle beim DGB NRW in der Regionalstelle Bielefeld. Sie berät und schult Betriebs- und Personalräte zu Themen des Betrieblichen Gesundheitsmanagements wie beispielsweise der Gefährdungsbeurteilung psychischer Belastungen und des Betrieblichen Eingliederungsmanagements. Auch Gesunde Führung und Demografischer Wandel stehen auf ihrer Agenda. Eva von Buch ist außerdem als zertifizierter Coach und als MBSR-Lehrerin tätig.

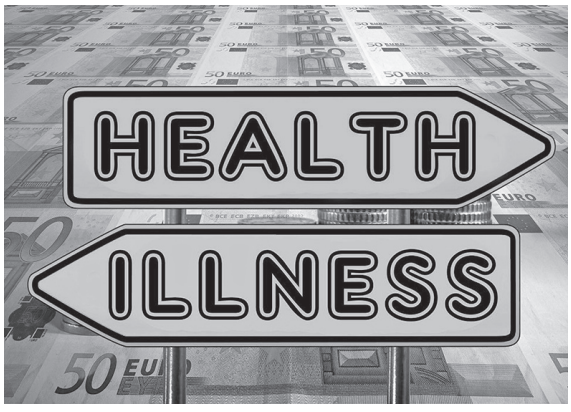
Veränderte Formen von Arbeit

Getragen werden die Veränderungs- und Umstrukturierungsprozesse unter anderem durch die Einführung neuer Formen von Projektarbeit. Das *agile* Projektmanagement beispielsweise umfasst unterschiedliche Methoden, die vor allem auf Flexibilität und Anpassung setzen. Statt ausführlicher und umfangreicher Planung zu Beginn eines Projekts werden das adaptive Planen sowie die schnelle Abstimmung im Team unterstützt. Agiles Projektmanagement hat insbesondere bei der Software-Entwicklung an Bedeutung gewonnen. Die Verantwortung jedes einzelnen Teammitglieds ist dabei hoch, entsprechend auch der Druck. Bei einer Belastungs- und Ressourcenanalyse des Instituts für Arbeit und Qualifikation (IAQ) der Universität Duisburg-Essen wiesen 20–40 % der befragten IT-Spezialisten Anzeichen von psychischer Erschöpfung auf. Als zentrale Bedingungsfaktoren wurden neben Zeitdruck, Arbeitsunterbrechungen und ungeplantem Zusatzaufwand auch widersprüchliche Arbeitsanforderungen, sozio-emotionale Belastungen und Synchronisations-Erschwernisse zwischen Erwerbsarbeits- und Familienrolle genannt.[6]

Die große Freiheit birgt Widersprüche. Häufig ist beispielsweise das Gehalt der Beschäftigten an Zielvereinbarungen gekoppelt. Im Zielvereinbarungsgespräch müssten Beschäftigte, deren Belastungsgrenze erreicht ist, die Übernahme weiterer Aufgaben oder Projekte ablehnen und damit auch auf die Gehaltserhöhung verzichten. Das fällt schwer, zumal, wenn nur ein Einkommen für den Unterhalt einer Familie sorgt oder wenn eine größere Anschaffung getätigt wurde. Auch ist die Angst oft groß, von den Vorgesetzen und im Unternehmen als *Minderleister* wahrgenommen zu werden. Womit wir wieder bei der Unternehmenskultur wären – und auch bei der individuellen, lebensphasenbezogenen Aushandlung von Anforderungen zwischen Arbeitgeber.in und Arbeitnehmer.in.

Zu den veränderten Arbeitsformen gehört auch die Zunahme des Phänomens Crowdworking. Frank Werneke, stellvertretender Vorsitzender der Vereinten Dienstleistungsgewerkschaft (ver.di) beklagt:

> *„Das Internet der Dinge tritt an die Stelle der bisher der Denkleistung von Menschen vorbehaltenen Teile der Arbeitswelt. Die Digitalisierung bedeutet einen revolutionären Umbruch – zurück zu einer Individualisierung und Vereinzelung der Arbeitnehmerschaft. Die Arbeiter von heute, das sind immer mehr Soloselbständige, Click- und Crowdworker, oft ohne jede Rechte."* [7]



Damit ist das Meiste schon gesagt. Click- und Crowdworker.innen profitieren von einer vermeintlichen Freiheit und nehmen dafür häufig in Kauf, dass sie zu einem Minimallohn arbeiten – in extremen Fällen sogar unbezahlt in Konkurrenz zu weltweit agierenden Spezialisten. Auch das hat viel mit Gesundheit zu tun. Vereinzelung, fehlende soziale Absicherung, um nur einige Folgen zu nennen, können dazu führen, dass die Beschäftigten krankheitsanfälliger werden – körperlich wie psychisch.

Interessierte Selbstgefährdung

In diesem Zusammenhang ist auch der Begriff der *Interessierten Selbstgefährdung* zu erwähnen – ausgelöst unter anderem durch Formen indirekter Steuerung wie die zuvor beschriebenen agilen Methoden. Ihr Einsatz führt dazu, dass eine größtmögliche Verantwortung bei einzelnen Mitarbeitenden verbleibt. Ein weiteres Beispiel für indirekte Steuerung ist das Zielvereinbarungsgespräch. Da die Beschäftigten ihre Zielvereinbarung selbst mit aushandeln, übernehmen sie auch die Verantwortung für die Zielerreichung. Und die setzt die Maßstäbe für das weitere Handeln. Vorgesetzte müssen überhaupt keinen Druck mehr auf Mitarbeiter ausüben, das übernehmen die ganz selbstverständlich selbst. Pausen, Urlaubszeiten, Erholungszeiten: Fast schon antiquiert klingen diese Begriffe in den Ohren mancher Projektmitarbeiter.

Dabei ist es grundsätzlich kein Problem, Erholungszeiten für eine begrenzte Zeit zu reduzieren – wenn danach eine Erholungsphase folgt im Sinne von weniger Zeitdruck, Arbeitsdichte, Geschäftsreisen etc. Gerade jüngere Beschäftigte und Führungskräfte sind auf diesem Auge aber blind, sie halten sich für unbegrenzt leistungsfähig und überschätzen häufig ihre Fähigkeiten. Mit der Folge, dass sie irgendwann ausgebrannt sind.

Anforderungen an Staat und Sozialpartner

Mit dem Arbeitsschutzgesetz, das seit 1996 unter anderem eine Gefährdungsbeurteilung von Arbeitsplätzen vorsieht (seit 2015 auch die Gefährdungsbeurteilung psychischer Belastungen!), wurde grundsätzlich gut für die Beschäftigten gesorgt. Es spricht dem Arbeitgeber eine Fürsorgepflicht zu, den Beschäftigten klare Rechte, die ihre Gesundheit im Betrieb schützen sollen. Und damit sind wir auch beim Haken: Das Gesetz bezieht sich auf einen klar umrissenen Rahmen, innerhalb dessen Arbeit stattfindet. Was ist mit *mobiler Arbeit*, *Homeoffice* und anderen Formen der (räumlichen und/oder inhaltlichen) Entgrenzung von Arbeit? Wie wird die Gefährdung einer permanenten Erreichbarkeit durch moderne Informations- und Kommunikationstechnologien (IuK) erhoben? Und wie soll sie eingedämmt werden?

Andrea Nahles, Bundesarbeitsministerin, hat mit ihrem *Grünbuch 4.0* einen ersten Aufschlag gemacht und darin wichtige Fragen gestellt, die Anforderungen an Arbeitsbedingungen der Zukunft betreffen – und damit auch den Aspekt der *Gesunden Arbeit 4.0*.[8] Ein *Weißbuch*, zu dem inzwischen ein erster Diskussionsentwurf vorliegt, soll Antworten auf die entsprechenden Fragen liefern.[9]

Arbeitgeberverbände und Gewerkschaften sind in der natürlichen Verantwortung, sich mit allen Aspekten von *Arbeit 4.0* auseinanderzusetzen – also auch mit dem der Gesundheit von Beschäftigten. Das betrifft besonders den Umgang mit neuen Formen der Belastung und Beanspruchung – sowohl an den Mensch-Maschine-Schnittstellen, also beispielsweise in der Produktion, wo menschliche Arbeitsleistung durch einen Roboter ersetzt wird, als auch im Bereich der Psyche (Druck, Überforderung, Arbeitsverdichtung, entgrenzte Arbeitszeiten, Probleme im Team oder mit Vorgesetzten etc.). Institutionen wie die *Nationale Arbeitsschutzkonferenz (NAK),* deren Arbeitsaufgaben im Arbeitsschutzgesetz festgelegt sind, müssen sich zukünftig ebenfalls intensiv mit dieser Thematik auseinandersetzen.

Anforderungen an die Arbeitgeber

Zwar gab es in der Vergangenheit erste Vorstöße von Unternehmen wie beispielsweise VW, die Nutzung moderner Informations- und Kommunikationstechnologien (hier: den Mailverkehr) der Beschäftigten per Betriebsvereinbarung zu regulieren. Es bleibt aber offen, wie erfolgreich derartige Regulierungsversuche sein können, wenn die Beschäftigten bereit und in der Lage sind, diese selbst zu unterlaufen. Auch hier stoßen wir wieder auf das Thema der Unternehmensphilosophie. Wenn es eigentlich gewollt ist, dass Beschäftigte bis zur Erschöpfung arbeiten und ihnen dies auch von ihren Vorgesetzten vorgelebt wird, ändert sich so schnell nichts in den Organisationen. Ein konsequent umgesetztes Betriebliches Gesundheitsmanagement kann diese Themen aufgreifen und in Abstimmung mit den Beschäftigten für gesunde Rahmenbedingungen sorgen. Das muss von der Geschäftsleitung allerdings gewollt und getragen werden.

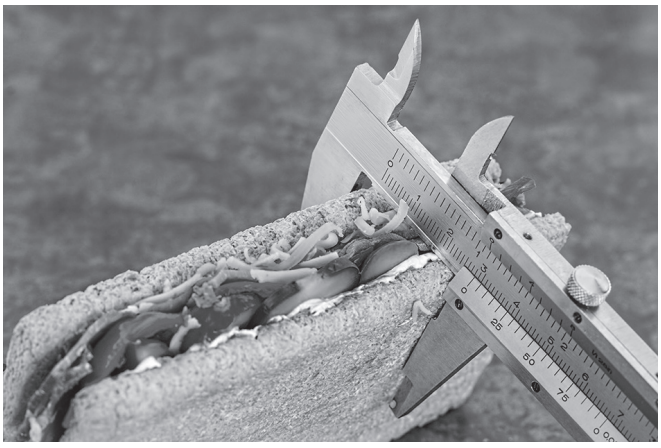
In vielen Unternehmen, besonders den größeren im Lande, werden schon längst neue Lösungen entwickelt, die Arbeit für gut qualifizierte Beschäftigte attraktiv gestalten sollen, um diese zu gewinnen oder im Unternehmen zu halten. Nicht selten fragen heute Bewerber im Vorstellungsgespräch nach dem Vorhandensein eines Betrieblichen Gesundheitsmanagements, Angeboten zur Gesundheitsförderung oder zur Vereinbarkeit von Beruf und Privatleben.

Noch nicht erwähnt sind dabei die zahlreichen ungelernten und geringqualifizierten Beschäftigten, deren Gesundheit durch Arbeitsformen wie Leih- und Werkvertragsarbeit erheblich beeinflusst ist. Wie eine sinnvolle und effektive *Arbeit 4.0* für sie aussehen kann, ist völlig offen. Dies trifft auch die erwähnten Click- und Crowdworker.innen.

Anforderungen an die Beschäftigten

Vor der vielleicht größten Herausforderung stehen die Beschäftigten selbst, wenn es darum geht, sich um die eigene Gesundheit zu kümmern. Denn der Spagat zwischen Leistungswillen und einem *achtsamen* Umgang mit der eigenen Gesundheit fällt oft schwer. Das Ringen um eine persönliche Lebensbalance beschäftigt viele Arbeitnehmer. Es müssen Entscheidungen für oder gegen bestimmte Lebens- und Arbeitsmodelle getroffen werden. Das setzt eine hohe Fähigkeit zur Selbstreflexion voraus. Eine gute soziale Vernetzung kann sehr hilfreich sein, wenn es darum geht, sich mit diesen Fragen auseinanderzusetzen. Für alle Beschäftigten dürfte es immer wichtiger werden, regelmäßig und in einer angemessenen Form für einen Ausgleich der Belastungen für Körper und Geist zu sorgen.

Unter den Beschäftigten sind sehr unterschiedliche Umgangsweisen mit diesen Anforderungen wahrzunehmen. Auf der einen Seite gibt es einen Hang zur geistigen wie körperlichen Selbstoptimierung, die gerne durch technische *Gadgets* unterstützt wird. Auf der anderen Seite nimmt beispielsweise die Zahl der stark übergewichtigen Arbeitnehmer zu, die den hohen Wert von Bewegung und gesunder Ernährung (noch) nicht erkannt zu haben scheinen – oder die vorhandene Informationen und Angebote für sich nicht nutzen können.



Die Anforderung, individuelle körperliche oder psychische Belastungspotenziale im beruflichen wie auch im privaten Umfeld frühzeitig zu identifizieren und angemessen darauf zu reagieren, ist komplex. Denn mit den Verlockungen einer flexiblen und selbstbestimmten Arbeitsgestaltung sind eben auch Entgrenzungsrisiken verbunden, die sich gesundheitsschädigend auswirken können, wie ständige Erreichbarkeit; Vereinbarung unrealistischer Zielvorgaben etc. Die Verantwortung besteht für viele Beschäftigte darin, an den entscheidenden Stellen auch einmal ein klares *Nein* zu äußern. Dieses Nein ist gleichzeitig ein *Ja* zu sich selbst und zur eigenen Gesundheit.

Fazit

Wenn wir also über Gesundheit in Zeiten von *Arbeit 4.0* sprechen, so stellt sich immer wieder die Ressourcenfrage. Was brauchen Beschäftigte, um neue Herausforderungen motiviert und zuversichtlich und im Rahmen ihres individuellen Leistungsvermögens angehen zu können? Innerhalb einer Organisation könnte man sie einfach danach fragen. In Interviews, Workshops, im Einzelgespräch. Das setzt voraus, dass Arbeitgeber Interesse haben am Gesundheitszustand und -empfinden ihrer Mitarbeitenden. Und an praktischen Lösungsansätzen für Probleme, die im Arbeitsalltag belasten. Ob das eine schwierige Teamsituation ist oder häufige Unterbrechungen im Produktionsablauf oder die Unvereinbarkeit der Arbeitszeiten mit der derzeitigen familiären Situation. … Die Beschäftigten sind die Expert.innen für ihre Arbeit, sie wissen häufig, welche Ressourcen sie bräuchten. … Schon allein, sie danach zu fragen, ist eine wichtige Ressource. Konkrete Ansätze könnten dann beispiels-

weise sowohl passgenaue Arbeitszeitmodelle sein als auch Fort- und Weiterbildungsmöglichkeiten.

Dabei kann die Nutzung der gesetzlich vorgeschriebenen Präventionsinstrumente *Gefährdungsbeurteilung*, auch psychischer Belastungen, und *Betriebliches Eingliederungsmanagement* durchaus hilfreich sein. Hier können Arbeitsplätze auf ihr Gefährdungspotenzial für die Beschäftigten hin überprüft werden. Und es können Team- oder Einzellösungen gefunden werden zur Auflösung von Belastungssituationen – gemeinsam mit den Beschäftigten.

In Zukunft wird es mehr innovative und nachhaltige Lösungen für gesunde *entgrenzte* Arbeitsplätze und Arbeitsbedingungen geben müssen. Diese Herausforderung gilt für alle Ebenen – Staat, Betrieb und Individuum. Die Form der Interventionen für gesunde Arbeitsbedingungen wird sich dabei vielleicht gar nicht so sehr verändern – eher die Frage der Zuständigkeit. Gelingt hier die Einbeziehung der Antonovskyschen Theorie von den Ressourcen, ist den Beschäftigten schon viel geholfen!

Referenzen

1 *http://www.bmas.de/DE/Schwerpunkte/Arbeiten-vier-null/arbeiten-vier-null.html*
2 *https://www.dak.de/dak/download/Gesundheitsreport_2016_-_Warum_Frauen_und_Maenner_anders_krank_sind-1782660.pdf*
3 *http://www.dgb.de/themen/++co++bb6fa620-595e-11e6-92da-525400e5a74a*
4 *https://www.barmer-gek.de/blob/34728/f3576976c7e2d74c84699fffcdb1f615/data/vortrag.pdf*
5 *https://www.barmer-gek.de/blob/34726/53b4d9e3b154a41468aa7de6e0edae4a/data/handout.pdf*
6 *http://link.springer.com/chapter/10.1007/978-3-658-01445-2_8*
7 *http://www.zeit.de/karriere/2016-10/gewerkschaften-digitalisierung-zukunft-arbeitnehmer-selbstaendige-crowdworking-tarifvertraege*
8 *http://www.bmas.de/DE/Service/Medien/Publikationen/A872-gruenbuch-arbeiten-vier-null.html*
9 *http://www.bmas.de/SharedDocs/Downloads/DE/PDF-Publikationen/a883-weissbuch.pdf?__blob=publicationFile&v=4*

Michael Ahlmann

Besprechung der Stellungnahme von *DIE LINKE* im Bundestag

zum Grünbuch *Arbeiten 4.0* des Bundesministeriums für Arbeit und Soziales vom 8. Juni 2016

Die Bundesregierung hat gemeinsam mit den Arbeitgeberverbänden eine Diskussion zum Thema Industrie 4.0 *angestoßen – ohne dass es meiner Meinung nach eine vierte industrielle Revolution gäbe. Darauf hat das Bundesministerium für Arbeit und Soziales (BMAS) ein* Grünbuch – Arbeit 4.0[1] *herausgegeben. Die Abgeordneten der* Linke.*n kritisieren in ihrer Stellungnahme*[2] *diesen Text. Mit dem Grünbuch will das BMAS eine gesellschaftliche Debatte zu den Auswirkungen der aus „4.0" resultierenden Veränderungen auf die Institutionen des Sozialstaates anstoßen. Ende des Jahres 2016 ist aufbauend auf dem Grünbuch ein* Entwurf zum Weißbuch Arbeiten 4.0 des BMAS *mit Handlungswegen und Lösungen erschienen*[3]*. Aus der Stellungnahme zum Grünbuch will ich insbesondere die sozialen Aspekte aufgreifen und auf einzelne Ansätze aus dem Entwurf zum Weißbuch verweisen. In der* FIfF-Kommunikation *4/2016 haben sich die Autor.innen mit wesentlichen Aspekten zum Thema* Zukunft der Arbeit – Arbeit der Zukunft: Wer steuert wen? *auseinandergesetzt. Im Folgenden entsprechen fettgedruckte und zentrierte Überschriften den jeweiligen Überschriften in der Stellungnahme* **DIE LINKE** *Meine Position zur Stellungnahme ist am Ende jedes Abschnitts kursiv gesetzt.*

Einleitung

Schwerpunkte des Regierungsansatzes *Industrie 4.0* sind Entwicklungen in der Fertigungstechnik und der Logistik, es geht aber auch um die Softwareentwicklung (*Smart Factory*, *Internet der Dinge* oder *Cyber-Physical Systems*). Es geht nach der Auffassung der *Linke.*n nicht um einen grundlegenden technologischen Wandel, sondern mehr um Spekulationen und Phantasien für die Zukunft. Entsprechende Untersuchungen über die Auswirkungen auf Arbeitsplätze differieren extrem – die Universität Oxford unterstellt 2013, dass 50 % der Arbeitsplätze in den USA durch Computer ersetzt werden, während das IAB 2015 nur 0,4 % der Arbeitsplätze in Europa betroffen sieht. Die Regierung will laut Grünbuch die Wettbewerbsfähigkeit der Industrie sichern, und so beachtet dabei nach Auffassung der *Linke.*n das Grünbuch weder den Einfluss des Kaufkraftzuwachses der Bevölkerung noch den des Wachstums des Binnenmarktes, also z. B. durch erfolgreiche Tarifrunden. Bei steigender Produktivität müssen nach Auffassung der *Linke.*n Umverteilungen, Verkürzungen oder eine Neuverteilung der Arbeitszeit erwogen werden.

Diese Forderung der Linke.*n teile ich und sehe hier dringenden Handlungsbedarf für Beschäftigte, Gewerkschaften, Politik und Öffentlichkeit. Laut IG Metall und dem Institut für Arbeitsmarkt- und Berufsforschung (IAB) sind im Jahr 2015 ca. 1,4 Milliarden Überstunden in Deutschland angefallen, 997 Millionen Überstunden davon ohne Bezahlung.*[4] *Dies ist ein Betrug der Arbeitgeber am Sozialstaat. Für mich folgt aus den unbezahlten Überstunden die Forderung: Freizeitausgleich oder Vergütung und Schaffen neuer Arbeitsplätze, um so Maßnahmen der Beschäftigungssicherung zu finanzieren.*

Digitalisierung in aller Munde, aber kaum Lösungen

„Digitalisierung" ist nicht klar definiert, vielmehr gibt es eine bunte, verworrene und oft offene Diskussion über verschiedene Bereiche des Arbeitslebens – stellt **DIE LINKE** fest. Folgen von *Industrie 4.0* in Zusammenhang mit Crowdworking oder dem Problem der räumlich-zeitlichen Entgrenzung in Verwaltungs- und Dienstleistungsbereichen werden ohne Bezug auf die Verknüpfung erörtert. *Industrie 4.0* will eine „vierte industrielle Revolution" bezeichnen. Gekennzeichnet ist der aktuelle Veränderungsprozess in Deutschland aus Sicht der *Linke.*n vor allem durch einen Rückgang der Tarifbindung, die Ausbreitung des Niedriglohnsektors, den Anstieg sogenannter atypischer Beschäftigung und instabilerer Erwerbsverläufe sowie durch das vermehrte Ausweichen auf Werkverträge. Sie sind Folge einer Politik des Sozialabbaus, der Arbeitsmarktderegulierung und der teilweisen Verdrängung von Arbeitsvorgängen durch Automatisierung und Robotereinsatz. **DIE LINKE** fordert Vorschläge zur sozialen Absicherung von Scheinselbständigen und zur Anpassung des Arbeitsrechts an neue Beschäftigungsformen wie Crowd- und Cloudworking. Praktische Maßnahmen der Regierung zur Bekämpfung prekärer Beschäftigung fehlen bisher.[5]

Hier müssen aus meiner Sicht Informatik-, Arbeits- und Sozialwissenschaften gemeinsam mit DGB und Hans-Böckler-Stiftung aktiv werden, Begriffe und Strukturen sauber abgrenzen und gute Maßnahmen entwickeln. In der FIfF-Kommunikation 4/2016 hat z. B. Prof. Wolfgang Däubler in seinem Beitrag erste Beispiele gebracht.

Wandel von Arbeit in Produktion, Fertigung und Vertrieb

Die Qualifikationen der Beschäftigten sollen sich beispielsweise verändern zu Facharbeiter.innen mit Ingenieurswissen, die den Produktionsablauf überwachen und bei Bedarf eingreifen können – lebenslange Weiterbildung ist somit erforderlich, um mit technischen Innovationen Schritt zu halten.

DIE LINKE setzt sich für die Einhaltung elementarer sozialer Grundrechte in der Arbeit ein, dies umfasst insbesondere das Recht auf Arbeit, gerechte Arbeitsbedingungen, angemessenen Lohn, Koalitionsfreiheit (Organisieren in Gewerkschaften) sowie die Teilhabe am wissenschaftlichen Fortschritt. Dabei müssen auch auf dem Gebiet der Arbeit die völkerrechtlich verbrieften spezifischen Lebenslagen von Frauen als auch Menschen mit Behinderungen berücksichtigt werden. Gewerkschaften haben diesen Trend erkannt und verschiedene Initiativen zur Weiterbildung Berufstätiger initiiert.

- Durch höhere Steuern für Unternehmen und Vermögende finanzierte Bildungszeitmodelle müssen von einem massiven Ausbau eines für alle Menschen zugänglichen Bildungssystems begleitet werden.

- Arbeitgeber.innen müssen die betriebliche Weiterbildung aktiv verbessern und finanzieren. Dazu schlägt **DIE LINKE** einen Weiterbildungsfonds vor, in den alle Unternehmen einer Branche einzahlen.

Meine Meinung: Neue Formen der vernetzten Fertigung und Logistik dürfen nicht dazu führen, Arbeitnehmer.innen bei der Arbeit lückenlos (aus Dateneingaben oder über RFID-Chips) zu überwachen.

Ich erwarte gravierend neue Anstrengungen, in der Schule möglichst alle Schüler.innen theoretisch und praktisch auf das Berufsleben vorzubereiten, ein „lebenslanges Lernen" staatlich/betrieblich zu organisieren und dies während bezahlter Freistellung von der Arbeit. Weitergehende Maßnahmen sind für erwerbslose junge Menschen und rentennahe Jahrgänge zu treffen, um Perspektivlosigkeit, Ausgrenzung und Altersarmut zu vermeiden und eine faire Verteilung der vorhandenen Arbeit zu sichern.

Wandel von Arbeit in der Dienstleistungsgesellschaft

Abhängige Beschäftigung

DIE LINKE sieht Flexibilisierung und Entgrenzung durch weltweiten Zugriff auf Daten als typisch für moderne Arbeitsorganisation an. Durch Digitalisierung werden viele Arbeitsprozesse transparenter – und damit mögliche Leistungsunterschiede. Leistungsdruck und psychische Belastungen lassen sich neben anderen Faktoren auch auf die IT-Entwicklung zurückführen. Deshalb ist die Forderung der Arbeitgeber nach Deregulierung von Arbeitsrechten zurückzuweisen, so **DIE LINKE**

Ich teile dies und fordere eine vertiefte Diskussion/Umsetzung der ILO-Normen (ilo.org) in Europa und weltweit.

Selbständigkeit

Im Jahr 2014 gab es in der Bundesrepublik 4,2 Millionen Selbständige. Rund die Hälfte davon waren sogenannte „Solo-Selbständige" (ohne Angestellte). **DIE LINKE** verlangt für diese Menschen eine faire Altersversorgung und Krankenversicherung.

Ich folge dieser Auffassung und fordere klare juristische und arbeitsrechtliche Abgrenzungen zwischen echter Selbständigkeit und „Scheinselbständigkeit". Letztere ist abzuschaffen.

Brüchige Erwerbsbiografien

DIE LINKE konstatiert, dass immer weniger Menschen aus Lohnarbeit ein sicheres und auskömmliches Einkommen erzielen können (Rückgang des Normalarbeitsverhältnisses). Teilzeit, Leiharbeit, Befristungen, Werkverträge, die Ausweitung des Niedriglohnsektors und der Rückgang der Tarifbindung sind weitgehend Folgen der Agenda-2010-Politik – weniger der Digitalisierung. Dies hat erhebliche Auswirkungen auf Rente und Krankenversicherung. Der im Grünbuch formulierte Prüfauftrag *Ob mit einem Wandel der Erwerbsformen neue Sicherungsdefizite auftreten?* und der bloße Hinweis auf das *Stichwort ‚Erwerbstätigenversicherung'* sind zu wenig. **DIE LINKE** fordert eine gesellschaftliche Mobilisierung gegen Leiharbeit, Befristung und Werkverträge.

Hier müssen meines Erachtens klare Konzepte gefunden werden, die ein sinnstiftendes Arbeitsleben und ein auskömmliches Bürgereinkommen ermöglichen. Die Verlagerung von „einfacher" Arbeit in „billigere" EU-Staaten mit Hilfe von EU-Geldern sollte ersetzt werden durch Ausbildung und Qualifizierung vor allem jugendlicher Erwerbsloser, um diese in ihrem Land in anspruchsvollere Arbeit zu bringen. Mit dem Kauf wertiger Produkte aus dieser Arbeit können wir dazu beitragen, den deutschen Exportüberschuss innerhalb der EU zu reduzieren.

Neue Formen von Arbeit

Michael Ahlmann als Aktiver auf einer Kundgebung der IG Metall

„Plattform-Ökonomie"

Internet-Anbieter.innen dringen inzwischen in weite Bereiche des Dienstleistungsgewerbes ein und bieten häufig auf einer Vielzahl digitaler Plattformen dezentral Dienste oder Produkte an.[6] Digitale Plattformen können damit die bestehende Wettbewerbssituation verschärfen oder bestehende Anbieter- und Arbeitsstrukturen verdrängen. Auf diesen Plattformen gibt es kein klassisches Zulieferer- beziehungsweise Arbeitsverhältnis. Der Erwerbsstatus der Anbietenden wird nicht erfasst, das Arbeitsrecht kennt noch keine spezifische Anwendung.

DIE LINKE *beschreibt hier vor allem das Übel. Für mich ist eine Integration von Plattformen in eine arbeitsrechtliche Struktur und eine geregelte Bezahlung geleisteter Arbeit umgehend zu entwickeln. Bestehende „analoge" Infrastrukturen dürfen nicht schematisch durch „digitale" abgelöst werden, um fatale lokale Auswirkungen zu vermeiden.*

Crowdworking/Clickworking/Cloudworking

DIE LINKE fordert:

- Die neue Solo-Selbständigkeit und Crowdworking sind abzusichern. Diese oft prekären Formen digitalisierter Arbeit müssen evaluiert und reguliert werden. Selbständige Crowdworker.innen müssen sozial abgesichert werden; beispielsweise durch eine Mindest-Vergütung für Solo-Selbständige und Einbeziehung in eine allgemeine Bürgerversicherung für Gesundheit und Pflege.[7]

- Mit der Digitalisierung ist auch eine neue Qualität der Internationalisierung der Arbeitsbeziehungen verbunden – ohne dass es ein entsprechendes internationales Vertragsrecht gäbe. Daher sind neue Konzepte für ein internationales Wirtschafts-, Arbeits- und Tarifrecht mit Sanktionsmacht dringend notwendig. Digitalisierung darf kein rechtsfreier Raum werden, in dem rechtsverbindliche Verpflichtungen aus dem UN-Sozialpakt, der Europäischen Sozialcharta und dem Grundgesetz ausgehebelt werden.

Zu den Begriffen Crowd- und Cloudworking gibt es grundlegende Gedanken[8] von Wolfgang Däubler, die auch auf kollektive Interessenvertretungen und Konfliktlösungsansätze verweisen. Hieraus sind gesellschaftliche Konzepte zu entwickeln, damit geleistete Arbeit auch bezahlt wird und keine „soziale Wüste" entsteht. Ein Modell wie z. B. die Künstler-Sozialversicherung reicht mir nicht.

Soziale Absicherung

Das Bundesministerium für Arbeit und Soziales thematisiert in dem Kapitel *Soziale Marktwirtschaft reloaded* die positiven Auswirkungen von Sozialpolitik auf sozialen Zusammenhalt und Verteilung des Reichtums. Dabei ist die Lohnquote gegenüber 2006 gesunken, die Vermögensverteilung ist deutlich ungerechter und gewachsen ist der Niedriglohnsektor. Die Agenda 2010 und die Hartz-Reformen sind hier entscheidende Stichworte.

Kritik **DIE LINKE**: Die Politik der verschiedenen Bundesregierungen hat die nachlassende Tarifbindung befördert. Der einzige Aspekt bei der sozialen Sicherung, der vom Bundesministerium für Arbeit und Soziales mit der zunehmenden Digitalisierung in Verbindung gebracht wird, ist die erwartete Zunahme von (Solo-)Selbständigkeit. Das soziale Sicherungssystem wird nominell fast paritätisch finanziert. Selbständigen wurde der Zugang zu gesetzlichen Sicherungssystemen erst spät und lediglich selektiv ermöglicht.

Gemeinsam mit **DIE LINKE** *fordere ich: Die Einbeziehung der Selbständigen verlangt eine grundsätzliche Kurskorrektur der Sozial- und Rentenpolitik, einen Ausbau und die strukturelle Weiterentwicklung der Systeme der sozialen Sicherung für alle Bürger.innen.*

Rente

Um insbesondere die gesetzliche Rentenversicherung zukunftsfest zu machen, fordert **DIE LINKE** gemeinsam mit Gewerkschaften und Sozialverbänden die Wiederherstellung eines den Lebensstandard sichernden und auch vor Armut schützenden Rentenniveaus („Sicherungsniveau vor Steuern" in Höhe von 53 Prozent) sowie seiner – vorwiegend – paritätischen Finanzierung und Ergänzung aus Steuermitteln durch Bundeszuschüsse und Beiträge für Kindererziehungszeiten. Denkbar wäre es, für den oberen Bereich etwa die Beitragsbemessungsgrenze in eine Beitragsäquivalenzgrenze umzuwandeln, ab der sich zusätzliche Beiträge nur noch anteilig leistungssteigernd auswirkten.

- **DIE LINKE** fordert sofort eine Mindestrente von zur Zeit 1050 € netto monatlich.
- **DIE LINKE** erwartet, dass der Solidarausgleich gestärkt wird und alle Erwerbstätigen in die Solidargemeinschaft der gesetzlichen Rentenversicherung einzubeziehen sind.
- Zeiten niedriger Löhne, der Erwerbslosigkeit, der Kindererziehung und Pflege müssen deutlich besser abgesichert werden, damit sie nicht zu Armutsrenten führen.

Diese Forderungen teile ich und erwarte eine Kopplung der Rente an Lohnentwicklung und Inflationsrate.

Gesundheit/Pflege

Die private Krankenversicherung bietet Selbständigen mit geringen Einkommen keine ausreichende gesundheitliche Versorgung. **DIE LINKE** fordert eine solidarische Bürger.innenversicherung in Gesundheit und Pflege wegen der konsequent am individuellen Einkommen orientierten Beitragshöhe. Gerade bei Gesundheit und Pflege dürfen neue Technologien nicht nach dem Prinzip „alles, was technisch geht" eingeführt werden. Der Schutz der Patientinnen und Patienten sowie ihrer sensiblen Gesundheitsdaten erfordern nach Auffassung der *Linke.*n, dass der belegte Patientennutzen in den Mittelpunkt gestellt wird.

Aus meiner Sicht gehört die private Krankenversicherung abgeschafft. Es sollten betriebliche Abkommen zwischen Unternehmen und Krankenkassen zum betrieblichen Gesundheitsmanagement vereinbart werden.

Mindestsicherungen

Forderung **DIE LINKE** *und meine*: Hartz IV ist abzuschaffen. Das System der Grundsicherung ist grundlegend zu einer sanktionsfreien Mindestsicherung für all diejenigen umzubauen, die die gesetzlich definierten Maßstäbe der Hilfebedürftigkeit erfüllen. Es soll eine einkommens- und vermögensgeprüfte, bedarfsdeckende, sanktionsfreie Mindestsicherung eingeführt werden. Mit der Mindestsicherung muss die Verarmung und Entwürdigung von allen Erwerbslosen und Menschen mit geringen Einkommen beendet werden.

Meine Forderung: Ähnlich einer Maschinensteuer müssen Konzepte und Maßnahmen zur Absicherung von Cloud- und Crowdworkern von den Auftraggebern finanziert werden.

Entgrenzung von Arbeit, psychische Belastungen und Arbeitsschutz

Unbestritten ist für **DIE LINKE**, dass neue Technologien die Arbeitswelt verändern. Dabei ist zu beachten, dass die Durchsetzungswahrscheinlichkeit neuer Technologien nicht allein von deren Machbarkeit abhängt, sondern in erster Linie ökonomischen Interessen folgt. Die Stressbelastung in der Arbeitswelt nimmt rasant zu. Die Zunahme von Arbeitsunfähigkeitstagen und psychischen Erkrankungen ist erschreckend.

- **DIE LINKE** fordert eine Reduzierung der gesetzlichen Höchstarbeitszeit.
- Modelle wie die *kurze Vollzeit* und flexible Modelle könnten das Versprechen der Digitalisierung, selbstbestimmter zu arbeiten und zu leben, für alle Wirklichkeit werden lassen.
- Erwerbstätige müssen das Recht auf Nichterreichbarkeit und das Recht auf E-Mail-freien Urlaub haben.

Damit Beschäftigte in Zukunft gesund das Rentenalter erreichen können, muss der Arbeitsschutz mit der technologischen und arbeitsorganisatorischen Entwicklung standhalten. Die steigenden Möglichkeiten der Leistungskontrolle von Beschäftigten befördern einen „beständig steigenden Leistungsdruck".

- **DIE LINKE** fordert eine effektive Anti-Stress-Verordnung gegen Dauerstress, Burn-Out und Arbeit auf Abruf.
- Um mögliche Risiken für die Gesundheit schon frühzeitig vor der Einführung neuer Technologien und Arbeitsmodelle zu

Michael Ahlmann

Michael Ahlmann, Dipl.-Ing., ist nach der Arbeit – als Entwicklungsingenieur und Betriebsratsvorsitzender bei ATLAS ELEKTRONIK in Bremen – 2014 in Rente gegangen. Innerhalb der IG Metall war er viele Jahre europaweit im Bereich Rüstungskonversion und in der gewerkschaftlichen Bildung aktiv. Nach langen Jahren im Arbeitskreis RUIN (Rüstung und Informatik) des FIfF und im Beirat ist Michael jetzt Mitglied des FIfF-Vorstandes und pendelt noch zwischen Kiel und Bremen. In Bremen ist er aktiv im Cyberpeace-Team und in der FIfF-Regionalgruppe.

erkennen, sind vorausschauende Gefährdungsbeurteilungen und Interventionen notwendig.

- Ganzheitliche Gefährdungsbegutachtungen können nur mit den Beschäftigten zusammen erstellt werden. **DIE LINKE** fordert daher im zweiten Schritt, Mitbestimmungsrechte auszuweiten, um Beschäftigte zu beteiligen.

Ich fordere ebenfalls mehr Selbstbestimmung für Beschäftigte bei Teil- und Vollzeit und Beteiligung an betrieblichen Konzepten.

Mitbestimmung

Der digitale Wandel fordert Gewerkschaften und betriebliche Interessenvertretungen heraus. **DIE LINKE** fordert Betriebs- und Personalräte als das notwendige Korrektiv, damit Beschäftigte ihre Vorstellungen mit einbringen und verhindern können, dass technologische Entwicklungen allein zu ihren Lasten umgesetzt werden. Dazu müssen zwingende Mitbestimmungsrechte erweitert werden. Notwendige Voraussetzung für die Handlungsmöglichkeit von Beschäftigten ist daher die Existenz eines Betriebsrates (zurzeit nur in 9 % der Betriebe) mit mehr Mitgliedern und hinreichenden Freistellungen.

Diese Forderungen einer Weiterentwicklung des Betriebsverfassungsrechts teile ich.

Digitalisierung als Beitrag zur Inklusion

Fünf Jahre UN-Behindertenrechtskonvention haben leider nicht viel an der Arbeitssituation von Menschen mit Behinderungen gebessert. Im Gegenteil: Die Arbeitslosenzahlen bei Behinderten steigen entgegen dem allgemeinen Trend weiter an. Die Digitalisierung und damit die Beschleunigung der Arbeitswelt stellen Menschen mit Behinderungen vor neue Herausforderungen.

- **DIE LINKE** setzt sich dafür ein, umfassende Barrierefreiheit und *Universelles Design* als allgemeine Grundprinzipien der Arbeitsstättengestaltung in der Arbeitsstättenverordnung festzuschreiben.

- **DIE LINKE** will auf Bundesebene verstärkt in Forschung und Entwicklung barrierefreier Arbeit investieren.

- **DIE LINKE** fordert, entschleunigte und inklusiv ausgestaltete Arbeitsbereiche zu schaffen, in denen auch Menschen mit hohem Unterstützungsbedarf am Arbeitsleben teilhaben können, z. B. im öffentlichen Dienst.

Diese Positionen zur Inklusion finde ich gut. Es fehlt allerdings ein Zeitplan für die Umsetzung.

Für ein neues Normalarbeitsverhältnis: DIE LINKE

Die Digitalisierung kann die Chance eines gesellschaftlichen Pfadwechsels bieten, der den neoliberalen Kapitalismus überwindet und den Menschen gute Arbeit und ein gutes Leben ermöglicht. Die gesellschaftliche Linke möchte der aktuellen Entwicklung des *Digitalen Wandels* ein Projekt entgegensetzen, das die Bedürfnisse der Menschen in den Fokus der Veränderung stellt. Arbeit muss Sicherheit für Beschäftigte bedeuten, damit das Leben wieder planbarer wird. Arbeit muss Mitbestimmung bedeuten, damit Veränderungen mit den Beschäftigten zusammen verwirklicht werden. Arbeit muss aber auch Selbstbestimmung bedeuteten, denn Arbeitszeit ist Lebenszeit.

Nicht ausreichend oder wenig behandelt werden im Grünbuch und in der Stellungnahme der Linke.*n die grundlegenden Auswirkungen der Digitalisierung auf die Ökologie und die Genderfrage.*

Wir werden die konkreten Auswirkungen auf die Arbeitswelt sehr genau beobachten müssen, um humane Konzepte und Maßnahmen entwickeln zu können. Für mich ist ein Gleichgewicht zwischen „Produktionsarbeit" und Freizeit und Reproduktionsarbeit zu schaffen, denn es gilt:

Arbeiten, um zu leben.

Anmerkungen

1 *http://www.bmas.de/DE/Service/Medien/Publikationen/A872-gruenbuch-arbeiten-vier-null.html*
2 *https://www.arbeitenviernull.de/fileadmin/user_upload/160608_RM_Die_Linke.pdf*
3 *http://www.bmas.de/DE/Service/Medien/Publikationen/a883-weissbuch.html*
4 *http://www.igmetall-berlin.de/aktuelles/meldung/mehr-jobs-statt-mehrarbeit/*
5 *Laut Entwurf Weißbuch sollen Selbständige in die gesetzliche Rentenversicherung kommen können, Crowdworker ähnlich wie Heimarbeitnehmer.innen eingeordnet werden.*
6 *Wolfgang Däubler klassifiziert diese Bereiche in seinem Beitrag in der FIfF-Kommunikation Heft 4/2016 (ab Seite 56).*
7 *Entwurf Weißbuch: Rentenversicherung für alle, Schutzbedürftigkeit von Crowdworking sichern.*
8 *Wolfgang Däubler unterscheidet drei Formen (Microtasks, anspruchsvolle Crowd-Aufgaben und Spezialisten-Crowdwork) – FIfF-Kommunikation Heft 4/2016 (Seite 56).*

Demonstration gegen die Sicherheitskonferenz 2014 – München
Foto: Metropolico.org, CC BY-SA 2.0

Wissenschaft & Frieden 1/2017 „Facetten des Pazifismus“ mit Dossier „Gender, Frauen und Friedensengagement“

Nicht alle, die sich zur Friedensbewegung zählen, sind Pazifist.innen. Friedensbewegte und Pazifist.innen teilen aber die Überzeugung, dass sich Konflikte anders lösen lassen, als durch Krieg. Sie setzen sich dafür ein, dass nicht-militärische Ansätze zum Zuge kommen, um Gewaltspiralen aufzubrechen und Menschen- und Völkerrechte zu schützen. W&F 1/2017 untersucht unterschiedliche Facetten des Pazifismus quer durch die Jahrhunderte, vom dreißigjährigen Krieg bis heute.

Im einzelen schreiben:

- *Christine Schweitzer* – Ein Plädoyer für den Pazifismus
- *Albert Fuchs* – Zu böse für Frieden durch Frieden? Über widerstreitende Menschenbilder
- *Helke Dreier* – Frauen und Frieden nach 1945
- *Norman Paech* – Pazifismus und Völkerrecht
- *Crinna Hauswedell* und *Jürgen Nieth* – Eine kleine Chronik des Pazifismus
- *Anna Lisa Schwartz* – „Deß armen Manns sehnliche Klag“ – Friedensvisionen im Dreißigjährigen Krieg
- *Sebastian Engelmann* – Die Pädagogin Minna Specht – Erziehung für den Frieden
- *Susanne Reitmair-Juárez* – Friedenskonzepte im Wandel – Analyse der Vergabe des Friedensnobelpreises
- *Trägerkreis Internationale Münchner Friedenskonferenz* – Schutz der Menschenrechte durch Prävention

Außerhalb des Schwerpunkts

- befasst sich *Rainer Rilling* mit dem Amtsantritt von US-Präsident Trump: Globale Polarisierung?;
- geht *Ina Wiesner* der Frage nach, warum sich in Deutschland die Soziolog.innen zum Thema Krieg kaum äußern: Das Schweigen der Soziologen;
- befasst sich *Eva Senghaas-Knobloch* mit der Situation in den den besetzten palästinensischen Gebieten und
- *Annette Schramm* mit der Situation in Sierra Leone.
- *Mirko Himmel* untersucht warum bei Massenvernichtungswaffen Abrüstung so schwer ist: Eine verpasste Chance? Die 8. Überprüfungskonferenz des Biowaffenübereinkommens.
- Ein *Dokument der Ständigen Vertretung der USA* bei der NATO vedeutlicht, wie die USA ihre Verbündeten einschwören: Atomwaffenverbot – bloß nicht!?

W&F liegt ein 16 seitiges Dossier bei: **„Gender, Frauen und Friedensengagement“**.

Gender, das sozial konstruierte Geschlecht, ist als Analysekategorie auch und gerade im Kontext von Krieg und Frieden wesentlich: in der Friedenswissenschaft, der Friedensarbeit, der Friedenspolitik und der Friedensbewegung. Das Jubiläum des Frauennetzwerks für Frieden bot die Gelegenheit, diese Ebenen miteinander zu verknüpfen und gleichzeitig eine häufig unterschätzte Größe besonders hervorzuheben: die unermüdliche humanitäre und politische Friedensarbeit von Frauen. W&F-Dossier 84 dokumentiert die Referate des Symposiums Fokus Gender im Friedensengagement – deutsche und europäische Perspektiven sowie Interview-Ausschnitte der anschließenden Festveranstaltung.

Wissenschaft & Frieden 1/2017 „Facetten des Pazifismus“, €9,00 plus Porto.

W&F erscheint vierteljährlich. Jahresabo 35€, ermäßigt 25€, Ausland 45€, ermäßigt 35€, Förderabo 60€. W&F erscheint auch in digitaler Form – als PDF und ePub. Das Abo kostet für Bezieher der Printausgabe zusätzlich 5€ jährlich – als elektronisches Abo ohne Printausgabe 20€ jährlich.

Bezug: W&F, Beringstr. 14, 53115 Bonn,
E-Mail: *buero-bonn@wissenschaft-und-frieden.de,*
www.wissenschaft-und-frieden.de

Mitgliederversammlung (MV) des FIfF

Berlin, 27. November 2016, 10:15–12:00 Uhr

– Beschlussprotokoll[1] –

Sitzungsleitung: Stefan Hügel als Vorsitzender des FIfF.

1. **Begrüßung und Feststellung der Beschlussfähigkeit und der Protokollführung**
   Zur Versammlung ist ordentlich eingeladen worden und diese ist dadurch beschlussfähig.
   Protokollführung: Sylvia Johnigk

2. **Beschlussfassung über Tages-, Geschäfts- und Wahlordnung**
   Geschäfts- und Wahlordnung werden von der MV in bekannter Form genehmigt. Der Tagesordnung wurde in der vorliegenden Form zugestimmt.

3. **Bericht des Vorstandes einschließlich Kassenbericht**
   Stefan Hügel berichtet über die kontinuierliche Arbeit des FIfF seit der letzten MV am 8.11.2015 und über den Haushalt mit Stand 17.11.2016. Außerdem berichten Vertreter der Regionalgruppen. Es wurden keine Beschlüsse gefasst.

4. **Bericht der Kassenprüfer**
   Für die am 11.5.2016 in Bremen durchgeführte Kassenprüfung durch Klaus Lüttich und Gernot Lucks berichtet Klaus Lüttich der MV. Aus dem Kassenprüfungsprotokoll: „Dem Vorstand wird eine dem Vereinszweck entsprechende, ordnungsgemäße Kassenführung bescheinigt. Einer Entlastung des Vorstandes steht nach unserer Auffassung nichts entgegen."

5. **Diskussion der Berichte**
   Termin Klausurtagung in Bremen 10. bis 12. März. 2017 in der Villa Ichon. Der Vorstand lädt die Mitglieder ein. Die GS wird sich um ein Hotel kümmern, aktuelle Nachrichten befinden sich auf der FIfF-Webseite.
   Es wurden keine Beschlüsse gefasst.

6. **Entlastung des Vorstandes**
   Die Kassenprüfer schlagen die Entlastung des Vorstands vor. Die MV entlastet den Vorstand einmütig bei 6 Enthaltungen.

7. **Neuwahl der Kassenprüfer**
   Die MV wählt im Block einmütig bei einer Enthaltung zu den neuen Kassenprüfern des FIfF: Klaus Lüttich (stimmt zu) und Gernot Lucks (hat im Voraus proklamiert, die Wahl anzunehmen).

8. **Diskussion über Ziele und Arbeit des FIfF, aktuelle Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen**
   Es wurden keine Beschlüsse gefasst.

9. **Anträge an die Mitgliederversammlung**
   Es lagen keine Anträge vor.

10. **Verschiedenes**
    Es lagen keine Anträge vor.

11. **Genehmigung des Protokolls**
    Das Protokoll wird einstimmig genehmigt.

1 Inoffizielle Fassung, redaktionell bearbeitet. Die genehmigte offizielle Fassung liegt in der FIfF-Geschäftsstelle vor.

bitte vormerken – bitte vormerken – bitte vormerken – bitte vormerken

FIfF-Konferenz 2017

TRUST – Wem kann ich trauen im Netz und warum?

33. FIfF-Konferenz, 20. bis 22. Oktober 2017, Universität Jena

Vortragende: Prof. Dr. Gabriele Schade (MDR-Rundfunkrat), Prof. Dr. Dorina Gumm (Fachhochschule Lübeck), Dr. Lutz Hasse (Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit) … und viele andere.

Geplante Workshops: „Algorithmen"; Free-to-Play-Spiele; Handys, aber sicher; IT-Sicherheit barrierefrei; Volkszählung – Zensus – Zensus-Vorbereitungs-Gesetz; Wardriving (Stadtbegehung)

Vorschläge für weitere Workshops bitte an:
orgateam@fiffkon.de

Außerdem: FIfF-Mitgliederversammlung mit Neuwahl des Vorstands (der Beginn wurde vorläufig auf Sonntag 10 Uhr festgesetzt)

Laufend weitere Informationen gibt es unter:
https://2017.fiffkon.de

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, Eberhard Zehendner
Schwerpunktredaktion	Benjamin Kees, Rainer Rehak, 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.biskup@gmx.de*. Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *http://www.fiff.de/regional*
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder
Titelbild	Videostill, Alexander Lehmann
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 Autor.innen-Meinung wieder.

Die FIfF-Kommunikation ist das Organ des FIfF und den politischen Zielen und Werten des FIfF verpflichtet. Die Redaktion behält sich vor, in Ausnahmefällen Beiträge abzulehnen.

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.

Wichtiger Hinweis: Wir bitten alle Mitglieder und Abonnenten, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

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

33. FIfF-Konferenz FIfFKon 2017
20. bis 22. Oktober, Universität Jena (siehe auch Seite 90)

FIfF-Kommunikation

2/2017 „Datenschutz handhabbar"
Stefanie Jäckel, Eberhard Zehendner
Redaktionsschluss: 5. Mai 2017

3/2017 „Freiheit 2.0"
Britta Schinzel
Redaktionsschluss: 4. August 2017

1/2018 „TRUST – Wem kann ich trauen im Netz und warum?"
Stefanie Jäckel, Eberhard Zehendner u. a.
Redaktionsschluss: 2. Februar 2018

W&F – Wissenschaft & Frieden

3/16 Politischer Islam
4/16 Weltordnungskonzepte (mit Dossier 83: Ziviles Peacekeeping)
1/17 Facetten des Pazifismus (mit Dossier 84: Gender, Frauen und Friedensengagement)
2/17 Flucht & Migration

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

#213 10 Jahre Versammlungsrecht der Länder
#214 Menschenrechtliche Fragen der Flüchtlingspolitik
#215 Geheimdienste vor Gericht
#216 Rechtspopulismus/Rechtsextremismus
#217 Der Islam als Herausforderung für das deutsche Religionsverfassungsrecht
#218 Rückkehr zum gerechten Krieg?

DANA – Datenschutz-Nachrichten

1/16 – Innere Sicherheit
2/16 – Rote Linien zur EU-DSGVO – Was ist daraus geworden?
3/16 – Beschäftigtendatenschutz in neuen Gewändern
4/16 – Tracking, Profiling, Werbung, Marketing
1/17 – Verbraucherschutz
2/17 – BDSG-Nachfolgegesetz (alternativ: Geheimdienste)
3/17 – 40 Jahre DVD

Das FIfF-Büro

Geschäftsstelle FIfF e. V.
Ingrid Schlagheck (Geschäftsführung)
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*

Bankverbindung
Bank für Sozialwirtschaft (BFS) Köln
Spendenkonto:
IBAN: DE79 3702 0500 0001 3828 03
BIC: BFSWDE33XXX

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

Schluss FIfF

„Erste U-Bahnhaltestelle mit ehrlichen Hinweisen zu Videoüberwachung“

Eine gemeinsame Aktion von FIfF und Digitalcourage im Herzen Berlins

Fotos: © Digitalcourage_SL CC-BY-4.0