

E...I...f...F...Kommunikation

Zeitschrift für Informatik und Gesellschaft

33. Jahrgang 2016

Einzelpreis: 7 EUR

1/2016 – März 2016

Kommerzialisierung des Sozialen



Markt und Macht im Zeitalter digitaler Kompletterfassung

ISSN 0938-3476

• Kryptologie & Krieg • Selbstbestimmt war gestern? • Ausgeglichen oder ausgepowert? •

Inhalt

Ausgabe 1/2016

inhalt

- 03 Editorial
- Stefan HÜgel

Forum

- 04 *Der Brief*: Köln Hauptbahnhof
- Stefan HÜgel
- 05 Betrifft: Cyberpeace – Bedrohungen
- Stefan HÜgel
- 07 Zur Militarisierung der kryptologischen Forschungs-
landschaft an deutschen Forschungseinrichtungen
- Thomas Gruber
- 12 Selbstbestimmt war gestern?
- Dietrich Meyer-Ebrecht
- 16 Thesen für die digitale Revolution
- Gernot Meier
- 18 Ausgeglichen oder ausgepowert?
- Anja Gerlmaier
- 23 Vertrauen erhalten – Datensicherheit und Daten-
schutz bei modernen Fahrzeugen
- Jürgen Bönninger und Udo Schüppel
- 28 Erprobung eines sozialen Netzwerkes für die Unter-
stützung von Familien
- Beate Blättner, Elisabeth Hintz, Werner Winzerling
- 32 Wie ich einen Blick auf die persönlichen Daten werfen
durfte
- Paul-Olivier Dehaye
- 35 Bericht über das Kolloquium *Emergente Systeme.
Information und Gesellschaft*.
- Hans-Jörg Kreowski
- 36 Offener Brief für die Beibehaltung von Bargeld
- AKtiVCongreZ
- 37 Datenschützer schockiert über sogenannten
„Datenschutzschild“
- Deutsche Vereinigung für Datenschutz
- 37 *Internationale Liga für Menschenrechte* protestiert
gegen Frankreichs Antiterror-Notstandspolitik

Retrospektive

- 58 Was ist so faszinierend an der Informatik?
- Dirk Siefkes

„FIfF-Konferenz 2015“

- 39 Smart-TVs im Fokus der Datenschutzaufsichtsbehörden
- Andreas Sachs
- 44 Fairere Computer
- Sebastian Jekutsch
- 45 FIfF-Konferenz 2015: Gedichte
- Hans-Jörg Kreowski
- 46 Zur Idee herrschaftsfreier kooperativer Internetdienste
- Christian Ricardo Kühne
- 50 Techno-Politics as Network(ed) Struggles
- Laura Fichtner
- 54 Internet-Profiling – Umfang, Risiken und Schutzmaß-
nahmen am Beispiel Google
- Angela Meindl

FIfF intern

- 56 Das FIfF verleiht 2016 wieder den FIfF-Studienpreis
- 57 Trauer um Dirk Siefkes
- Hans-Jörg Kreowski
- 64 Allein? Überhaupt nicht!
- Birgit und Michael Ahlmann

Lesen & Sehen

- 65 Informatik und Gesellschaft. Festschrift zum
80. Geburtstag von Klaus Fuchs-Kittowski
- Frank Fuchs-Kittowski, Werner Kriesel (Hg.)
- 66 Praxishandbuch lebensphasenorientiertes Personal-
management, Anja Gerlmaier et al (Hg.)
- Dagmar Boedicker

Rubriken

- 67 Log 1/2016
- Stefan HÜgel
- 75 Impressum/Aktuelle Ankündigungen
- 76 SchlussFIfF

Editorial

Kommerzialisierung des Sozialen – Markt und Macht im Zeitalter digitaler Kompletterfassung, das war das Motto unserer FfF-Konferenz, die vom 6. bis zum 8. November 2015 in Erlangen stattfand. Diese Ausgabe enthält Beiträge aus der Konferenz, zusammen mit einer Vielfalt von Berichten zu weiteren Themen.

Die Konferenz war bereits Thema in der vorigen Ausgabe, in der wir über die Tagung allgemein, über die Verleihung des *FfF-Studienpreises 2015* und über die Mitgliederversammlung mit den Vorstandswahlen berichteten. Dieses Heft enthält zunächst den Beitrag von *Andreas Sachs*, der von den Untersuchungen zur Privatheit von *Smart-TVs* berichtet, die am Bayerischen Landesamt für Datenschutzaufsicht in Ansbach durchgeführt wurden. Das Ergebnis der Untersuchung sollte uns aufmerksam machen: „Das anonyme Fernsehen wurde faktisch abgeschafft. Der Weg, den Smart-TV nicht mit dem Internet zu verbinden, bleibt natürlich bestehen, nur ist dann auch das ‚Smart‘ nicht mehr nutzbar“, stellt Sachs in seinem Beitrag fest. *Sebastian Jekutsch* verweist in einem kurzen Teaser auf seinen Blogbeitrag, den er zum Thema *Fairere Computer* verfasst hat und *Hans-Jörg Kreowski* hat bei der Abendveranstaltung einige Gedichte vorgetragen, die wir ebenfalls in dieser Ausgabe wiedergeben.

Größeren Raum nimmt der zweite Teil des Schwerpunkts ein, der die Beiträge der Träger:innen des FfF-Studienpreises enthält. *Christian Ricardo Kühne*, der den ersten Preis für seine Arbeit *GNUet und Informationsmacht* erhalten hatte, wirft einen kritischen Blick auf die Entwicklung des Internets, wie wir es heute kennen, und entwickelt in seinem Essay das Konzept der herrschaftsfreien kooperativen Internetdienste. Er greift damit das gesellschaftliche Problem „einer aus den Fugen geratenen Informationsmacht“ an, das „in der Verfassung der Telekommunikationsnetze, in denen hauptsächlich Kommunikation verarbeitet wird, und der Verfassung der Informationsverarbeitungsinstanzen, die derzeit die Form von zentralistisch organisierter Informationsverarbeitung haben“, liegt.

Laura Fichtner wurde für ihre Arbeit *Techno-Politics als Network(ed) Struggles* ausgezeichnet. „Wie kann staatliche Überwachung im Sinne der von *Edward Snowden* enthüllten Dokumente als politisches Mittel verstanden werden?“, fragt sie und untersucht den Zusammenhang zwischen der Infrastruktur des Netzes und der Politik. „Die Analyse ... hat gezeigt, dass es möglich ist, in der NSA-Affäre strukturelle Aspekte zu identifizieren, die zeigen, wie solche Überwachungsmethoden auf den strukturellen Aufbau des globalen Netzwerkes abzielen. Indem sie ein zentralisiertes Schattennetzwerk kreieren, suchen sie gewisse globale geopolitische Bestrebungen ins Internet zu übertragen und dort zu verfestigen“, so ihr Fazit.

Die Ergebnisse unserer Preisträgerin *Angela Meindl* waren bereits Thema in der *FfF-Kommunikation 2/2015: Internet-Profiling – Umfang, Risiken und Schutzmaßnahmen am Beispiel Google*. In dieser Ausgabe werden die Ergebnisse nochmals zusammengefasst. Sie stellt in ihrer Arbeit fest, „dass es nicht länger akzeptiert werden darf, dass Daten von Internetnutzer:innen unbemerkt erhoben und gespeichert werden.“

Im ersten Hauptbeitrag des aktuellen Teils, *Zur Militarisierung der kryptologischen Forschungslandschaft an deutschen Forschungseinrichtungen*, stellt *Thomas Gruber* die Frage, „inwiefern sich

ein militärischer Nutzen der Kryptologie auch in der hiesigen zivilen Forschungslandschaft abbildet und welche Konsequenzen sich daraus ergeben.“ Die „höchst bedenklichen Militarisierungstendenzen“, so resümiert er, „stehen allerdings jedweder wissenschaftlichen Intention einerseits und der Idee der gesamten Kryptologie andererseits krass entgegen. ... Fern von monetären Interessen gälte es innerhalb der kryptologischen Forschungsgemeinschaft, das Vertrauen gegenüber Akteur:innen aus dem Militär-, dem Staats- und dem Wirtschaftssektor in Frage zu stellen.“

In seinem Beitrag *Selbstbestimmt war gestern?* fragt *Dietrich Meyer-Ebrecht* nach den Auswirkungen, die sich ergeben, wenn wir das Entscheiden Maschinen überlassen. „Die Gefahr der Algorithmen, die uns Entscheidungen abnehmen, ist nicht nur, dass wir uns von ihnen in einen (fremdgelenkten) Mainstream saugen lassen. ... So werden die gepriesenen Gesetze des Marktes außer Kraft gesetzt – nicht mehr der Kunde ist der König –, und die politische Willensbildung wird den Bürgern unbemerkt aus der Hand genommen“, so sein Fazit.

Eine in der *FfF-Kommunikation* vielleicht ungewohnte Perspektive der Digitalisierung bietet *Pfarrer Gernot Meier*, der seine 10 Thesen für die digitale Revolution aus theologischer Sicht entfaltet.

Über den Umgang von High-Tech-Unternehmen mit der Arbeitskraft schreibt *Anja Gerlmeier* in ihrem Beitrag *Ausgeglichen oder ausgepowert?*, in dem sie die Ergebnisse eines Projekts darstellt, in dem die Nutzung der menschlichen Kompetenzen in unterschiedlichen Arbeits- und Lebensphasen untersucht wurden. Sie stellt fest, dass es für anspruchsvolle Arbeits- und Lebensphasen „in den meisten Unternehmen offenbar Handlungsbedarf, aber bisher keine angemessenen Unterstützungsangebote oder Arbeitsgestaltungs- und Laufbahnkonzepte gibt.“ Das Spannungsfeld zwischen Datenaustausch bei moderner Fahrzeugtechnik, um den Straßenverkehr sicherer, effizienter und ressourcenschonender zu gestalten, und Anforderungen des Datenschutzes und der Datensicherheit beleuchten *Jürgen Bönninger* und *Udo Schüppel* in ihrem Beitrag *Vertrauen erhalten – Datensicherheit und Datenschutz bei modernen Fahrzeugen*. Über das Projekt *FamTIME* zur Erprobung eines sozialen Netzwerkes für die Unterstützung von Familien berichten *Beate Blättner*, *Elisabeth Hintz* und *Werner Winzerling*. Der Erfahrungsbericht von *Paul-Olivier Dehaye*, in dem er berichtet, *Wie ich einen Blick auf die persönlichen Daten werfen durfte, die ein milliardenschweres Unternehmen über mich besitzt* und weitere Kurzberichte und Rezensionen runden die Ausgabe ab.

Eine traurige Nachricht ereilte uns nach Redaktionsschluss: Unser Beirats- und früheres Vorstandsmitglied *Professor Dr. Dirk Siefkes* ist am 19. März 2016 verstorben. Gemeinsam mit einem Nachruf von *Hans-Jörg Kreowski* haben wir ihm zur Erinnerung seinen Beitrag aus der *FfF-Kommunikation 2/1998, Was ist so faszinierend an der Informatik?* als Retrospektive in die Ausgabe aufgenommen.

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

Stefan Hügel
für die Redaktion



Köln Hauptbahnhof

Liebe Leserinnen und Leser, liebe Mitglieder des FfF,

einige Tage nach Silvester 2015 eskalierten die Medienberichte. Was sich zunächst wie eine ganz normale Silvesternacht darstellte – eine erste Meldung der Polizei verlautete: „Ausgelassene Feiern, Stimmung weitgehend friedlich“ –, wurde zum Skandal und beherrschte tagelang die Schlagzeilen der Zeitungen, nicht nur in Deutschland. Die erste Einschätzung der Polizei stellte sich einige Tage später als Fehleinschätzung heraus, wie rund 1.000 Strafanzeigen wegen sexueller Übergriffe, Eigentums- und Körperverletzungsdelikten belegen. Offenbar ist die Situation am Kölner Hauptbahnhof eskaliert, war die Polizei weitgehend machtlos. Der Kölner Polizeipräsident musste als Folge der Ereignisse gar seinen Posten räumen.

Wie konnte es zu dieser Fehleinschätzung kommen? Falsch verstandene politische Korrektheit, sagen einige, und behaupten, die verharmlosende Veröffentlichung sei erfolgt, um die Täter, die sie in den Reihen ausländischer Mitbürger:innen und Geflüchteter vermuten, zu schützen. Oder war es vielleicht doch eine ganz „normale“ Silvesternacht und solche Übergriffe gab es auch schon in den Vorjahren – nur dass sie zuvor von der breiten Öffentlichkeit nicht zur Kenntnis genommen und von den Opfern nicht zur Anzeige gebracht wurden?

Eines ist klar: Sexuelle Übergriffe sind inakzeptabel, und wenn es sich dabei um Straftaten handelt, entsprechend zu ahnden. Egal, ob sie von Menschen aus Luxemburg, Syrien, Deutschland, Japan, den Niederlanden oder irgend einem anderen Staat begangen werden. Egal, ob die Täter:innen säkulare Humanist:innen, christlichen, muslimischen, hinduistischen, buddhistischen oder eines anderen Glaubens sind.

Die allzu einfache Erklärung für die Vorfälle in Köln (und, weniger beachtet, auch in anderen Großstädten) wurde dann schnell politisch ausgeschlachtet und in eine Kampagne gegen eine offene Flüchtlingspolitik umgemünzt. Die Folgen sind besorgniserregend: Es drängt sich der Eindruck auf, dass „Köln Hauptbahnhof“ eine Art Dammbbruch markiert, dessen Folgen das Land nach rechts kippen lassen. Dies scheinen auch die Ergebnisse der letzten Wahlen in Hessen, Baden-Württemberg, Rheinland-Pfalz und Sachsen-Anhalt zu belegen. Die Ereignisse leisteten einem Rassismus vor allem in sozialen Netzwerken Vorschub, der in keiner Weise hinzunehmen ist. Die Anträge auf den kleinen Waffenschein und die Nachfrage nach Waffen wie Pfefferspray schnellten



Der Kölner Hauptbahnhof um 1900 – friedliche Zeiten?

nach oben. (Inwieweit die Medien aufgrund des in solchen Fällen inzwischen üblichen Stakkatos von Sensationsberichten, vor allem auf den Internet-Portalen, eine Mitverantwortung für die entstehende Stimmung trifft, mögen sie selbst beurteilen.)



Auch die gewohnten wohlfeilen politischen Reaktionen aus den etablierten Parteien geben wieder zur Sorge Anlass. Einmal mehr wurden Strafverschärfungen gefordert, schnellere Abschiebung „straffällig“ gewordener Asylbewerber. Die Beteuerung, dass die offensichtliche Beteiligung von Menschen mit Migrationshintergrund an den Taten aber nicht dazu führen dürfe, „dass nun Flüchtlinge gleich welcher Herkunft, die bei uns Schutz vor Verfolgung suchen, unter einen Generalverdacht gestellt werden“, wirkt dabei wie ein Lippenbekenntnis. So wenig Straftaten akzeptabel sind, so wenig kann es die Lösung sein, Menschen in ein Land abzuschieben, in dem ihnen Verfolgung und Tod drohen. Prävention und eine Stärkung des Rechtsstaats wurden gefordert – gerade letzteres eine Forderung, die man gerne auch aus diesen Kreisen hören würde, wenn wieder einmal Grundrechte in Deutschland und Europa abgebaut werden sollen. Es erscholl der Ruf nach Videoüberwachung – dumm nur, dass es am Kölner Hauptbahnhof bereits Videoüberwachung gibt, die Aufnahmen – aus der Ferne und bei Nacht – aber erwartungsgemäß weitgehend unbrauchbar waren.

Unsere Gesellschaft muss mit Ereignissen wie an Silvester am Kölner Hauptbahnhof angemessen umgehen. Das heißt, Schutz vor Übergriffen zu bieten und Straftäter mit den angemessenen Mitteln des Rechts zu verfolgen. Es heißt nicht, solche Ereignisse gegen Bevölkerungsgruppen und gegen die Grundrechte politisch zu instrumentalisieren.

Mehrere schreckliche Anschläge mit vielen Toten ereigneten sich in den letzten Tagen – in Brüssel, in Bagdad und in Lahore. Es ist wohl nachvollziehbar, dass uns die Ereignisse im nahen Belgien, in der Hauptstadt Europas, stärker berühren als die Ereignisse im (vergleichsweise) fernen Irak und in Pakistan, doch sollten wir bei der Trauer um die Opfer von Brüssel die Opfer von Bagdad und Lahore nicht vergessen.

Auch hier gab es die leider inzwischen gewohnten Reaktionen. Kirsten Fiedler, die als *Managing Director* von EDRI in Brüssel arbeitet, schreibt dazu:

Am Tag danach stellt sich langsam die Frage, wie die Politik antworten wird. Denn seit 9/11 gibt es nach jedem Anschlag dasselbe erbärmliche Ritual: Es wird danach gerufen, Sicherheitsmaßnahmen maßlos aufzurüsten.

(netzpolitik.org, 23. März 2016)

Die Aufzählung der Details spare ich mir hier; es sei empfohlen, den vollständigen Beitrag auf *netzpolitik.org* zu lesen. Genauso wie in Köln gilt: Unsere Gesellschaft muss mit solchen Ereignissen angemessen umgehen. Dieser Tage ist wieder häufig vom „An-

griff auf unsere Freiheit und unsere westlichen Werte“ die Rede – vielleicht lohnt es, auch einmal die Perspektive eines Drohnenopfers in Pakistan auf die westlichen Werte einzunehmen.

Absolute Sicherheit ist eine Illusion – so schweres fällt, das angesichts der Todesopfer zu akzeptieren. Das heißt selbstverständlich auch, Terroristen und andere Straftäter zu verfolgen und nach den Maßstäben des Rechts angemessen zu bestrafen.

Stefan Hügel

Es heißt nicht, solche Ereignisse gegen Bevölkerungsgruppen und gegen die Grundrechte politisch zu instrumentalisieren – und die Reaktion darauf erst zu dem eigentlichen „Angriff auf unsere Freiheit“ zu machen.

Mit Fliffigen Grüßen

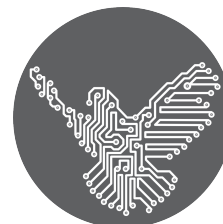
Stefan Hügel



Betrifft: Cyberpeace

Bedrohungen

*Diesmal funktioniert alles.
(Spliff, „Computer sind doof“, 1982)*



Wir leben heute unter vielfältigen Bedrohungen. Gerade haben uns die Anschläge in Brüssel wieder die Verwundbarkeit unserer hochintegrierten und -technisierten Zivilisation vor Augen geführt. Man kann den Terrorismus dieser Anschläge als Angriff auf Europa und unsere Gesellschaft begreifen. Man kann ihn aber auch als Reaktion auffassen – auf die Bedrohung, die unsere westlichen Gesellschaften ihrerseits für die Gesellschaften des Nahen Ostens darstellen: Durch konventionelle militärische Angriffe und durch Cyberwarfare, wie Drohnenangriffe und Angriffe auf Industrieanlagen. Wir führen einen unerklärten, neuen Krieg in diesen Staaten – wer diesen Krieg angefangen hat, hängt wie so häufig vom Standpunkt ab.

Allgegenwärtige Bedrohung – das war das Umfeld, in dem das FlifF 1984 gegründet wurde. Es ist heute kaum noch vorstellbar, ständig unter dem Damoklesschwert einer Auslöschung der Menschheit, mindestens aber der uns vertrauten Zivilisation, zu leben. Ständiger Fluglärm durch übende Tiefflieger führte uns die Bedrohung jeden Tag plastisch vor Augen und Ohren. Offenbar gab es mehrere Vorfälle, bei denen es nur der Besonnenheit einzelner Menschen im letzten Moment zu verdanken war, dass es damals nicht zum Äußersten kam.

Verstärkt wurde die Bedrohung durch das SDI-Programm, im Volksmund auch *Star Wars* genannt, des damaligen US-Präsidenten Ronald Reagan. Experten der Informatik, die sich kurze Zeit später im FlifF zusammenfinden sollten, wussten: Was uns hier als Mittel gegen die atomare Bedrohung verkauft werden sollte, verstärkte diese zusätzlich, indem man Maschinen – damals noch weniger zuverlässig als heute – mit der Entscheidung betrauen wollte, das atomare Feuer bei einem Angriff des Gegners auszulösen. Der *Unsicherheitsfaktor* Mensch, der zuvor noch das Schlimmste verhindert hatte, konnte *endlich* ausgeschaltet werden. Der Versuch, diesen automatisierten Atomtod, oder *Atomkrieg aus Versehen*, verfassungsrechtlich anzugreifen, scheiterte bekanntermaßen.

Die Gefahr der weltweiten atomaren Vernichtung scheint (vorläufig) gebannt. Die Bedrohungen durch Cyberwarfare sind heute real, erscheinen aber abstrakt und sind für viele unsichtbar – lediglich wenn Cyberkriminelle eine große Zahl von Computern mit Schadsoftware infizieren, wie es derzeit mit der Ransomware *Locky* geschieht, wird uns die Bedrohung bewusst. Auch hier wurden lebenswichtige Einrichtungen – Krankenhäuser – geschädigt. Wenn es sich hier auch um Kriminelle handelt und nicht um Militärbehörden: Die Methoden sind die gleichen und sie richten die gleiche Art von Schaden an.

Bedrohungen durch Cyberwarfare lassen sich unter vier Kategorien fassen: Bedrohung der Grundrechte und der Sicherheit unserer Infra-

struktur durch Maßnahmen der Ausspähung und Überwachung, Bedrohung des Lebens Unschuldiger und rechtsstaatlich als unschuldig geltender durch Drohnen – ferngesteuert oder autonom –, Bedrohung von technischen Anlagen – militärisch oder zivil – durch Schadsoftware und Bedrohung unserer Demokratie durch *Information Warfare*, die Täuschung und Manipulation der Öffentlichkeit – auch unbeabsichtigt – durch Medien und nachrichtendienstliche Mittel.

Überwachung

Cyberwarfare beginnt mit der Überwachung der Zivilgesellschaft – diese Ausspähung der Menschen verletzt ihre Privatsphäre und damit die Menschenwürde als ein elementares Menschenrecht. Doch der Schaden, den die Überwachungsmaßnahmen anrichten, ist größer: Voraussetzung für die Überwachung ist die Manipulation von IT-Systemen und die Geheimhaltung oder sogar der absichtsvolle Einbau von Schwachstellen. Die Folge sind unzuverlässige und unsichere Computer- und Kommunikationssysteme wie Internet oder Mobilfunknetze, von deren reibungslosem Funktionieren gleichzeitig weite Teile unserer Gesellschaft abhängig sind. Durch die Ausrüstung für die Cyberwarfare wird auch in Friedenszeiten die Sicherheit der zivilen IT-Infrastruktur ausgehöhlt und untergraben.

Drohnenangriffe

Ausspähung und Computermanipulationen bereiten konventionelle militärische Operationen vor, beispielsweise rechtswidrige Drohnenangriffe durch die Ortung von Zielpersonen, und sie sind damit die Grundlage aggressiver (kriegerischer) Operationen. „*We kill people based on Metadata*“, diese Aussage des ehemaligen Direktors von CIA und NSA, General Michael Hayden, macht den Zusammenhang zwischen nachrichtendienstlicher Ausspähung und extralegalen Tötungen klar. Drohnenangriffe for-

dern laufend zahlreiche Opfer unter Unbeteiligten. Angriffe, die auf unsicheren Eigenschaften der Ziele basieren (*Signature Strikes*) richten sich gegen Opfer, gegen die nicht einmal ein hinreichender Verdacht besteht. Computergestützte militärische Operationen erzeugen zusätzlich die Illusion eines *sauberen* Krieges und senken damit die Schwelle des Einsatzes. Weiter gesteigert wird das Bedrohungspotenzial durch Systeme, die autonom agieren, also automatisiert töten. Dass wir von einer funktionierenden Maschinenethik noch weit entfernt sind, zeigt vielleicht auch der Fall des Microsoft-Chatbots *Tay*, der sich binnen kurzer Zeit vom virtuellen Hipster-Mädchen zum Hitler-Bot entwickelte und nach kurzer *Umlernphase* autonom Hass-Kommentare twitterte.

Schadsoftware

Staatliche Cyberkrieger sind heute die ressourcenstärksten Hackerorganisationen weltweit. Ihre Cyberangriffe sind nicht zu kontrollieren und gefährden neben ihren eigentlichen Zielen auch zivile Systeme, wie etwa Systeme zur Sicherstellung lebenswichtiger Ressourcen (Wasser, Energie), Krankenhäuser oder Chemiewerke. Der gegen eine iranische Atomanlage gerichtete *Stuxnet*-Wurm breitete sich weltweit aus. Wir können wohl davon ausgehen, dass es weitere gefährliche Trojaner vom *Stuxnet*-Format als *APT* – *Advanced Persistent Threats* – von staatlicher Herkunft gibt.

Die Schadsoftware Stuxnet, entdeckt im Jahre 2010, wurde für einen Angriff auf die Urananreicherungsanlage des Iran in Natanz und das Kernkraftwerk Buschehr eingesetzt. Es handelt sich dabei um ein Schadprogramm zum Angriff auf ein System zur Überwachung und Steuerung der Firma Siemens (Simatic S7), das in die Steuerung von Frequenzumrichtern, z.B. zur Steuerung der Geschwindigkeit von Motoren, eingreift. Durch Manipulation der Drehzahl wurden die Zentrifugen zur Urananreicherung beschädigt. Die Schadsoftware wurde dafür über mobile Feldprogrammiergeräte (spezielle Notebooks) in die physisch isolierten Prozesssteueranlagen eingeschleust. Aufgrund seiner hohen Komplexität und seines Zieles, Steuerungssysteme von Industrieanlagen zu sabotieren, gilt Stuxnet bisher als einzigartig. Es wird angenommen, dass die Schadsoftware durch staatliche Akteure in den USA und in Israel gezielt zur Zerstörung iranischer Atomanlagen entwickelt wurde; für staatliche Stellen spricht die hohe Komplexität und der damit verbundene Aufwand für die Erstellung der Software.

Der Einsatz von Cyberwaffen durch Staaten ist eine Kriegshandlung mit erheblichem Eskalationspotenzial, die die internationale Sicherheit erheblich gefährdet.

Manipulation

Aufgrund ihrer mangelnden Transparenz sind militärische und geheimdienstliche Institutionen grundsätzlich schwer zu kontrollieren. Informationen zu Bedrohungen und Schwachstellen können manipuliert, verfälscht oder irreführend sein. Demokratische und parlamentarische Gremien werden falsch und unzureichend informiert oder schlicht belogen. Kontrollgremien sind ungenügend ausgestattet und können deswegen ihrer Aufgabe nicht umfassend nach-

kommen. Die unzureichende Information des NSA-Untersuchungsausschusses hat uns das Beispiel der NSA-Selektoren deutlich vor Augen geführt. Wie stichhaltig die Gründe für Geheimhaltung sind, kann die Öffentlichkeit nicht überprüfen – die Einstufung wird von den zu kontrollierenden Behörden selbst vorgenommen. Uns allen bekannt ist die Behauptung des damaligen Chefs des Bundeskanzleramts, Ronald Pofalla, als er die Debatte um die Snowden-Dokumente mit den Worten für beendet erklärte, die Vorwürfe seien nun „vom Tisch“. Dieser Manipulationsversuch brachte Pofalla vor allem Häme ein. Doch Manipulation kann nicht immer so schnell aufgedeckt werden. Auch das zuverlässig einsetzende Medienstakkato nach Anschlägen – wenn auch nicht politisch, sondern wohl eher wirtschaftlich motiviert – trägt zur Verunsicherung der Bevölkerung bei und wird zu gern politisch ausgenutzt, um sofort Forderungen nach weiterer Aufrüstung bei Militär, Geheimdiensten und anderen Sicherheitsbehörden zu erheben.

... und Deutschland mittendrin

Nachrichtendienste kaufen beispielsweise *Zero-Day-Exploits* auf, um die damit verbundene Kenntnis von Schwachstellen in Softwaresystemen für Angriffe nutzen zu können. Auch wenn dem BND bisher offenbar weniger Geld bewilligt wurde als beantragt: Dies macht sehr deutlich, dass sich auch deutsche Behörden am Cyberkrieg beteiligen wollen. Nach den *Strategischen Leitlinien Cyber-Verteidigung* des Bundesministeriums der Verteidigung hätten offensive Cyber-Fähigkeiten das Potenzial, das Wirkspektrum der Bundeswehr signifikant zu erweitern. Möglich seien offensive Maßnahmen zur Beeinträchtigung von fremden Informations- und Kommunikationssystemen sowie der darin verarbeiteten Informationen. Das wäre nicht nur ein Verstoß gegen die Verpflichtung zur *Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, die das Bundesverfassungsgericht 2010 festgestellt hat, sondern auch gegen die verfassungsrechtliche Unzulässigkeit von Angriffskriegen. Auch Drohnen sind ein Thema für die Bundeswehr: Nachdem die Nutzung der Drohne *EuroHawk* an fehlenden Genehmigungen für den Einsatz gescheitert ist, ist die Anschaffung auch von Kampfdrohnen offenbar geplant (möglicherweise Drohnen wie die israelische *Heron* oder die US-amerikanische *Reaper*, die acht *Hellfire*-Raketen tragen kann). Später soll es offenbar auch eine deutsche Beteiligung an der Entwicklung einer europäischen Drohne geben – Berichten zufolge sind hierfür 660 Millionen Euro eingeplant. Im Projekt *Eikonal* ist Deutschland auch an der Ausspähung des Frankfurter Knotens DE-CIX beteiligt.

Bedrohungen

Die Bedrohungen durch Cyberwarfare sind vielfältig. Auch wenn wir nicht mehr unter dem Damoklesschwert des millionenfachen Atomtods leben müssen: Cyberwaffen bedrohen uns und andere. Und sie haben auch indirekte Folgen: Kann ein potenzieller Selbstmordattentäter in einer europäischen Hauptstadt auch dadurch zum Terrorakt motiviert werden, dass er mitansehen muss, wie seine Familie im Feuer eines Drohnenangriffs ums Leben kommt?

Bedrohungen produzieren Angst und Angst produziert neue Bedrohungen: Die Rüstungsspirale nicht nur im Cyberspace muss ein Ende haben.



Zur Militarisierung der kryptologischen Forschungslandschaft an deutschen Forschungseinrichtungen

Die ganze Mathematik ist in drei Teile geteilt: die Kryptographie (bezahlt von der CIA, dem KGB und Ähnlichen), die Hydrodynamik (unterstützt von den Hersteller:innen von Atom-U-Booten) und die Himmelsmechanik (finanziert vom Militär und anderen Institutionen, die sich mit Raketengeschossen auseinandersetzen, wie die NASA).¹

– Vladimir Arnold

Für jede Form des Umgangs mit sensiblen Daten gilt eine zentrale Prämisse: Was nicht mitgehört und mitgelesen werden soll, wird verschlüsselt. Daher sind Techniken der Verschlüsselung auch in zahlreichen Bereichen des alltäglichen Lebens zu finden – in der privaten Kommunikation, bei bargeldlosen Geldtransfers, bei der Speicherung von personenbezogenen Daten (wie beispielsweise Patientenakten) und vielem mehr. Kaum verwunderlich also, dass sich das auch in der Forschung zu Verschlüsselungstechniken widerspiegelt: Die Kryptologie ist derzeit eines der am intensivsten beforschten Teilgebiete der angewandten Mathematik. Ebenso offensichtlich wie der individuelle und zivile Nutzen sicherer Verschlüsselung ist allerdings auch ein staatlicher, wirtschaftspolitischer und militärischer. Die Forschung an neuen Verschlüsselungstechniken wird dabei gepaart mit Angriffen auf bereits etablierte Systeme, was zur Abschirmung eigener kritischer Daten und der simultanen Abhörung des gewählten Feindes oder Gegners befähigt.

Mit einem Blick auf die Arbeit deutscher Forschungseinrichtungen stellt sich die Frage, inwiefern sich ein militärischer Nutzen der Kryptologie auch in der hiesigen zivilen Forschungslandschaft abbildet und welche Konsequenzen sich daraus ergeben. Nach einer kurzen begrifflichen und historischen Einordnung der Kryptologie soll hierzu anhand fachtypischer Beispiele die Militarisierung der kryptologischen Forschungslandschaft veranschaulicht werden. Die Formen der militärisch-akademischen Kooperation lassen sich dabei wie folgt gliedern:

- Militärische Drittmittelkooperationen mit deutschen Universitäten
- Kriegsrelevante Forschungsprojekte an deutschen Forschungsinstituten mit universitärer Beteiligung
- Offener Austausch zwischen militärisch und zivil Forschenden auf kryptologischen Fachtagungen
- Beeinflussung der zivilen Forschungslandschaft durch militärische Interessenträger:innen

Begrifflichkeiten und Forschungsbereiche der Kryptologie

Fachlich teilt sich die Kryptologie in die *Kryptographie*, die Forschung zu möglichst sicheren Systemen der Verschlüsselung, und die *Kryptoanalyse*, die Suche nach erfolgversprechenden Angriffsschemata und Schwachstellen etablierter Kryptosysteme.² Beide Fachbereiche sind in der Kryptologie allerdings fast untrennbar eng verwoben – mit gutem Grund. Mathematisch lässt sich die Sicherheit eines Kryptosystems nicht beweisen – in endlicher Zeit ist jede Verschlüsselung zu brechen. Mit Hilfe der Kryptoanalyse kann aber verdeutlicht werden, ob dieser endliche Zeitraum für ein Menschenleben realistisch wäre. Das Abwägen, Ausprobieren und die Suche neuer Angriffstaktiken auf Kryptosysteme ist also auch ein ständiger Legitimationsfaktor für die Güte der Verschlüsselung.

Der Namens- und Definitionsraum kryptologischer Forschung begründet sich weitgehend auf eine mathematisierte Darstel-

lung von Strukturen und Algorithmen zur Ver- und Entschlüsselung von Nachrichten. Dabei sind die verschiedenen Verfahren in der Kryptologie so zahlreich wie vielfältig: Es existieren *symmetrische* (*Private-Key*) und *asymmetrische* (*Public-Key*) Verschlüsselungstechniken, Methoden zum sicheren Schlüsselaustausch, Identifikationsverfahren und vieles mehr. Auch kryptoanalytische Angriffe auf gesamte Kryptoverfahren oder auf verwundbare Teile der theoretischen Konzepte nehmen eine zentrale Rolle in der kryptologischen Forschung ein.

Die historische Verbindung zwischen Kryptologie und Krieg

Schon die Stichworte *Mathematik* und *Krieg* verleiten oft zur Assoziation mit der von der nationalsozialistischen Wehrmacht im Zweiten Weltkrieg genutzten Chiffriermaschine *Enigma* und deren spektakulärer Entschlüsselung durch alliierte Mathematiker:innen in Bletchley Park. Und auch sonst ist die Militärgeschichte durchzogen mit der Entwicklung möglichst sicherer Kryptosysteme und feindlichen Angriffen auf dieselben: die *Skytale*, die von den Spartanern 404 v. u. Z. benutzt wurde, um Kriegsbotschaften zu übermitteln;³ die *Caesar-Chiffre*, mit der der römische Feldherr seine Kommunikation auf dem Schlachtfeld verschlüsselte;⁴ die Nutzung der *Vigenère-Chiffre* durch die Südstaaten im US-amerikanischen Bürgerkrieg und die erfolgreichen kryptoanalytischen Angriffe der Nordstaaten;⁵ die Entschlüsselung des *Zimmermann-Telegramms*, das zum Kriegseintritt der USA im Ersten Weltkrieg führte;⁶ die kryptoanalytischen Angriffe des US-Militärs auf japanische Militärcodes, die den Kriegsverlauf der 1940er-Jahre im Pazifik grundlegend änderte⁷, und vieles mehr. Zu beachten ist dabei vor allem eine Parallele: Die taktisch relevanten Nachrichten, die innerhalb einer Kriegspartei versandt wurden, sollten so sicher als möglich verschlüsselt sein. Erfolgreiche feindliche Angriffe auf die verwendete Verschlüsselung veränderten andererseits nicht selten den Kriegsverlauf erheblich. Mit der zunehmenden Bedeutung der Kryptographie im zivilen Sektor der Kommunikation gerät oft die Tatsache in den Hintergrund, dass die Kryptologie ein Kind des Krieges ist. Denn die kryptologischen Anwendungen reichten in den ersten Jahrhunderten ihrer Entstehung kaum

über die Ver- und Entschlüsselung kriegs- oder staatsrelevanter Nachrichten hinaus.

An der Bedeutung der Kryptologie für die Kriegsführung hat sich selbstverständlich auch in modernen Kriegen nichts geändert. Allein die *National Security Agency (NSA)* dient in ihrer Geschichte und nach aktuellen Erkenntnissen über ihr Wirken als exemplarische Stellvertreterin für die zentrale Rolle der Kryptologie im militärischen und wirtschaftlichen Wettstreit zwischen Nationalstaaten.^{8,9} Die NSA wurde auf Befehl des US-Präsidenten Harry S. Truman im Jahr 1952 unter Geheimhaltung und ohne Rücksprache mit dem Kongress als Zusammenschluss diverser militärischer Geheimdienste – zunächst zur *Armed Forces Security Agency* – gegründet. Zwar blieb die NSA nach wie vor dem US-Verteidigungsministerium unterstellt, doch sollte sie nach Trumans initialer Intention der gesamten US-Regierung dienen; eine Aufgabe, die nach wie vor die Ziele der Behörde bestimmt. Die NSA akquiriert sensible elektronische Kommunikationsdaten, entschlüsselt diese und wertet sie schließlich unter militär- und wirtschaftspolitischen Gesichtspunkten aus. Geschichtlich hat sich allein die politische Lage, nicht die Zielsetzung der geheimdienstlichen Arbeit gewandelt: Im Kalten Krieg, im selbsterklärten *Kampf gegen den Terrorismus* oder in der Spionage in „befreundeten“ Staaten – immer war und bleibt das Ziel, mit kryptologischen Mitteln einer militärischen und wirtschaftlichen Überlegenheit des US-amerikanischen Staates zuzuarbeiten.

Direkte Drittmittelkooperation mit deutschen Universitäten

Für eine geheime Kommunikation zwischen zwei Personen mittels eines symmetrischen Kryptosystems gilt es, sich zunächst auf einen gemeinsamen Schlüssel zu einigen, mit dem die Nachrichten verschlüsselt werden können. Da aber Nachrichtenkanäle oft abhörbar sind, muss eine sichere Methode zum Schlüsselaustausch über jene Kommunikationswege gefunden werden. Der Diffie-Hellman-Schlüsselaustausch beispielsweise nutzt die diskrete Exponentialfunktion als sogenannte *Einwegfunktion*, also eine Funktion, deren Umkehrfunktion – der diskrete Logarithmus – nur unter enormem Rechenaufwand zu lösen ist.

An dieser Stelle knüpft auch die Fragestellung des Bundesministeriums der Verteidigung an, von dem die Universität Leipzig 2013 mit einer Studie zu den „Möglichkeiten und Grenzen der Berechnung des diskreten Logarithmus“ beauftragt wurde.¹⁰ Das militärische Interesse an der Berechenbarkeit einer Funktion, mit der die Sicherheit ganzer Kryptosysteme steht und fällt, ist denkbar vielseitig begründet: Einerseits bietet sie Ansatzpunkte für kryptologische Angriffe auf feindliche Kommunikationsstrukturen in deutschen Kriegseinsätzen oder auf andere selbstgewählte Ziele außerhalb kriegerischer Handlungen wie Privatpersonen, Staaten oder Unternehmen. Andererseits gibt eine solche Analyse Aufschluss über die derzeitige und zukünftige Sicherheit der eigenen Kryptosysteme, mit denen die Kommunikation in ebendiesen Konflikten verschlüsselt wird. Die Auslagerung einer solchen Studie in ein universitäres Forschungsprojekt scheint sinnvoll: Das Thema des diskreten Logarithmus entstammt direkt der theoretischen algebraischen Forschung.

Im mathematischen Sinne stellt die diskrete Exponentialfunktion mit einer gut gewählten strukturellen Basis eine äußerst vielversprechende Einwegfunktion dar – ein diskreter Logarithmus kann zunächst nicht in realistischer Zeit rechnerisch bestimmt werden. Die Angreifbarkeit einer Verschlüsselung hängt allerdings nicht allein von einer Berechenbarkeit des diskreten Logarithmus ab, sondern auch von möglichen Schwachstellen der zugrunde liegenden mathematischen Strukturen und der jeweiligen Umsetzung des Verschlüsselungsalgorithmus. Im Oktober 2015 stellten einige Kryptolog:innen auf der *Conference on Computer and Communications Security* (z.Dt. *Konferenz zur Computer- und Kommunikationssicherheit*) einen Angriff auf eine weit verbreitete Implementierung des Diffie-Hellman-Schlüsselaustauschs (namens *DHE_EXPORT*) vor – die *Logjam-Attacke*. Diese kryptoanalytische Attacke basiert auf einer massiven Vorberechnung von Werten gewisser diskreter Logarithmen und benötigt daher eine enorme Rechenleistung der verwendeten Infrastruktur.¹¹ Allerdings stehen gerade großen Unternehmen sowie staatlichen und militärischen Akteur:innen jene Hochleistungsrechner meist auch zur Verfügung. Die Analyse geleakter NSA-Dokumente legt nahe, dass der amerikanische Geheimdienst den Logjam-Angriff bereits durchführen kann, was bedeuten würde, dass ein erheblicher Teil einiger im Internet genutzter Verschlüsselungssysteme angreifbar wäre (genauer 66 % aller IPsec-VPNs und 26 % der SSH-Server).¹²

Einige der neuesten Angriffsschemata auf die diskrete Exponentialfunktion befassen sich mit der vergleichsweise jungen *Elliptic Curve Cryptography* (kurz *ECC*).¹³ Gravierende Fehler in der Implementierung der ECC-Kryptosysteme wären zwar vermeidbar, sind allerdings keinesfalls immer offensichtlich – oft werden unsichere Algorithmen erst in diesbezüglichen mathematischen oder informatischen Forschungsprojekten aufgedeckt. Ein Beispiel für die Ausnutzung einer unzureichenden Implementierung sind sogenannte *Seitenkanalattacken*: Angreifer:innen können bei einem ECC-System häufig schon über die Rechenzeit der Exponentialfunktion Informationen über den verwendeten Schlüssel gewinnen.¹⁴

Forschungsprojekte an externen Forschungsinstituten mit universitärer Beteiligung

Außerhalb des engeren universitären Kontexts finden sich Interessent:innen für kriegsrelevante Forschung auch an externen Forschungseinrichtungen. Institute zur Förderung angewandter Forschung – wie beispielsweise die Fraunhofer-, Leibnitz- oder Max-Planck-Institute – verstehen sich meist als Dienstleister für Staat, Militär, Industrie und Wirtschaft, in deren Kreisen sie Forschungsergebnisse als Produkte vermarkten und vertreiben. Allerdings überschneidet sich nicht selten die personelle Besetzung eines Instituts stark mit nahegelegenen Hochschulen – viele Projekte überlagern sich in die staatlich wohlfinanzierte Bildungseinrichtung und die Forschungsinhalte werden von den Lehrstuhlinhaber:innen zur Weiterbearbeitung an den Mittelbau und die Studierenden herangetragen. So wird auch eine unproblematisierte Form der Rüstungsforschung an deutschen Forschungseinrichtungen möglich, die Mitglieder der Hochschulen mit einbezieht und einen Verweis auf den außeruniversitären Charakter der Projekte bei kritischen Nachfragen über kriegsrelevante Forschung zulässt.

Kryptologisch relevant ist in diesem Sinne beispielsweise die Zusammenarbeit zwischen der Arbeitsgruppe *Cyber Analysis and Defense* des *Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE)* mit Sitz in Wachtberg-Werthhoven und den Hochschulen in Bonn.¹⁵ Große Teile der Angestellten des FKIE und dessen Institutsleitung finden sich in der Personalstruktur des Instituts *Informatik 4* der Universität Bonn wieder und auch inhaltlich entsprechen sich einige Forschungsbereiche der beiden Einrichtungen.^{16,17,18} Kriegsrelevante Forschungsergebnisse werden über das FKIE beworben, wie beispielsweise regelmäßig auf der stark militärisch geprägten Fachausstellung des *Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung (AFCEA)* – im Jahr 2015 unter dem Motto „IT ‚organisiert‘ – Bundeswehr und Behörden in der digitalen Welt“.^{19,20} Eines der laufenden kryptologisch orientierten Projekte am FKIE ist die Entwicklung eines Systems für den „sicheren Informationsaustausch zwischen militärischen Einheiten“ in der „vernetzten Operationsführung“ namens *IDP/MIKE*.²¹ Die Zusammenarbeit zwischen dem FKIE und den Bonner Hochschulen wird hierbei nicht öffentlich benannt, sie findet sich aber thematisch in mehreren studentischen Abschlussarbeiten wieder.^{22,23,24}

Das Ziel des IDP-MIKE-Systems ist, ein *Virtual Private Network (VPN)* zu implementieren, das in militärischen Einsatzszenarien eine fehlerresistente und dynamische private Kommunikation innerhalb einer Kriegspartei ermöglicht. Ursprünglich bildet ein VPN – wie schon der Name sagt – ein privates Netzwerk für ausgewählte Kommunikationspartner:innen, die sich in einem offenen oder unsicheren Netzwerk (z. B. im Internet oder einem öffentlichen lokalen Netzwerk) befinden. Innerhalb des VPN kann schnell und zuverlässig kommuniziert werden, nach außen wird die Kommunikation verschlüsselt. Herkömmliche VPNs fußen meist auf der Annahme eines während der Kommunikation feststehenden Rechners ohne plötzliche Verbindungsabbrüche und der Eigeninitiative der einzelnen Nutzer:innen beim Kommunikationsaufbau. Beide Voraussetzungen sind in Kriegsszenarien nicht immer erfüllbar, der taktische Mehrwert eines VPNs zwischen den militärischen Einheiten wäre allerdings unbestreitbar. Daher stehen bei der Entwicklung der IDP-MIKE-Software drei wünschenswerte Eigenschaften im Mittelpunkt:

- Das VPN soll von fachfremden Nutzer:innen (z. B. Soldat:innen)
- unter schwierigen Einsatzbedingungen (z. B. Krieg)
- möglichst wartungsfrei verwendbar sein.²⁵

Für die Softwarelösung bedeutet das konkret, dass netzwerkfähige Geräte innerhalb einer Kriegspartei sich selbstständig er-

kennen, miteinander verbinden und bei einem Netzwerkausfall erneut die Kommunikation aufbauen können – insgesamt also eine mobile, dynamische VPN-Lösung. Tests zur Praktikabilität des IDP-MIKE-Systems wurden auf dem Kommunikationsserver *QUAKSBw (Querschnittlicher Anteil Kommunikationsserver Bundeswehr)* durchgeführt, der ein Bindeglied zwischen sprach- und datenbasierter Kommunikation sowie den Fernmeldemitteln der Bundeswehr darstellt.^{26,27} Schließlich wurde IDP/MIKE auch auf der Rüstungsmesse der AFCEA vorgestellt und als militärische Kommunikationslösung beworben. Der Weg kryptologischer Methoden und Forschungsansätze von einem externen Institut über die universitäre Forschungslandschaft in die deutsche Kriegsplanung ist im Fall des VPNs am FKIE daher einwandfrei nachvollziehbar und unmissverständlich kommuniziert.

Austausch auf kryptologischen Fachtagungen

Neben der direkten Beeinflussung akademischer Forschungsthemen durch Drittmittelkooperationen steht militärischen und geheimdienstlichen Akteur:innen auch der Besuch von internationalen Forschungskonferenzen offen. Gerade bei der Suche nach neuen Kooperationsmöglichkeiten bieten die akademischen Konferenzen einen umfassenden Einblick in die aktuell beforschten Themengebiete. Die Teilnehmenden der meisten Konferenzen sind verschiedenster Nationalitäten. Und so teilen die Forscher:innen, egal welcher Herkunft, ihr Wissen mit den Zuhörer:innen aus Militär und Rüstungsindustrie. Das nimmt auch Forscher:innen deutscher Universitäten nicht aus, die auf kryptologischen Konferenzen meist sehr zahlreich vertreten sind und Ergebnisse ihrer universitären Forschung direkt an Interessierte aus Militär und Rüstungsindustrie weitergeben.

Im Jahr 2009 wurde beispielsweise der NSA-Mitarbeiter J. F. Dillon vom Programmkomitee der *International Conference on Finite Fields and Their Applications* (z.Dt. *Internationale Konferenz zu endlichen Körpern und deren Anwendungen*) eingeladen, um über seinen Erkenntnisstand zur Existenz von *APN-Polynomen*²⁸ zu referieren.²⁹ Der Nutzen dieser Polynome besteht in der Kryptographie vor allem in ihrer Robustheit gegenüber kryptoanalytischen Angriffen (genauer: der Differenziellen Kryptoanalyse).^{30,31} Dillon stellte in seinem Vortrag die Akquise neuer Erkenntnisse mit einer abschließenden Frage an die Forschungsgemeinde über die Existenz von APN-Polynomen vor.³²

Die Sicherheit von Kryptosystemen gegenüber der Differenziellen Kryptoanalyse spielt für die NSA-Forscher:innen seit der Implementierung des *Data Encryption Standard (DES)* eine zent-

Thomas Gruber

Thomas Gruber ist Mathematiker und promoviert an der Universität Bremen zum Thema Verquickung mathematischer und informationstechnologischer Forschung an deutschen Forschungseinrichtungen mit der modernen Kriegsführung. Er ist Stipendiat der Rosa-Luxemburg-Stiftung und Mitglied der Informationsstelle Militarisation (IMI) in Tübingen.

rale Rolle. Schon im Jahr 1974 legte die NSA dem Unternehmen IBM nahe, den diesbezüglichen Entwicklungsstand unveröffentlicht zu lassen, was erst im Jahr 1994 bekannt wurde.³³ Die Nutzung des exklusiven Wissens über die Angreifbarkeit und Sicherheit von Kryptosystemen für die Kriegsführung ist leicht nachvollziehbar: Während die NSA selbst sichere Kryptostandards verwendet, können die neu entdeckten Angriffsschemata für eine Kryptoanalyse der feindlichen militärischen Kommunikation genutzt werden. Bis heute hat sich an dieser Praxis nur wenig geändert – zu groß ist anscheinend der kalkulierte Nutzen von Hintertüren in aktuellen Verschlüsselungsschemata für den Geheimdienst.

Beeinflussung der zivilen Forschungslandschaft durch militärische Interessenträger:innen

Die Beeinflussung der kryptologischen Forschung durch militärische Interessenträger:innen beschränkt sich allerdings nicht nur auf Verschwiegenheit bei neuen kryptologischen Forschungserkenntnissen. Sie umfasst auch die Distribution kompromittierter Kryptostandards, die es Angreifer:innen ermöglichen, die jeweilige Verschlüsselung zu brechen. In jüngster Vergangenheit waren dabei vornehmlich Public-Key-Systeme oder Methoden zum Schlüsselaustausch betroffen, die auf der Basis elliptischer Kurven arbeiten.

Ein prominentes Beispiel der geheimdienstlichen Beteiligung bei der Verbreitung eines unsicheren Kryptosystems ist der Pseudozufallsgenerator *Dual_EC_DRBG*.³⁴ Im Jahr 2013 wurde via eines von Edward Snowden geleakten Dokuments bekannt, dass eine Sicherheitslücke im *Dual_EC_DRBG* existiert, die der Sicherheitsfirma RSA von der NSA mit 10 Millionen Dollar bezahlt wurde.³⁵ Zufallszahlen sind essentieller Bestandteil vieler Kryptosysteme – so auch beispielsweise des Diffie-Hellman-Schlüsselaustauschs. Ein ausreichendes Zusatzwissen über die im Kryptosystem verwendeten Zufallszahlen würde es Angreifenden ermöglichen, das gesamte Verschlüsselungsverfahren offenzulegen.

Ungeachtet seiner Schwachstelle erfuhr der Pseudozufallsgenerator *Dual_EC_DRBG* weite Verbreitung in der kryptologischen Anwendung und der akademischen Forschung. Begründet liegt die Anerkennung solch fehlerhafter Standards vornehmlich in der Politik der US-Normierungsbehörde *NIST* (kurz für *National Institute of Standards and Technology*). Das *NIST* gibt Empfehlungen für die Normierung etablierter Kryptosysteme und beherzigt dabei geheimdienstlich und von Unternehmen entwickelte Implementierungen, wie die der NSA und des Sicherheitskonzerns RSA. Die *NIST*-Standards sind außerdem weitgehend alternativlos, die einzigen Ausnahmen bilden von Forscher:innen entwickelte, quelloffene Implementierungen, die als Antwort auf die Sicherheitslücken entstehen. Der Nutzen weit verteilter fehlerhafter Kryptosysteme für die moderne Kriegsführung ist also noch unmittelbarer als der einer bloßen Zurückhaltung von Informationen: Durch gut getarnte Hintertüren in den jeweiligen Implementierungen, die durch eine Veröffentlichung in *NIST*-Standards als sichere Verschlüsselungsschemata legitimiert werden, bleiben Abhöraktionen lange Zeit unbekannt. Die *NIST*-Kurven und -Algorithmen werden auch von feindlichen Akteur:innen genutzt und bieten damit eine willkommene, offene Flanke für kryptoanalytische Angriffe.

Fazit

Ob historisch oder in der aktuellen Forschung – die Kryptologie ist und war stets eine wichtige Informationsquelle staatlicher und militärischer Interessenträger:innen bezüglich der Kommunikationssicherheit und der Datenakquise. Neue Ergebnisse der kryptologischen Forschung wirken sich dabei oft stark auf taktische Neuerungen in geheimdienstlichen und militärischen Aktionen aus, wie auch die staatlichen und militärischen Akteur:innen erheblichen Einfluss auf die universitäre Forschung zur Kryptologie nehmen.

Bei der Analyse möglicher Militarisierungstendenzen innerhalb der kryptologischen Forschungslandschaft fällt auf, dass sich Entwicklungen im Forschungssektor oft nur schwer auf einzelne Staaten beschränken lassen. Das liegt zum einen an den selbstverständlichen internationalen Kooperationsbestrebungen von Forscher:innen, zum anderen am transnationalen Agieren von Geheimdiensten, staatlichen Institutionen und Konzernen. Auch ist es oft nicht mehr möglich, militärische Interessen von staatlichen oder wirtschaftlichen zu trennen – zu nah liegen die (geo-)politischen Ziele der jeweiligen Akteur:innen meist beisammen. Staatlich legitimierte (und oft mit der Wahrung von Menschenrechten begründete) Kriege dienen häufig wirtschaftlichen Interessen wie der Absatzmarkterschließung. (Das bestätigten auf Seiten der deutschen Politik auch der ehemalige Bundespräsident Horst Köhler und der ehemalige Verteidigungsminister Guttenberg.^{36,37})

Für ein Fazit über die Militarisierung der kryptologischen Forschungslandschaft an deutschen Universitäten muss ob der Intransparenz der geheimdienstlichen und staatlichen Kooperationsprojekte differenziert werden. Einerseits besteht ein starker Informationsfluss aus der universitären Forschung in militärische Anliegen; die Universitäten und Forscher:innen erhalten im Gegenzug Geld, Stiftungsprofessuren, genießen ein gesteigertes Renommee in militärischen Kreisen oder nutzen Kooperationsmöglichkeiten zum Aufbau von Netzwerken. Eine äußerst restriktive Veröffentlichungspolitik bis hin zur Erwirkung von Geheimhaltungsklauseln für die Forschenden verhindert allerdings meist den Rückfluss der Ergebnisse in die akademische Forschung. Andererseits beinhalten die staatlichen Veröffentlichungen zu neuen Kryptostandards oft zusätzlich fehlerhafte, fehleranfällige oder mit Hintertüren versehene Komponenten, die wiederum nach und nach von universitären Forscher:innen und deren Kollektiven oder Whistleblower:innen aufgedeckt werden müssen. Ein parasitär anmutender Informationsfluss von Seiten der Geheimdienste und die willentliche oder zumindest in Kauf genommene Sabotage universitärer Kryptologie für Geldmittel und infrastrukturelle oder personelle Verbesserungen prägen also die Form der Militarisierung der Kryptologie.

Diese höchst bedenklichen Militarisierungstendenzen stehen allerdings jedweder wissenschaftlichen Intention einerseits und der Idee der gesamten Kryptologie andererseits krass entgegen. Wissenschaftliche Arbeit lebt von Transparenz und einer öffentlichen Diskussion von Forschungsergebnissen. Sollte außerdem die absichtliche Verbreitung fehlerhafter Kryptosysteme weiter um sich greifen, muss die Legitimation der gesamten institutionalisierten Forschung eines Bereiches, der sich mit einer verlässlich sicheren und vertraulichen Kommunikation befasst, infrage gestellt werden.

Sowohl gesamtgesellschaftlich als auch wissenschaftlich wäre also ein grundlegendes Interesse begründet, der Militarisierung der kryptologischen Forschung entgegenzuwirken. Dieser Position entgegen stehen die Geldgeber:innen für militärrelevante Forschung, staatliche Tendenzen zur Liberalisierung des Bildungssektors und in diesem Zuge meist auch die einzelnen Universitätsleitungen. Zivil- und Transparenzklauseln – also die Selbstverpflichtung einer Institution, nur für friedliche Zwecke zu forschen und die aktuellen Drittmittelkooperationen zu veröffentlichen – in den Grundordnungen einzelner deutscher Universitäten stellen eine erste politisch erkämpfte Antwort auf die Militarisierung der Forschung dar. Gerade im Bereich der Kryptologie als stark transnational agierende Wissenschaft mit einem gewissen US-Zentrismus kann aber eine Zivilklausel oft nur Drittmittelprojekte an den jeweiligen Institutionen verhindern. Diese Einschränkung betrifft also nur einen kleinen Teil der militärrelevanten Forschung zur Kryptologie. Jede weitere Form des Widerstands bedarf daher einer kritischen Öffentlichkeit, sowohl einer gesamtgesellschaftlichen – ausgedrückt im politischen Kampf – als auch einer wissenschaftlichen. Die Frage nach Verantwortung stellt sich also nicht nur an die politische Öffentlichkeit, sondern auch an die direkt involvierten Forscher:innen, die als Fachkundige am besten Forschungsoperationen auf den gesellschaftlichen Nutzen und die Verträglichkeit prüfen können. Fern von monetären Interessen gälte es innerhalb der kryptologischen Forschungsgemeinschaft das Vertrauen gegenüber Akteur:innen aus dem Militär-, dem Staats- und dem Wirtschaftssektor in Frage zu stellen.

Anmerkungen

- 1 Übersetzung des Autors aus dem Englischen.
- 2 Die Möglichkeiten zur Wahl eines Verschlüsselungsverfahrens und des Austausches eines Schlüssels sind so unterschiedlich wie zahlreich – im Verlauf des Artikels werden entsprechende Grundlagen umrissen.
- 3 Jordan, Craig: *Secret History: The Story of Cryptology*. Chapman & Hall/CRC, 2013. S. 4–5
- 4 ebd., S. 11–12
- 5 Kahn, David: *The Codebreakers: The Story of Secret Writing*. Simon & Schuster, 1996. S. 217–218
- 6 Jordan, Craig: *Secret History: The Story of Cryptology*. S. 185–187
- 7 ebd., S. 293–311
- 8 ebd., S. 342–367
- 9 United States SIGINT System, January 2007 Strategic Mission List, <http://cryptome.org/2013/11/nsa-sigint-strategic-mission-2007.pdf>, 29.02.2016.
- 10 Kleine Anfrage: Militärische und sicherheitstechnische Forschung in Sachsen seit 2009, http://edas.landtag.sachsen.de/viewer.aspx?dok_nr=12635&dok_art=Drs&leg_per=5&pos_dok=-1, 01.03.2016. S. 6
- 11 Adrian, David, et al.: *Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice*. 22nd ACM Conference on Computer and Communications Security, 2015
- 12 Wobei bei der Nutzung von elliptischen Kurven ebenso auf eine fehlerfreie Implementierung zu achten ist, wie die oben stehenden Ergebnisse zeigen.
- 13 Stinson, Douglas R.: *Cryptography: Theory and Practice*, Third Edition. Chapman & Hall/CRC, 2006. S. 254–267
- 14 Remote Timing Attacks are Still Practical, <http://eprint.iacr.org/2011/232.pdf>, 02.03.2016.
- 15 Beide Bonner Hochschulen besitzen eine seit 2015 in der jeweiligen Grundordnung verankerte Zivilklausel.
- 16 Fraunhofer FKIE: *Institutsleitung*, <http://www.fkie.fraunhofer.de/de/ueber-uns/institutsleitung.html>, 02.03.2016.
- 17 Fraunhofer FKIE: *Forschungsbereiche*, <http://www.fkie.fraunhofer.de/de/forschungsbereiche.html>, 02.03.2016.
- 18 Universität Bonn: *Institute of Computer Science 4*, <https://net.cs.uni-bonn.de/start/>, 02.03.2016.
- 19 AFCEA Fachausstellung 2015, https://www.afcea.de/29_fa-131.html, 02.03.2016.
- 20 FKIE auf der AFCEA Fachausstellung 2015, [https://www.afcea.de/1400.html?tx_mhbranchenbuch_pi1\[detail\]=29&cHash=6f0eb2587cd75b505dff8d2363a26a97](https://www.afcea.de/1400.html?tx_mhbranchenbuch_pi1[detail]=29&cHash=6f0eb2587cd75b505dff8d2363a26a97), 02.03.2016.
- 21 IDP / MIKE – Sicherheit zwischen Kommunikationspartnern, <http://www.fkie.fraunhofer.de/de/forschungsbereiche/cyber-analysis-and-defense/projekt-idp-mike.html>, 02.03.2016.
- 22 Christof Fox: *Konzeption eines SOA-konformen Discovery Mechanismus zur Verbesserung der Fehlertoleranz eines Gruppenschlüssel-managements*, http://www.leischner.inf.fh-bonn-rhein-sieg.de/aa/thesis/08_Fox_MIKE-IDP.htm, 10.2.2016.
- 23 Shirish Negi: *Evaluation and Optimization of the Group Key Management IDP-MIKE over VHF Data Links*, <https://net.cs.uni-bonn.de/de/nc/aktuelles/newsansicht/708/e8d00ec903a483e2f6d361bfa-9b8438e/>, 02.03.2016.
- 24 Anastasia Danilova: *Bewertung des IDP-MIKE-Systems in Bezug auf Replay- und DoS-Angriffe*, <http://net.cs.uni-bonn.de/nc/news/singleview/584/2ccfc86b9375cec3546458bceb644c07/>, 02.03.2016.
- 25 <http://www.fkie.fraunhofer.de/de/forschungsbereiche/cyber-analysis-and-defense/projekt-idp-mike.html>, 02.03.2016.
- 26 http://www.leischner.inf.fh-bonn-rhein-sieg.de/aa/thesis/08_Fox_MIKE-IDP.htm, 10.2.2016.
- 27 Oberst Warnicke: *Das Kommunikationssystem der Bundeswehr für den Einsatz (KommSysBwEins)*, https://www.afcea.de/fileadmin/downloads/Fachausstellung/23_Fachausstellung_2009/Anmeldung/2-20101214_KommSysBwEins-VortragAFCEA_SKUKdo-mit.pdf, 02.03.2016.
- 28 Almost Perfect Nonlinear Polynomial
- 29 Abstracts of the 9th International Conference on Finite Fields and their Applications, <http://claudeshannoninstitute.ucd.ie/fq9/AIFq9Abstracts.pdf>, 29.02.2016.
- 30 Wikipedia: *S-Box*, <https://de.wikipedia.org/wiki/S-Box>, 02.03.2016.
- 31 Highly resistant Boolean functions for cryptography, <http://iml.univ-mrs.fr/~ritzenth/AGCT/talks/rodier.pdf>, 02.03.2016.
- 32 APN Polynomials: An Update, <http://mathsci.ucd.ie/~gmg/Fq9Talks/Dillon.pdf>, 02.03.2016.
- 33 Coppersmith, Don: *The Data Encryption Standard (DES) and its strength against attacks*. IBM Journal of Research and Development, 1994, 38. S. 243–250
- 34 Exclusive: Secret contract tied NSA and security industry pioneer, <http://www.reuters.com/article/us-usa-security-rsa-idUSBRE9B-J1C220131221>, 29.02.2016.
- 35 Hintertüren und Schwächen im kryptographischen Standard SP 800-90A, <https://www.mathematik.de/ger/presse/ausdenmitteilungen/artikel/dmvm-2014-0012.pdf>, 29.02.2016.
- 36 Köhler: Krieg für freien Handel, <http://www.sueddeutsche.de/politik/bundeswehreinsatze-koehler-wirtschaftsinteressen-militaerisch-durchsetzen-1.950594>, 02.03.2016.
- 37 Guttenberg auf Köhlers Spuren, <http://www.taz.de/!5132558/>, 02.03.2016.



Selbstbestimmt war gestern?

Wenn wir das Entscheiden Maschinen überlassen

Freemee, ein Hype – vor allem bei den U20. Facebook war die Blaupause für Freemee. Nur kann Freemee viel mehr. Freemee bietet Lebenshilfe. Freemee verspricht Erfolg – bessere Schulnoten, Anerkennung, Rat in allen Lebenslagen. „Du solltest heute Abend lieber noch etwas Mathe für die Klausur morgen üben, statt zu chillen“, „du solltest mal einen cooleren Haarschnitt versuchen – der käme bei Henry sicher gut an“, „du solltest mal wieder regelmäßiger joggen – du bist in letzter Zeit ziemlich kurzatmig“ – mit seinen Textmeldungen auf deinem Smartphone verfolgt dich Freemee auf Schritt und Tritt und verspricht dir ein besseres Leben, wenn du seinen Ratschlägen folgst. Wenn du Freemee teilhaben lässt an deinem Leben, an deinen Kontakten, an deinen Wegen, an deiner Umgebung, an deinen Biodaten, an deinen Gefühlen ...

Prolog

Freemee – „befreie mich“ – ist eine Schöpfung aus der Feder Marc Elsbergs. Wie schon in *Blackout* setzt Elsberg in seinem neuen Roman *ZERO – Sie wissen, was du tust* Technik in Szene, die zum Alltag in unserer digitalen Gesellschaft gehört.¹ Er gestaltet sie mit nur ein wenig Phantasie aus und greift damit nur ein wenig in eine Zukunft, die keineswegs mehr das Attribut *Science-Fiction* verdient. Und er konstruiert auf dieser Basis einen Thriller.

Eigentlich wollte ich eine Rezension über *ZERO* schreiben. Und im Grunde ist sie damit auch schon geschrieben, denn viel mehr sollte der Rezensent über einen Thriller auch nicht verraten, als dass er ihn mit hoher Spannung verschlungen hat. Aber dann wurde doch mehr daraus: Der Stoff weckt Vorstellungen, vor allem dystopische. Elsbergs Geschichte ist nicht nur hoch spannend. Sie vermittelt auch so ganz nebenher – anschaulich vereinfachend –, wie Big-Data-Technologien Daten über persönliches Verhalten, selbst über intimste Details, aggregieren und daraus mit ihren Analyse- und Lern-Algorithmen Ratschläge für den Alltag ableiten. Und wie diese Ratschläge dank des umfassenden maschinellen Wissens über unser Leben so plausibel in den Kontext unseres Handelns und Wollens passen, dass wir uns unversehens von ihnen leiten lassen. Wir erfahren auch, dass an den Stellschrauben der Algorithmen gedreht werden kann, und wie uns die produzierten Ratschläge und Entscheidungshilfen damit sanft und unbemerkt in eine beabsichtigte Richtung drängen können.

Mit einem Mal wird deutlich, in wie vielen alltäglichen Situationen wir uns bereits auf maschinelle Ratschläge stützen, uns von Maschinen sogar folgenreiche Entscheidungen abnehmen lassen. Wie ein Sog zieht uns das wachsende Angebot an Alltagshilfen unmerklich in eine Abhängigkeit hinein. Hinterfragen wir ihre Vertrauenswürdigkeit und Neutralität? Können wir uns vor dem Manipuliertwerden schützen?

Ist die Anfrage nicht gerade sehr speziell formuliert, spuckt die Suchmaschine im Allgemeinen viele Tausend Treffer aus. Wir schauen üblicherweise kaum mehr als eine Handvoll auf der ersten Seite an, im Verlass darauf, dass die Maschine weiß, welche Treffer für uns am relevantesten sind. Nachrichtenextrakte, Kaufentscheidungen, Hotelauswahl, Reisebuchung, Partnersuche – wir stehen nicht mehr verwirrt vor endlosen Alternativen – die Maschine hat schon eine Auswahl besorgt, die auf unsere Bedürfnisse und Wünsche bestens abgestimmt zu sein scheint.

Wir stehen nicht mehr orientierungslos an Straßenkreuzungen und versuchen uns auf Stadtplänen oder Landkarten zurechtzufinden. Das Geoinformationssystem schlägt uns die *beste* Route vor. Oder noch einfacher: Wir folgen den Pfeilen auf unserem Navigationsdisplay. Und schon spekulieren wir auf die nächste Errungenschaft für den Individualverkehr, das autonome Auto. Es wird nicht nur den Weg finden, es wird uns auch die Fahrtsscheidungen abnehmen, rechtzeitig bremsen vor dem Stauende, Hindernissen ausweichen, Verkehrsregelungen beachten. Wir werden nicht mehr vor unserem leeren Kühlschrank stehen und nachdenken müssen, was einzukaufen ist: Der Lieferant steht schon vor der Tür, wusste bereits Bescheid, was uns ausgegangen war, und hat die zu uns passenden Produkte ausgewählt.

Wir wissen auch unsere Gesundheitsvorsorge in guten Händen: Das Sensorarmband misst unsere Vitalparameter. Wir liefern Blutwerte, Stresslevel, Herzrhythmus und viele andere Körperdaten und erhalten dafür Ratschläge, wie wir gesünder leben können. Diabetiker lassen sich an die Justierung ihres Blutzuckerspiegels erinnern. Schlaganfallpatienten werden vor einer neuen Attacke gewarnt. Zu Sport, Bewegung und Körpertraining lassen wir uns durch Tabellen und Statistiken motivieren – Lust und Spaß waren ziemlich unzuverlässige Anreize. Und wie befinden wir uns gerade? Schluss mit dem subjektiven *Körpergefühl* – jetzt haben wir unsere Körperdaten. Demnächst machen wir morgens ein Selfie und erfahren, ob wir zufrieden oder gestresst sind.

Die hilfreichen Ratgeber

Fachbücher, Nachschlagewerke, Lexika sind schon lange nicht mehr unsere erste Quelle für Sachinformationen. Brauchen wir eine schnelle Auskunft oder möchten wir uns umfassender über Sachverhalte und Geschehnisse informieren, ist unser erster Schritt die Anfrage bei einer Suchmaschine, bevorzugt Google.

Wer die Wahl hat, hat die Qual

Wann ist eine Entscheidung eine wirkliche Entscheidung? Eigentlich erst, wenn ich vor einer Situation stehe, in der ich keinen Anhaltspunkt mehr habe, welche Wahl die *richtige* ist, welche Folgen meine Wahl haben wird. Das ist unbequem, verunsichert, nötigt zu einer Auseinandersetzung mit dem Unbekannten. Das

ist besonders unbequem, wenn ich für die Folgen Verantwortung übernehmen muss. So ist es nur zu verständlich, dass wir uns nicht nur in unserem privaten Leben Entscheidungshilfen anvertrauen, sondern gerade auch in der Ausübung unserer Berufe. Musste vormals der Kredit-Sachbearbeiter seinem persönlichen Wissen über den kreditsuchenden Kunden vertrauen, seiner Menschenkenntnis und am Ende seinem *Bauchgefühl*, wird er heute keine Kreditvergabe mehr verantworten wollen, ohne das Schufa-Ranking des Kunden abzufragen. Der Versicherungsagent wird sich die von der Versicherung zu tragenden Risiken vor dem Abschluss einer Police personenbezogen errechnen lassen. Ärzte lassen sich von Expertensystemen Diagnosevorschläge machen und Therapie-Empfehlungen geben. Banker kaufen und verkaufen Wertpapiere auf Grund von Prognoserechnungen. Oder sie überlassen den Börsenhandel sogar vollends dem Computer, der die Geschäfte in Millisekunden abwickelt.

Es interessiert dabei kaum, dass die Entscheidungskriterien, die den maschinellen Entscheidungen zugrunde liegen, rational meist nicht mehr nachvollziehbar sind. Wenn der Bestand an Daten nur genügend groß ist, greifen algorithmische Verfahren, die ihre Entscheidungsregeln aus dem Datenmaterial selbst – und selbsttätig – herleiten: *Big Data* und *Deep Learning*, das Yin und das Yang der maschinellen Entscheidung. Die Repräsentativität der zugrunde liegenden riesigen Datenmengen macht die Wahrscheinlichkeit hoch, dass die Maschine eine Entscheidung *richtig* fällt, dass sie dem Arzt die zum Krankheitsbild des Patienten bestpassende Diagnose liefert, dass sie dem Banker die bezüglich der Kreditwürdigkeit des Kunden zuverlässigste Prognose abgibt. Statistisch gesehen. Und unter der Voraussetzung, dass die dem Lernprozess zugrunde liegenden Daten auch für den ganz individuellen Einzelfall repräsentativ sind.

Wem das Schicksal des *Outliers* nicht wichtig ist, wer gelegentliche Fehltreffer tolerieren kann, der wird die maschinellen Ratgeber gerne für seinen Job nutzen – wenn sie ihm nur einen strategischen Vorteil versprechen. Er wird sie vielleicht sogar nutzen *müssen*, um sich nicht zu disqualifizieren. So zum Beispiel im Polizeidienst: Am Anfang stand die Rasterfahndung, heute mit einer fast lückenlosen Ausspähung optimiert zum Konzept des *Predictive Policing* – Straftaten vorhersagen aus Bewegungsdaten, Kontakten, Verhaltensmustern, persönlichen Daten beobachteter Personen. Die Geheimdienste haben uns solches Vorgehen vorexerziert und perfektioniert. Und immer ist es einfacher, den Fehlgriff – Unschuldige fallen einem *Signature Strike* zum Opfer, die Rakete trifft ein Krankenhaus – einer technischen Unzulänglichkeit zuzuschreiben, als persönlich Verantwortung dafür zu übernehmen. Im militärischen Umfeld ist es daher nur konsequent, wenn auch strategische Entscheidungen zunehmend von hoch automatisierten C3I-Systemen geleitet und tak-

tische Entscheidungen in absehbarer Zukunft vollends autonomen Waffensystemen übertragen werden.

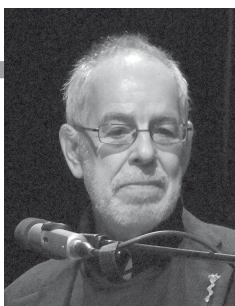
Selbstbestimmtheit – leichtfertig aufgegeben?

Es lebt sich leichter, wenn ich nicht beständig vor Entscheidungen stehe. Die Fußgängerampel lässt mich die vielbefahrene Straße – relativ – sicher überqueren. Auf die Grünphase warten zu müssen, ist störend, aber ein geringer Preis für die Sicherheit. Als meine Kinder alt genug waren, um dieses Konzept verinnerlicht zu haben, erfuhren sie von mir zu ihrer Überraschung, dass man durchaus auch bei Rot queren kann – wenn die Straße leer ist. Und wenn man bereit ist, die Verantwortung für sich selber zu übernehmen – das heißt: Augen aufmachen, Situation beurteilen, Risiko abschätzen. Ich wollte, dass sie selbstbestimmte Menschen werden. Sie mussten akzeptieren, dass selbstbestimmt zu leben unbequem ist, sogar riskant sein kann, mit Unsicherheiten umzugehen erfordert. Aber dass es auch einen Lohn einbringt! Der ist allerdings nicht ohne Weiteres offensichtlich, sodass wir leicht vergessen wertzuschätzen, wie es unser Leben bereichert, selbstbestimmt handeln zu dürfen.

Dennoch, es lebt sich leichter, wenn man Unsicherheitsgefühlen und Verantwortungsdruck ausweichen kann. Das Angebot an Entscheidungshelfern ist vielfältig und immer und überall verfügbar. Produktempfehlungen, Restaurantvorschläge, Nachrichtenauswahl sind so subtil auf unsere persönliche Situation abgestimmt, passen so plausibel zu unserem persönlichen Lebensstil, dass wir es für unsere eigenen Entscheidungen halten, wenn wir ihnen folgen. Wir müssen uns nicht mehr auf trügerische Gefühle verlassen – unser Körpergefühl, wenn es um die Einschätzung unseres Gesundheitszustandes geht, unser Bauchgefühl, wenn es um die Vertrauenswürdigkeit im Geschäftsverkehr geht –, stehen uns doch scheinbar kompetente Instanzen mit rationalen Analysen zur Seite.

Gewiss, es gibt ernsthafte Bedenken dagegen, sich kritiklos auf die Nutzung all dieser Dienste einzulassen. Wir kennen die Spielregeln nicht, wissen wenig oder nichts über die Intentionen der Dienstleister. Wir kennen nicht die Filterkriterien, wir können die Neutralität der statistischen Analysen nicht nachprüfen, Algorithmen und Zusammensetzung der Datenkörper werden uns nicht offengelegt. Die Währung, mit der wir für die Dienstleistung zahlen, sind unsere persönlichen Daten, umso wertvoller, je intimer die Details über unser Privatleben sind, die aus ihnen entschlüsselt werden können. Wir sagen uns, dass wir kritisch damit umgehen, uns der Risiken und Kosten bewusst sind, uns beschränken – wiewohl die Versuchung stark ist, im Alltag alle Bedenken hintanzustellen. Wir fragen uns nicht, was das

Dietrich Meyer-Ebrecht



Dietrich Meyer-Ebrecht ist stellvertretender Vorsitzender des FfF. Er war bis 2004 Inhaber des Lehrstuhls für Bildverarbeitung der RWTH Aachen.

fortschreitende Ablegen unserer Bereitschaft zu eigenständigen Entscheidungen mit *uns* macht. Vielleicht sollten wir das?

Wenn ich mir diese Frage stelle, merke ich, dass ich Gefahr laufe, meine Neugier zu verlieren, meine Lust zur Entdeckung von Unbekanntem, den Nervenkitzel vor dem Unerwarteten. Oder ist dieser Prozess gar unmerklich schon weit fortgeschritten? Vermisse ich schon die Erfolgserlebnisse durchgestandener Entscheidungsqualen, diese wohltuende Bestätigung des Egos als ein autonomes Wesen? Hat mich nicht das Bewusstsein, Entscheidungen, große wie kleine, eigenständig richtig getroffen zu haben und die Konsequenzen falsch getroffener Entscheidungen ausgestanden zu haben, stark gemacht für das Unberechenbare vor mir?

Das Persönliche sollte hier nicht von Belang sein, wohl aber sollten wir auf allgemeine Entwicklungen schließen. Autonome Entscheidungen machen komplexe mentale Prozesse erforderlich. Selbst einfachen Handlungsentscheidungen liegt eine Wechselwirkung zwischen weit verteilten Hirnregionen zugrunde. Das Gehirn berücksichtigt dabei die Art des Stimulus, gleicht diesen mit dem Kontext ab, ruft Wissen ab, tauscht Informationen aus und leitet schließlich die passende Reaktion ein, die uns dann ganz selbstverständlich erscheint.² Die Komplexität dieser Prozesse lässt sich auch daraus ablesen, dass die Psychologie der Entscheidung mittlerweile ein eigenständiges aktuelles Forschungsgebiet ist. Es wäre nun verwunderlich, wenn uns die Fähigkeit zu einem derart komplexen mentalen Prozess *ab ovo* gegeben wäre. Sie wird vermutlich, ähnlich der Befähigung zu kognitiven Prozessen, erlernt: *Learning by Doing* – Entscheidungsprozesse werden trainiert, an alltäglichen Situationen und in dem Maße, in dem wir ein selbstbestimmtes Ego entwickeln, an folgenreicheren Aufgaben. Mit dieser Entwicklung einhergehen auch die Ausbildung des Selbstvertrauens und die Fähigkeit zur Selbstkontrolle.

Einmal erlernt, hält fürs Leben? Das müsste noch bewiesen werden. Vielleicht geht es wie mit dem Treppensteigen: Wir können es noch, aber wenn uns ein Fahrstuhl geboten wird, nehmen wir die Treppe nur widerwillig. Werden wir, je mehr Entscheidungen wir uns abnehmen lassen, entscheidungsträge? Wenn eine Handlung belohnt wird, hier mit der Bequemlichkeit, dass wir die Mühe für eine eigenständige Entscheidung und ihre Risiken vermeiden, wird dies unser Handeln reflexhaft verstärken. Wo immer sich neue Angebote eröffnen, werden wir sie nutzen. Wir verlieren dabei die Wertschätzung für ein hohes Gut, das uns gegeben ist, die Freiheit des selbstbestimmten Handelns. Wird Menschen die Möglichkeit zum selbstbestimmten Handeln genommen, wird ihnen ihre Würde genommen. Lassen wir uns darauf ein, dass wir uns in unseren Entscheidungen in immer umfassenderem Maße von Dritten leiten und lenken lassen, geben wir einen Teil unserer Würde ab, aus freien Stücken.

Über die Aushöhlung der Demokratie von innen

Dies, so könnte man nun sagen, läge in der Verantwortung jedes Einzelnen. Nur müssen wir befürchten, dass dieses Verhaltensmuster zu einem gesellschaftlichen Trend wird. Gehen wir von der Hypothese aus, dass eigenständiges Entscheiden trainiert wird – *Learning by Doing* –, muss uns nachdenklich machen, dass die jetzt heranwachsende Generation – die „Generation S“, wie *Smartphone* – bereits in einem Alter, in dem Grundfertigkeit-

ten am effizientesten erlernt werden, nicht mehr gefordert ist, eigenständiges Entscheiden in komplexeren Kontexten zu trainieren. Denn schon ist es auch für die Heranwachsenden zur Routine geworden, die Vielzahl der Hilfen zu nutzen, wo immer eine Entscheidungsfindung nötig wird.

Menschen bestärken sich gegenseitig in Verhaltensmustern, wenn diese nicht nur die Besonderheit Einzelner sind, sondern zur Gruppennorm werden: Mach ich's wie die anderen, minimiere ich das Risiko einer Fehlentscheidung. Über die gesellschaftlichen Folgen einer solchen Entwicklung kann man heute nur spekulieren. Wird es zur gesellschaftlichen Norm werden, dass selbstbestimmtes Handeln nicht mehr ein selbstverständlich in Anspruch genommenes Gut ist, dass es keine Wertschätzung mehr erfährt (so wie bereits „Privatsphäre war gestern“ postuliert wurde)? Wird mit dem Bedürfnis zur eigenverantwortlichen Gestaltung unseres eigenen Lebens auch die Bereitschaft zur gestalterischen Teilhabe am öffentlichen Leben schwinden? Das wäre fatal: Es würde das Fundament unseres demokratischen Gesellschaftssystems aufweichen.

„Das Recht auf individuelle Selbstentfaltung kann nur wahrnehmen, wer die Kontrolle über sein Leben hat. Dies setzt jedoch informationelle Selbstbestimmung voraus. Es geht hier um nicht weniger als unsere wichtigsten verfassungsmäßig garantierten Rechte. Ohne deren Einhaltung kann eine Demokratie nicht funktionieren. Ihre Einschränkung unterminiert unsere Verfassung, unsere Gesellschaft und den Staat.“ Mit diesem Kernsatz artikulieren neun Wissenschaftler:innen in ihrem jüngst veröffentlichten *Digital Manifest* ihre Sorge um eine Aushöhlung der Demokratie.^{3,4} Das *Manifest* brandmarkt den Missbrauch der Macht, die die Wirtschaft durch unsere fortschreitende Abhängigkeit von ihren digitalen Dienstleistungen über uns gewonnen hat. Über die immer umfangreichere Aggregation der Informationen über unser privates Leben – ganz in diesem Sinne wird derzeit für die Abschaffung des Bargeldes geworben – können wir von der Wirtschaft und von einer von wirtschaftlichen Interessen geleiteten Politik im Verband mit der Medienindustrie immer subtiler manipuliert werden. Wir laufen Gefahr, dass damit die demokratischen Mechanismen der gesellschaftlichen Willensbildung ausgehebelt werden.

Gewinnstreben in der Wirtschaft, Machtstreben in der Politik als treibende Kräfte dieses Prozesses – diesen Faktoren die alleinige Verantwortung zuzuschreiben, wäre jedoch zu einfach. Wir sind es, die sich manipulieren lassen, wenn wir unsere Fähigkeiten zum selbstbestimmten Handeln verkümmern lassen, wenn wir nicht mehr die Mühe aufbringen wollen, durch eigene Recherche der Vereinnahmung durch die gefilterten und auf uns zugeschnittenen Dienstleistungs- und Informationsangebote zu widerstehen. Es bedarf keines gewaltsamen politischen Aktes, allein unser mangelndes Interesse wird unsere Demokratie aushöhlen und zu einer Oligarchie werden lassen, in der wir als interesse- und willenlose Rädchen mitlaufen.

Eigens beklemmende Vision

1973 schreibt der Biologe Manfred Eigen in seinem Nachwort zu Ingo Rechenbergs „Evolutionstrategie“:⁵ „Wird der Mensch in einer unbegrenzten technischen Evolution das Steuer in der

Hand behalten können? Oder wird er einmal zur mehr oder weniger bedeutungslosen Zelle eines gigantischen sich selbst fort-pflanzenden und ständig optimierenden Automaten absinken?“ Für einen Evolutionsbiologen ist dies eine folgerichtige Option. Einzeller vergesellschaften sich, der Überlebensvorteil ist die treibende Kraft. Die Vorteile einer Aufgabenverteilung führen zu einer fortschreitenden Ausdifferenzierung der Zellen, zu ihrer Festlegung in einer organisierten Struktur – dem Organismus – und zu ihrer totalen Abhängigkeit vom Funktionieren des Organismus. Das Selektionskriterium ist nun nicht mehr, „was nützt der Zelle“, sondern „was nützt dem Organismus“.

Dies zu übertragen auf die Evolution des Menschen und seiner Gesellschaft ist eine beklemmende Vorstellung, aus der Sicht der damaligen Technik allenfalls vorstellbar als die Einschließung der Menschen in ihre Wohnzellen, in denen sie über Rohrleitungen und Transportsysteme mit allem für Leben und Arbeiten Notwendigen versorgt werden. Das Beruhigende an solchen dystopischen Science-Fiction-Visionen ist, dass sie, extrapoliert aus der jeweils zeitgenössischen Technikszenarie, nicht gut real vorstellbar sind und deshalb gern ins Absurde abgewiesen werden. Im Rückblick allerdings erfahren wir nicht selten, wie erschreckend vorausschauend die Visionen waren.

Die Eigensche Vision müssen wir heute nicht mehr physisch interpretieren. In dem Maße, in dem wir uns, immer und überall vernetzt, einspinnen lassen in einen Datenkokon, selber aktiv daran mitwirkend, werden wir zum Teil eines Metasystems. Wir bewegen uns ungehindert, fühlen uns frei und sind doch in unseren Handlungsentscheidungen gesteuert. Die Fremdsteuerung entzieht sich unserer Wahrnehmung durch ihr subtiles Zusammenwirken auf allen Ebenen des Alltags. Den Anfang haben wir gemacht, indem wir uns daran gewöhnt haben, uns dort nicht mehr selbst zu entscheiden, wo uns Entscheidungen angeboten werden.

Wer nun denkt, ich bin frei, ich habe meinen freien Willen, ich muss mich nicht darauf einlassen mitzuspielen, ich bewahre mir meine Selbstbestimmtheit – auch für den hält die Evolutionsgeschichte eine Analogie bereit: all die Spezies, die sich nicht auf den Evolutionspfad zu komplexeren Organismen begeben haben, die weiterhin ihr zelluläres Einzelleben führen. Nun ja, sie werden vom Immunsystem dieser Organismen unnachsichtig verfolgt, sobald sie versuchen, von ihm zu profitieren. Andere, wie zum Beispiel Darmbakterien, haben sich schon von ihnen einverleiben lassen, als willige Arbeitssklaven.

Epilog

Analogien sind immer mit Vorsicht zu verwenden. Unsere digitale Technikwelt ist nicht das Ergebnis einer Evolution im biologischen Sinn, deren Ziel einzig und allein die Verbesserung der Überlebenschancen der Arten ist. Zwar wirkt auch hier im Ansatz das Grundprinzip der Evolution – Mutation und Selektion. Jedoch ist die Technikwelt von Menschen ersonnen worden, sie gehorcht von Menschen entworfenen Gesetzen, sie wird von Menschen gelenkt. Machteliten – Menschen! – bestimmen die Entwicklungsziele. Machteliten, politische und wirtschaftliche, bestimmen Einsatz und Anwendung mit dem Ziel ihrer Machterhaltung und Maximierung der Gewinne.

All die wunderbaren Alltagshelfer dienen diesen Zielen. Die Gefahr der Algorithmen, die uns Entscheidungen abnehmen, ist nicht nur, dass wir uns von ihnen in einen Mainstream saugen lassen. Dieser Mainstream ist nicht dem Ziel verschrieben, dass möglichst alle Menschen gleichermaßen profitieren. Dass Algorithmen *per se* „fair“ sind, ist eine Illusion.⁶ Wir erfahren nicht, welcher Bias eingebaut ist, um die Richtung, die der Mainstream nimmt, zu beeinflussen. So werden die gepriesenen Gesetze des Marktes außer Kraft gesetzt – nicht mehr der Kunde ist der König –, und die politische Willensbildung wird den Bürgern unbemerkt aus der Hand genommen. Ein kleiner Bias, ein sanfter Druck in die gewünschte Richtung ist alles, was dazu nötig ist, wenn wir uns einmal umgarnen lassen haben: *Big Nudging*, sanftes und konzertiertes Anstupsen in allen Lebenslagen.⁷

Für Machterhalt und Gewinnmaximierung der Machteliten – beides nur denkbar unter einer fortschreitenden Aufspreizung der Schere in unserer Gesellschaft – sind demokratische Mechanismen hinderlich. Indem sich die digitale Gesellschaft diesen Kräften ohne zu hinterfragen ausliefert, wird sie zum willigen Helfer bei der Aushöhlung der Demokratie.

Wir sind die erste Generation, die dies bereits im Ansatz erlebt, und womöglich die letzte, die die Richtung dieses Trends noch beeinflussen könnte.

Für Hinrich Jansen Dittmer, der mich auf meinem beruflichen Weg in einer entscheidenden Phase begleitete, der mich die Achtung lehrte vor den Wirkungen der Technik auf Menschen und Gesellschaft, der die Schwierigkeiten eines interdisziplinären Arbeitens mit mir durchlebte, der viel zu diesem Text zu sagen gehabt hätte, aber nun viel zu früh starb.

Anmerkungen

- 1 Elsberg, Marc (2014): *ZERO. Sie wissen, was du tust*. München: Blanvalet
- 2 Siegel, Markus; Buschman, Timothy J.; Miller, Earl K. (2015): *Cortical information flow during flexible sensorimotor decisions*. In: *Science*, 348:6241, 1352–1355
- 3 Helbing, Dirk; Frey, Bruno S.; Gigerenzer, Gerd; Hafen, Ernst; Hagner, Michael; Hofstetter, Yvonne; van den Hoven, Jeroen; Zicari, Roberto V.; Zwitter, Andrej (2016): *Digitale Demokratie statt Datendiktatur*. In: *Spektrum der Wissenschaft*, Januar 2016, S. 50–58; vgl. auch <http://spektrum.de/news/wie-algorithmen-und-big-data-unsere-zukunft-bestimmen/1375933>
- 4 Meyer-Ebrecht, Dietrich (2015): *Das Digital Manifest. Neun Wissenschaftler.innen artikulieren ihre Sorge um eine Aushöhlung der Demokratie – ein Kommentar*. In: *FlFF-Kommunikation* 4/15, S. 6 f.
- 5 Rechenberg, Ingo (1973): *Evolutionsstrategie: Optimierung technischer Systeme nach Prinzipien der biologischen Evolution*. *Problemata*, 15. Stuttgart-Bad Cannstadt: Frommann-Holzboog
- 6 Maaß, Max (2015): *Faire Algorithmen*. In: *FlFF-Kommunikation* 4/15, S. 10–12
- 7 Epstein, Robert (2016): *The new mind control*. Aeon, 18.02.2016. <https://aeon.co/essays/how-the-internet-flips-elections-and-alters-our-thoughts>



Thesen für die digitale Revolution

Seit einigen Jahren befassen sich die Evangelische Akademie Baden in der Evangelischen Landeskirche in Baden und auch der Deutsche Evangelische Kirchentag immer stärker mit der Digitalen Revolution, einer Revolution, die unmerklich alle und alles durchdringt. Die äußere Haut der Revolution, die viele Menschen wahrnehmen und an der viele Menschen mit großer Freude partizipieren, ist das Internet. Zusätzlich forcieren diese technischen Entwicklungen auf nicht so bekannten, aber genauso wichtigen Pfaden zeitgleich sehr positive Entwicklungen und Forschungen, z.B. innerhalb der Medizin oder in den Sozialwissenschaften. Die überwiegende Zahl davon ist sehr zu begrüßen und noch stärker zu fördern. Parallel werden zurzeit von großen wirtschaftlichen und politischen Akteuren Weichen für die nächsten Jahre gestellt. Diese Weichenstellungen werden das Konzept Mensch prägnant beeinflussen. In welchen Aushandlungsprozessen sich dieses Konzept befindet und wer die Akteure auf diesem Feld sind, wird in der evangelischen Theologie u. a. in der christlichen Anthropologie bedacht. Die theologische Anthropologie reflektiert gegenwärtige Entwicklungen in der Gesellschaft und ihren Einfluss auf das Konzept Mensch auf dem Hintergrund von Aussagen aus der Bibel. Ein Ort, an dem diese theologischen Fragestellungen immer wieder durch Vorträge, Diskussionen und Workshops wie z.B. zur digitalen Selbstverteidigung bedacht werden, ist die Evangelische Akademie Baden in der Evangelischen Landeskirche in Baden.

In den letzten Jahren zeigte sich, dass zu den letzten freien Akteuren, neben NGOs, Aktivistinnen und Aktivisten, die (evangelischen) Kirchen gehören. Sie haben durch ihre weltweite Vernetzung (schon vor dem Internet) besondere Möglichkeiten und durch ihre klare Bezugnahme auf die Bibel einen Referenzrahmen, der meistens frei von parteipolitischem Gezänk oder wirtschaftlicher Einflussnahme ist. In diesem Kontext wurden auch die theologischen Thesen zur Digitalisierung geschrieben. Sie sollen zu einer längst überfälligen, bisher nur marginal geführten, durchaus kontroversen Diskussion anregen und je nach Lesart der Thesen auch zu eigenen Positionierungen aufrufen.

1. Uns Menschen ist die Freiheit geschenkt, uns zu verändern. Deshalb: Du sollst dir kein Bildnis machen.

Die Überwachungssysteme forcieren Bilder von uns, und unsere eigene digitale Gedankenlosigkeit erlaubt es, dass Bilder unseres gesamten Lebens von uns gemacht werden. Bilder, auf die wir festgenagelt werden können. Bilder, denen wir uns nicht mehr entziehen können. Diese Bilder werden aus den Datenspuren und unseren Lebensgewohnheiten erstellt. Diese Bilder machen Maschinen. Menschen sind heute dabei schon weitgehend unbeteiligt. Aber diese von Maschinen hergestellten Bilder bestimmen die Menschen weiter. Wenn dann Entscheidungen von Menschen aufgrund dieser maschinell erstellten Daten anstehen, ist es kaum noch erkennbar, warum eine Person in ein solches Raster gefallen ist. Diese Bilder können unser Leben so determinieren, dass wir nie mehr die Möglichkeit haben, uns aus dieser Gefangenschaft zu befreien. Das Recht auf Vergessen, die Löschung von Daten oder die Angabe eines Verfallsdatums hat für die Gesamtheit der Verbreitungs-, Speicher- und Darstellungsmöglichkeiten im Internet eher kosmetischen Charakter. Es gibt oftmals kein Vergessen und somit auch keinen Neuanfang. Auch die Speicherung von Metadaten kann Bilder erzeugen, die ohne Kontext falsch sind. Wenn man z.B. bei einem Notar, einem Krebspezialisten und einer Pfarrerin anruft, könnte man an Fragen zum Lebensende denken oder an eine Jassrunde mit Freunden.

2. Wir Menschen sind nach Gottes Bild geschaffen. Deshalb: Du sollst die Unterschiedlichkeit schützen und nicht aus deiner scheinbaren Normalität, Jugend, Kraft oder Gesundheit Kapital schlagen.

Je mehr Daten ich den Konzernen zur Verfügung stelle, desto besser wird mein momentaner persönlicher Rabatt sein. Je mehr ich einem gerechneten Standard entspreche, desto besser passe ich in das jeweilige Belohnungssystem. Heute wird immer mehr

die natürliche körperliche Unterschiedlichkeit in den Blick genommen, da sie hauptsächlich als ein Kostenfaktor gesehen wird. Aber umso unsolidarischer trifft es Menschen, die aufgrund ihrer körperlichen Unterschiedlichkeit, die ein Algorithmus berechnet hat, aus diesem Raster herausfallen.

3. Uns ist der andere als Bruder und Schwester in Christus anvertraut. Deshalb: Du sollst die Integrität deines Nächsten schützen.

Viele Menschen haben nicht die Möglichkeit, sich mit Verschlüsselungen zu schützen, d.h., sie können oder dürfen diese nicht nutzen. Das bedeutet zurzeit, die Welt der Computernutzer zerfällt in die, die sich abschirmen und schützen können, und in den Rest. Wenn es mein Nächster oder meine Nächste nicht vermag, ist sie diesem Treiben hoffnungslos ausgeliefert. Wenn ich aktiv anfangs, mich zu schützen und auf meine Integrität achtgebe, wenn ich anfangs, einen Kreis um mich zu ziehen, in den keiner, den ich nicht dazu eingeladen habe, hineinkommen darf, dann werden sich langsam digitale Kulturtechniken entwickeln, die es allen ermöglichen, so zu handeln. Im Umkehrschluss bedeutet das, wenn ich mich nicht schütze, bin ich nicht nur selber schuld, sondern jede Datei, jede E-Mail, jede Information, die unverschlüsselt durch das Netz gesendet wird, schützt auch meinen Nächsten nicht und verändert das System auf Dauer nicht.

4. Uns ist von Gott die Verantwortung und die Freiheit gegeben. Deshalb: Du sollst deine Freiheit und damit die des Nächsten schützen.

Menschen verändern ihre Gewohnheiten, wenn sie abgehört werden. Sogar wenn dies nur theoretisch möglich ist. Welche Ausmaße und Auswirkungen das annehmen kann, zeigt die jüngere deutsche Geschichte. Uns Menschen ist aber diese Grundfrei-

heit des Lebens gegeben worden und diese Freiheit wird zerstört. Die Privatheit ist nicht nur gefährdet, sondern sie ist beseitigt. Man könnte den Eindruck haben, dass Grundrechte angesichts der Software der Geheimdienste und der Untätigkeit der Politik nur noch literarischen Charakter haben oder von einer anderen Zeit zeugen. Der Schutz der Freiheit, sich zu äußern und digital Meinungen zu bilden, betrifft nicht nur Ärzte, Journalistinnen, Richter, Anwälte oder Pfarrerinnen und Priester, sondern alle. Und ganz besonders die, die sich z. B. um die Aufdeckung von Missständen kümmern, Lobbies bilden oder ganz einfach ihre Rechte und Pflichten als Bürger wahrnehmen. Ein Seelsorge- oder Beichtgeheimnis, sofern elektronische Medien genutzt werden oder Geräte wie einige Smartphones oder IP-Telefone in der Nähe herumliegen, erscheint nicht mehr zusicherbar.

5. Uns allen sind von Gott viele Gaben verliehen worden. Deshalb: Du sollst deine digitalen Fähigkeiten zu deinem und vor allem zum Nutzen anderer verbessern.

Das Internet und seine technischen Möglichkeiten, aber auch die Technik, die uns umgibt, ist voll von vielen und oftmals ungenutzten Möglichkeiten. Irgendjemand hat sie für uns programmiert, und meistens nutzen wir sie einfach. Strom, Wasser, der Aufzug, die Ampelanlage und vieles mehr wird über digitale Technik gesteuert. Das macht unser Leben in fast allen Bereichen einfacher und spart darüber hinaus viel Energie und Kosten. Manche Technologien kommen uns dabei sehr nahe und erlauben anderen, uns gleichsam nackt zu sehen. Politische Einstellungen, sexuelle Vorlieben oder persönliche Lebensweisen sind kein Geheimnis mehr. So bleibt den Bürgerinnen und Bürgern nur übrig, sich selbst um ihre digitale Selbstverteidigung zu kümmern. Es gilt heute, durch den Geist der Freiheit wieder zum Akteur des eigenen (digitalen) Lebens zu werden. Setze dich dafür ein, Menschen ihre Angst und Hilflosigkeit zu nehmen, die oft durch Unkenntnis hervorgerufen wird. Das macht wirklich Arbeit – ist aber notwendig.

6. Gott hat uns den Geist der Freiheit geschenkt, der uns frei machen wird. Deshalb: Du sollst nicht einfach glauben, was du in deiner eigenen Informationsblase zu lesen, sehen und hören bekommst.

Hierarchiefrei, partizipativ, sozial und offen etc. sollten die digitalen Medien sein. Leider ist das nicht (mehr) gegeben, und wir Userinnen und User tun alles dafür, dass das Internet immer mehr von multinationalen Konzernen marktwirtschaftlichen Prämissen

unterworfen wird. Das wäre so, als würde uns eine Firma die Atemluft zuteilen, je nachdem, was wir sagen wollten. Oder die Lieferung von Farben geht nur dann schnell, wenn das Bild passt, das gemalt werden soll. Um dieses freie Atmen im Netz zu schützen, sind unter anderem drei Dinge essentiell notwendig: Netzneutralität, offene WLANs (wie die Freifunk-Initiative) und offene Software (Verschlüsselung habe ich schon genannt). Das Konzept des freien Wissens, der freien Zugänglichkeit zu allen Informationen, des bunten, fröhlichen, sozialen Lebens im Netz ist nicht deshalb schlecht, weil Überwachungseinrichtungen es konterkarieren. Es wird sich aber nur dann für uns und die nachfolgenden Generationen als freie Medienverbundmaschine durchsetzen, wenn wir es wieder zurückerobern. Es gilt, Kulturtechniken zu entwickeln, um leicht Informationen und Positionen sowie die Entstehung von Information und ihre Funktion im Feld zu analysieren. In der Zukunft werden diese Kulturtechniken im neuen sechsstündigen Pflichtfach „Informationsmanagement und Wissensknoten“ an Schülerinnen und Schüler vermittelt werden.

7. Uns sind von Gott Phantasie, Ideenreichtum und die Möglichkeit geschenkt worden, sich und alles andere immer wieder neu zu erfinden. Deshalb: Du sollst das Leben von dir und von anderen durch die Digitalisierung bereichern und die Berechnung dort zurückweisen, wo sie dich beziffert.

Unzählige Menschenleben wurden schon gerettet, weil jemand sein Mobiltelefon dabei hatte und sofort Hilfe holen konnte oder weil Mediziner Verfahren in der Krebsterapie mit Hilfe von großen Datenmengen und zugehörigen Algorithmen weiterentwickeln konnten. Unzählige Menschen können heute an politischen oder kulturellen Ereignissen rund um den Erdball teilnehmen, Informationen gleichsam *vor Ort* von involvierten Personen bekommen oder einfach leicht mit anderen kommunizieren, obwohl sie sich z. B. nicht mehr gut bewegen können. Unzählige Möglichkeiten, Chancen und Ideen lassen sich durch den Einzug der digitalen Medien verwirklichen. Diese Chancen zu sehen, sich nicht von Personen irritieren zu lassen, die uns digitale Demenz bescheinigen, oder in einen Internet-Alarmismus zu verfallen, ist das Gebot unserer Zeit. So ist es notwendig, Digitalisierung zu fördern, die allen Menschen zugutekommt. Bereiche, die Unterstützung brauchen, gibt es genug. Der Schattenseite, der Bezifferung des Lebens, ist aber Einhalt zu gebieten. Das Diktat des Ertrages, des quantifizierenden marktorientierten Denkens, das durch die Digitalisierung in ein neues Zeitalter eingetreten ist, das Diktat der Leistungsziffern und die Ausweitung der Ökonomisierung auf alle Bereiche wie Religion, Kultur und Wissenschaft müssen zurückgewiesen werden.

Gernot Meier



Pfarrer Dr. **Gernot Meier** ist Religionswissenschaftler, Studienleiter an der Evangelischen Akademie Baden in den Bereichen Wissenschaft, Kultur, Medien und Weltanschauungen und Landeskirchlicher Beauftragter für Weltanschauungsfragen.

8. Gott hat in uns und um uns viele mögliche Welten angelegt. Deshalb: Du sollst Möglichkeiten eröffnen, Ambiguitäten aushalten und dich nicht in eine Orientierung der berechneten Welt flüchten.

Wir leben in der Postmoderne, die mit ihren vielen Optionen Menschen Angst machen kann. Orientierungen für sich zu finden und das Leben in seiner Unbestimmtheit zu meistern, ist eine große Aufgabe. Hier stellt sich die Frage, was sind unsere Maßstäbe, und welche Modelle berücksichtigen wir dabei. Aus der technischen Moderne haben wir das Berechnen der Welt übernommen, und es hilft uns im täglichen Leben. Bei der Suche nach einem Partner oder einer Partnerin oder der schnellsten Verbindung von Paris nach Karlsruhe. Berechnung ist aber kein Ersatz für den Verlust von Orientierung in der Postmoderne, nicht einmal geografisch. Wenn wir anfangen, Algorithmen Erkenntnis zuzuschreiben und den Zukunftsforschern glauben, dass man mit extremen Datenmengen (*Big Data*) alles berechnen kann, haben wir aufgegeben, nach dem Warum zu fragen. Setze dich dafür ein, dass ethische Entscheidungen in all ihrer Komplexität sich an der lebendigen Welt orientieren und dass unsere Entscheidungen sich nicht von berechneten Zielvorgaben gänzlich bestimmen lassen. Die Welt darf nicht zu einer Statistik werden, in deren Gefolge mögliche Richtgrößen eine schöne neue Welt erschaffen.

9. Uns ist der Sonntag geschenkt worden. Deshalb: Du sollst bei anderen nicht erwarten, dass sie sofort auf deine E-Mail antworten, und bezahle die Menschen für ihre digitale Arbeit oder mache es einfach selbst.

Im Fluss der Daten und im Sog der Zeit lernen wir gerade auf digitalen Wellen zu surfen. Von Information zu Information, von Post zu Post, von Sound zu Sound. Jeder Mensch muss hier seine eigene Geschwindigkeit finden, seine Art, mit den „Ansprüchen“ der digitalen Medien umzugehen. Dazu gehört auch, dass bei Fragen, bei denen es nicht um Leben und Tod geht oder

man die Liebe des Lebens verlieren könnte, auch Zeit vergehen kann, bis du eine Antwort bekommst. Setze dich aktiv dafür ein, dass Arbeitsbedingungen und die Digitalisierung so zusammenkommen, dass es für die Menschen kein Rennen gegen die Zeit ist. Dazu gehört auch, vor allem im Kontext der *Industrie 4.0*, zwischen Möglichkeit und dringender Notwendigkeit zu unterscheiden. Dazu gehört auch, dass wir lernen müssen: Wenn wir im Netz etwas gratis bekommen, sind wir nicht der Kunde, sondern das Produkt. Das müssen wir durchbrechen – für uns wie für die anderen. Für uns, weil wir keine Produkte mehr werden dürfen, und für die vielen Menschen, die online ihren Lebensunterhalt verdienen. Journalisten, Programmiererinnen oder auch Literaturschaffende oder Musikerinnen müssen ihren fairen Anteil ohne Zwischenvermarktungssysteme bekommen. Auch sie wollen in Frieden am Samstagabend tanzen gehen, am Sonntag mit ihren Liebsten unterwegs sein und nicht als Klick- und Schreiblemming in einem dunklen Büro enden.

10. „Ich sitze oder stehe auf, so weißt du es; du verstehst meine Gedanken von ferne. Ich gehe oder liege, so bist du um mich und siehst alle meine Wege. Denn siehe, es ist kein Wort auf meiner Zunge, das du, HERR, nicht schon wüsstest. Von allen Seiten umgibst du mich und hältst deine Hand über mir.“ Ps 139,2

Der Psalmendichter, der diese Zeile vor ca. 2500 Jahren schrieb, sah darin wahrscheinlich etwas sehr Positives, und auch heute erleben viele Menschen diese Zeilen für sich als einen Schutz in ihrem Leben. Der Adressat ist allerdings Gott, und nach meiner Überzeugung sind diese Dinge Gott allein vorbehalten. Nach allem, was im Kontext der digitalen Revolution bekannt ist, wird das Ziel zukünftig sein, schon wenige Zeit – vielleicht nur wenige Sekunden – bevor ein Mensch etwas denkt, plant, kaufen will oder entscheidet, es schon vorher zu wissen. Hier setzen sich Menschen und deren Maschinen an diese Stelle – dorthin, wo eigentlich nur Gott stehen dürfte.



Anja Gerlmaier

Ausgeglichen oder ausgepowert?

Wie High-Tech-Unternehmen mit Arbeitskraft umgehen

Der IT-Sektor zählt schon seit Längerem zu den Wirtschaftsbereichen mit einem ausgeprägten Fachkräftengpass. Prognosen zufolge wird sich das in den nächsten 20 Jahren durch den demografischen Wandel weiter verschärfen. Vermehrte Bemühungen, die Absolventen-Quoten in den IT-Berufen zu erhöhen, ausländische Fachkräfte anzuwerben oder gezielt weibliche Fachkräfte zu fördern, sind viel versprechende Ansätze, um die Innovationsträger der Zukunft zu gewinnen. Doch wie sieht es dann später mit der Erhaltung und Weiterentwicklung des begehrten Humankapitals in der Erwerbsbiografie aus? Dieser Frage ging das vom Bundesministerium für Bildung und Forschung finanzierte Forschungsvorhaben PINOWA nach.

Das *intellektuelle Kapital* weiblicher und männlicher Informatiker, Ingenieure und Techniker stellt ein kostbares Gut dar. Demoskopien gehen davon aus, dass sich aufgrund der demografischen Umwälzungen der Fachkräftemangel bei bestimmten IT-Tätigkeiten und Ingenieursberufen in den nächsten Jahren eher verschärfen wird.¹

Viele IT-Unternehmen setzen angesichts dieser Entwicklungen auf modernes Personalmanagement: Sie unterstützen ihre Beschäftigten beim Berufseinstieg, in der Familiengründungsphase oder vor dem Renteneintritt. Ausgeklügelte Karriere- und Anreiz-Systeme, *Kicker* und Entspannungszonen in der Firma oder Angebote zur Kinderbetreuung sollen ebenfalls dazu beitragen, dass

sich die hochqualifizierten Wissensarbeiter in ihrem Unternehmen wohl fühlen und leistungsbereit bleiben. Diese Bemühungen können jedoch nicht darüber hinwegtäuschen, dass Entwicklungsarbeit heute in ausgeprägten Hochleistungskulturen stattfindet.

Zwei widersprüchliche Tendenzen sind zu beobachten. Zum einen werden die verfügbaren Innovationspotenziale der Beschäftigten im ungünstigsten Fall eher verschlissen als gepflegt und weiter entwickelt, wie Ergebnisse der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin zeigen: Gerade Ingenieure und verwandte Berufsgruppen sind überdurchschnittlich von psychischen Belastungen wie Arbeitsunterbrechungen, Leistungsdruck und Multitasking betroffen, die als wichtige Risikofaktoren für die Entstehung von Stress und psychischer Erschöpfung bekannt sind² (siehe auch Abbildung 1). Zum anderen werden vorhandene Innovationspotenziale innerhalb der Belegschaften nicht ausreichend erschlossen, trotz zum Teil umfangreicher Angebote zur Personalentwicklung. Fehlende Karriereperspektiven, etwa für Teilzeitbeschäftigte oder erfahrene Mitarbeitende, aber auch unzureichende *Return-to-Work*-Konzepte für Beschäftigte nach längeren Erkrankungsphasen tragen dazu bei, dass kreative Köpfe mit viel Knowhow abwandern oder sich in eine *innere Kündigung* begeben.³ Auch wenn die meisten Unternehmen im Entwicklungsbereich über ausgeklügelte Kennzahlen- und Controlling-Systeme verfügen: Belastbare Daten über lebensphasenspezifische Gesundheitsindikatoren oder Qualifikationsbedarfe besitzen sie in der Regel nicht.

	Elektroberufe	Ingenieure, Chemiker, Physiker, Mathematiker	Gesundheitsberufe	Gesamt
bei der Arbeit gestört, unterbrochen	42 %	54 %	55 %	44 %
verschiedenartige Arbeiten gleichzeitig betreuen	44 %	73 %	68 %	58 %
starker Termin- und Leistungsdruck	56 %	61 %	62 %	52 %

Abbildung 1: Psychische Belastungen, die mit zunehmendem Alter Einfluss auf die Leistungsfähigkeit ausüben, Quelle: Institut Arbeit und Qualifikation, Daten: BAuA, Stressreport 2012

Eine neue Perspektive: Arbeits- und Lebensepisoden

Als neuer Lösungsansatz für dieses Problem wurde das Konzept der „anspruchsvollen Arbeits- und Lebensepisoden“⁴ entwickelt. Es geht davon aus, dass es innerhalb der beruflichen und privaten Lebenswelt anspruchsvolle bzw. herausfordernde *Episoden* geben kann: Charakteristisch für Episoden ist, dass sie für die Betroffenen neuartige Situationen darstellen, für die es zunächst keine routinisierten Handlungs- und Bewältigungsmuster gibt. Sie gehen deswegen häufig mit einer erhöhten Beanspruchung einher. Der Begriff Episode impliziert dabei, dass es sich in der Regel um eine zeitlich befristete Phase handelt, die innerhalb einer Erwerbsbiografie auftreten kann, aber nicht muss. Im Rahmen der Erwerbsbiografie können Arbeits- und Lebensepisoden aufeinander folgen, aber sich auch überlagern. Sie sind nicht als starre Konstrukte mit einem klar festgelegten zeitlichen Rahmen anzusehen, sondern als begrenzte Phasen, aus denen sich ein Individuum auch wieder herausbewegen kann.

Durch diese spezifische Perspektive ist eine Lebensphasenorientierung von personalwirtschaftlichen Konzepten wie etwa dem *Diversity-Management* zu unterscheiden. Letztere gehen in der Regel davon aus, dass allein die Erzeugung von Diversität ausreicht, um neue Ideen und Perspektiven in ein Unternehmen zu bringen.⁵ Mit der Fokussierung auf Unterschiede wie männlich/weiblich, jung/alt, oder die Differenzierung von Beschäftigten mit und ohne Handicap bzw. nach ethnischen Hintergrund besteht jedoch das Risiko, Attribute hervorzuheben, die tendenziell stigmatisieren und deshalb für die Erzeugung von Chancengleichheit eher kontraproduktiv sind. Zum anderen kann dadurch leicht übersehen werden, dass etwa männliche und weibliche Beschäftigte in bestimmten Arbeits- und Lebensepisoden (beispielsweise der Familiengründungsphase) sich ähnlicher sind als Geschlechtsgenossinnen und -genossen, die sich in gänzlich anderen Arbeits- und Lebenssituationen befinden. Ziel dieser neuen und differenzierteren Betrachtung ist es deshalb zum einen, die organisationalen Voraussetzungen zu schaffen für eine bessere Bewältigung anspruchsvoller Arbeits- und Lebensepisoden – wie etwa die erste Verantwortungsübernahme bei Berufseinstiegern, aber auch familiäre oder gesundheitliche Krisen. Zum anderen können es so ausgerichtete praktische Analysewerkzeuge den Unternehmen ermöglichen, lebensphasenspezifische Handlungsbedarfe in der Personalarbeit präziser zu identifizieren.⁶

Methodisches Vorgehen

Um zu ermitteln, in welchen anspruchsvollen Arbeits- und Lebensepisoden sich ungünstige Formen psychischer Beanspruchung und Kompetenznutzung finden lassen, wurde ein mehrstufiges, multi-methodales Analysedesign gewählt:

Im Rahmen von Workshops mit etwa 20 betrieblichen Expertinnen und Experten (Personalverantwortliche, Betriebsräte) wurden diese gebeten, potenziell anspruchsvolle Lebensepisoden zu benennen, für die sie einen erhöhten personalwirtschaftlichen Handlungsbedarf sehen.

Aufbauend auf diesen Bewertungen erfolgte die Entwicklung eines Indikatoren-Rasters, anhand dessen die als *anspruchsvoll* eingestuften Arbeits- und Lebensepisoden operationalisiert werden konnten. In einem dritten Untersuchungsschritt wurden anhand von Befragungsdaten zunächst Personen identifiziert, die gemäß Indikatoren-Cluster einer anspruchsvollen Arbeits- und Lebenssituation zugeordnet werden konnten. Die Datenbasis bildeten dabei Belastungs- und Ressourcenanalysen von 254 Ingenieuren und IT-Spezialisten aus drei Unternehmen. In diesem Sample konnten 171 Personen einer anspruchsvollen Arbeits- und Lebensepisode zugeordnet werden. Im letzten Schritt wurden die Unterschiede analysiert zwischen den Befragten in einer anspruchsvollen Arbeits- und Lebensepisode im Hinblick auf ihr Beanspruchungserleben, den subjektiv erlebten Kompetenzeinsatz und die Motivation.

Psychische Beanspruchungen in anspruchsvollen Arbeits- und Lebensepisoden

Gibt es Arbeits- und/oder Lebensepisoden im Erwerbsverlauf von IT-Spezialisten und Ingenieuren, die mit einer erhöhten psy-

chischen Erschöpfung verbunden sind? Von einer solchen Annahme der *Übernutzung* der persönlichen Leistungsvoraussetzungen wurde ausgegangen, wenn Beschäftigte aufgrund von quantitativer Überforderung Erschöpfungssymptome entwickeln. Das wäre etwa dann der Fall, wenn Beschäftigte angeben, dass sie sich nach der Arbeit erschöpft fühlen, das Gefühl haben, die derzeitige Tätigkeit auf Dauer nicht ausüben zu können, oder schon morgens Gefühle von Zerschlagenheit empfinden.

Betrachtet man die Verteilung der berichteten Erschöpfungssymptome über die Erwerbsphasen hinweg, so zeigt sich, wie in Tabelle 1 dargestellt: Bei den jungen Beschäftigten bis zum Alter von 30 Jahren findet sich im vorliegenden Sample mit 33 % ein geringerer Anteil stark erschöpfter Personen. Im mittleren Erwerbsabschnitt zwischen 31 und 50 Jahren ist dagegen jede.r Zweite hochgradig psychisch erschöpft (53 % bei den 31- bis 40-Jährigen bzw. 52 % bei den 41- bis 50-Jährigen), während bei den Beschäftigten im späteren Erwerbsabschnitt das Erschöpfungsniveau etwas geringer ist (45 % bei den unter 50-Jährigen).

Die berufliche Orientierungsphase (Alter unter 30 Jahre) scheint für die jungen Beschäftigten jedoch nicht immer von geringer Beanspruchung gekennzeichnet zu sein: Zwar ist das Beanspruchungsniveau bei Berufseinsteigern, die gerade eine Ausbildung oder ein Trainee-Programm absolviert haben, mit einem Anteil von 27 % Hochbeanspruchten relativ gering. Junge IT-Spezialisten oder Ingenieure, die erste Verantwortung für Projekte oder Fachgebiete übernehmen, weisen jedoch mit einem Anteil von 67 % Hochbeanspruchter ein überdurchschnittliches Maß von psychischer Erschöpfung auf. Auch der Anteil von Beschäftigten, die sich in einer Episode sekundärer Qualifizierung (beispielsweise Promotion, duales Studium) befinden, ist mit 46 % Hochbeanspruchten deutlich höher als der Durchschnitt dieser Altersgruppe.

Der mittlere Erwerbsabschnitt – die „Rushhour des Lebens“ – ist für viele Beschäftigte von zentralen, wegweisenden Lebensentscheidungen geprägt. In dieser Zeit werden häufig die Weichen gestellt für die weitere Laufbahn und Karriere. Es ist für viele auch die Phase, in der Beschäftigte sich entscheiden, ob sie eine Familie gründen wollen oder nicht. Der mittlere Erwerbsabschnitt (von 31 bis 50 Jahren) weist in unserem Sample die größte Anzahl von Befragten mit erhöhten Beanspruchungswerten auf (Tabelle 1).

Über dieses Niveau hinausgehende Beanspruchungswerte liegen vor allem in Episoden vor, in denen Karriere und erste Führungsverantwortung mit einer Familiengründung einhergingen (60 %). Das Erschöpfungsniveau in Episoden mit erster Personalverantwortung erweist sich dagegen als vergleichbar mit dem Altersdurchschnitt. Im mittleren Erwerbsabschnitt finden sich erwartungsgemäß auch die meisten Episoden einer Familiengründung. Die Beanspruchungswerte sind unter den Befragten in diesen Episoden stark abhängig von der Arbeitszeit, womit vermutlich auch geschlechtsspezifische Unterschiede zusammenhängen. Der Anteil von hochbeanspruchten Befragten, die in der Familiengründungsphase in Vollzeit tätig sind (im Sample fast ausschließlich Männer), ist eher unterdurchschnittlich (34 %). Teilzeitbeschäftigte, in unserem Sample überwiegend Frauen, wiesen dagegen Werte im Durchschnitt des Referenzalters auf. Weil diese Episode von unseren betrieblichen Expertinnen und Experten als Zielgruppe mit Handlungsbedarf charakterisiert wurde, ist es ein irritierender Befund, dass Beschäftigte, die in den letzten drei Jahren das Unternehmen oder die Tätigkeit gewechselt hatten, eher ein unterdurchschnittliches Beanspruchungsniveau haben. Der Anteil der Hochbeanspruchten, die sich in einer solchen Episode befanden, liegt mit 18 % deutlich unter dem Durchschnittswert.

Wie Tabelle 1 zeigt, ist auch in der Phase zwischen 40 und 50 Jahren das Beanspruchungsniveau der Befragten mit 52 % Hochbeanspruchten noch als sehr hoch anzusehen. Erst mit der

Episode	Anteil Hochbeanspruchter in % (Altersdurchschnitt)	Anteil Hochbeanspruchter in dieser Erwerbs-/Lebensphase in % (Altersspanne)
Berufseinstieg	27 % (25 Jahre)	33 % (< 30 Jahre)
Erste Verantwortungsübernahme	67 % (27 J.)	33 % (< 30 J.)
Sekundäre Qualifizierungsphase	46 % (29 J.)	33 % (< 30 J.)
Tätigkeits-/Unternehmenswechsel	18 % (39 J.)	53 % (31-40 J.)
Karrierephase	50 % (38 J.)	53 % (31-40 J.)
Karriere während Familiengründung	60 % (33 J.)	53 % (31-40 J.)
Familiengründung in Vollzeit	33 % (38 J.)	53 % (31-40 J.)
Familiengründung in Teilzeit	50 % (40 J.)	53 % (31-40 J.)
Episode mit gering verfügbarem Spezial-Knowhow	82 % (44 J.)	52 % (41-50 J.)
Familiäre Krise	83 % (47 J.)	52 % (41-50 J.)
Gesundheitskrise	82 % (48 J.)	52 % (41-50 J.)
Spezialisierungsfall	71 % (51 J.)	45 % (> 51 J.)
Statusbezogener Abstieg	67 % (56 J.)	45 % (> 51 J.)
Ausgleitphase	31 % (56 J.)	45 % (> 51 J.)

Tabelle 1: Psychische Erschöpfung im Erwerbsverlauf und in anspruchsvollen Lebensereignissen, Quelle: eigene Erhebung

späteren Erwerbsphase ab 50 Jahren sinkt es etwas ab (45 %). Allerdings finden sich auch bei den 40- bis 50-Jährigen anspruchsvolle Episoden, in denen überdurchschnittlich viele Beschäftigte ein darüber hinausgehendes Beanspruchungsrisiko aufweisen: In der Untersuchung sind das insbesondere Episoden, in denen Beschäftigte aufgrund von knappem Spezial-Know-how in mehreren Projekten parallel eingesetzt werden (82 % Hochbeanspruchte). Vergleichbar viele Hochbeanspruchte finden sich auch in Episoden mit gesundheitlichen Krisenerfahrungen oder bei krisenhaften Familiensituationen (wie etwa Trennungen oder Pflege von Familienangehörigen), die im mittleren Erwerbsabschnitt verstärkt auftreten. Überdurchschnittlich viele Beanspruchte können auch in Lebensepisoden identifiziert werden, die als *Spezialisierungsfälle* (71 %) oder als statusbezogener beruflicher Abstieg erlebt werden (67 %). Die letzten beiden Episoden werden allerdings nur von sehr wenigen Beschäftigten genannt. Günstigere Beanspruchungswerte als im Durchschnitt dieser Altersgruppe haben Beschäftigte, die in den nächsten zwölf Monaten aufgrund von Altersteilzeit oder einem regulären Renteneintritt das Unternehmen verlassen. Hier beträgt der Anteil Hochbeanspruchter nur 31 %.

Unternutzung individueller Kompetenzen und Erfahrungen

Nach dem Beanspruchungsaspekt wird nun untersucht, inwieweit IT-Spezialistinnen und IT-Spezialisten sowie Ingenieurinnen und Ingenieure in ihrer Erwerbsbiografie Phasen erleben, in denen sie ihre Kompetenzen und Fähigkeiten nicht ausreichend einsetzen können: Eine Unternutzung persönlicher Ressourcen wurde dann als gegeben gesehen, wenn Beschäftigte angaben, bei ihrer derzeitigen Tätigkeit ihre Kompetenzen und Fähigkeiten in hohem Maße nicht einsetzen zu können.⁷ Als Unternutzung wurde auch gewertet, wenn Beschäftigte das Gefühl hatten, dass ihre Ideen und Vorschläge im Betrieb auf wenig Interesse stießen.

Über die Erwerbsbiografien hinweg zeigt sich dabei erwartungsgemäß, dass nur vergleichsweise wenige Beschäftigte in den untersuchten Entwicklungsbereichen eine Unternutzung von Kompetenzen erleben: Im Erwerbsverlauf sind es vor allem die älteren Beschäftigten (über 51 Jahre) mit 38 %, die sich im Hinblick auf ihre Fähigkeiten und Ideen nicht richtig eingesetzt fühlen (Tabelle 2). Auch bei den 41- bis 50-Jährigen hat etwa jeder Dritte das Gefühl, dass seine Kompetenzen nur unzureichend vom Unternehmen genutzt werden.

In der beruflichen Orientierungsphase erleben vergleichsweise wenige Befragte eine unzureichende Nutzung ihrer Kompetenzen (28 %). Dennoch gibt es Episoden, die von einer Unterforderung gekennzeichnet sein können: Etwa jede.r Dritte, die/der von der Ausbildung in den Beruf wechselt oder erste Verantwortung für Aufgaben übernimmt, hat das Gefühl, die zuvor erworbenen Kompetenzen bei der aktuellen Tätigkeit nicht einsetzen zu können.

In späteren Erwerbsabschnitten ist der Anteil von Befragten deutlich höher, die sich im Hinblick auf ihre Kompetenznutzung unterfordert fühlen. Es sind interessanterweise Personen mit im Unternehmen knappem Spezial-Knowhow, die im Durchschnitt häufiger angeben, sich hinsichtlich der Nutzung ihrer Kompetenzen unterfordert zu fühlen (43 %). Auch Personen mit gesundheitlichen Krisenerfahrungen erleben ihre Tätigkeit häufiger als unterfordernd (41 %). Das könnte damit zusammenhängen, dass Führungskräfte bei gesundheitlichen Einschränkungen von Mitarbeitenden dazu neigen, diese auf so genannte *Schonarbeitsplätze* zu setzen, womit eine Qualifikationsabstufung verbunden sein kann (zum Beispiel Wechsel von Projektarbeit in eine Stabsfunktion). Besonders Personen, die sich in einer Episode statusbezogenen beruflichen Abstiegs oder in einer beruflichen Spezialisierungsfälle befinden, weisen überdurchschnittlich hohe Werte qualitativer Unterforderung auf (67 % bzw. 43 %).

Episode	Stark unternutzt in % (Altersdurchschnitt)	Stark unternutzt in dieser Erwerbs-/ Lebensphase in % (Altersspanne)
Berufseinstieg	33 % (25 Jahre)	28 % (< 30 Jahre)
Erste Verantwortungsübernahme	33 % (27 J.)	28 % (< 30 Jahre)
Sekundäre Qualifizierungsphase	27 % (29 J.)	28 % (< 30 Jahre)
Tätigkeits-/Unternehmenswechsel	24 % (39 J.)	22 % (31-40 Jahre)
Karrierephase	25 % (38 J.)	22 % (31-40 Jahre)
Karriere während Familiengründung	20 % (33 J.)	22 % (31-40 Jahre)
Familiengründung in Vollzeit	11 % (38 J.)	22 % (31-40 Jahre)
Familiengründung in Teilzeit	25 % (40 J.)	22 % (31-40 Jahre)
Episode mit gering verfügbarem Spezial-Knowhow	43 % (44 J.)	34 % (41-50 Jahre)
Familiäre Krise	17 % (47 J.)	34 % (41-50 Jahre)
Gesundheitskrise	41 % (48 J.)	34 % (41-50 Jahre)
Spezialisierungsfälle	43 % (51 J.)	38 % (> 51 Jahre)
Statusbezogener Abstieg	67 % (56 J.)	38 % (> 51 Jahre)
Ausgleitphase	31 % (56 J.)	38 % (> 51 Jahre)

Tabelle 2: Unternutzung im Erwerbsverlauf und in anspruchsvollen Lebensepisoden, Quelle: eigene Erhebung

Fazit: blinde Flecken in der Personalarbeit

Die Ergebnisse deuten darauf hin, dass in den untersuchten Entwicklungsbereichen in allen Erwerbsphasen spezifische anspruchsvolle Arbeits- und Lebensepisoden vorzufinden sind, die mit einem deutlich erhöhten Beanspruchungsrisiko und der Gefahr einhergehen, dass vorhandene Innovationspotenziale und Knowhow aufgrund der jeweiligen persönlichen Arbeits- und Lebenssituation unerschlossen bleiben. Traditionelle Personalmanagement-Strategien, die sich vor allem auf den Übergang ins Berufsleben, die Familiengründungsphase sowie den Erwerbsaustritt konzentrieren, greifen hier zu kurz. Im Hinblick auf die psychische Beanspruchung und Unternutzung von Kompetenzen erwiesen sich Arbeits- und Lebensepisoden wie die Phase der ersten Verantwortungsübernahme, Phasen als Träger knappen Spezial-Knowhows oder Episoden gesundheitlicher Krisen als weitaus kritischer. Die vorhandenen Daten lassen keinen Rückschluss darauf zu, ob erfolgreiche Personalmanagement-Strategien die geringen Beanspruchungswerte in Phasen des Berufseinstiegs, der Familiengründung und des altersbedingten Unternehmensaustritts bewirkt haben, oder ob es sich um Episoden handelt, für die insgesamt ein geringerer Handlungsbedarf besteht als bisher vermutet.

Dagegen konnte in der Analyse eine Reihe von anspruchsvollen Arbeits- und Lebensepisoden innerhalb der Erwerbsbiografie von hoch qualifizierten Beschäftigten identifiziert werden, für die es in den meisten Unternehmen offenbar Handlungsbedarf, aber bisher keine angemessenen Unterstützungsangebote oder Arbeitsgestaltungs- und Laufbahnkonzepte gibt.

Gute Praxisbeispiele für eine lebensphasenorientierte Arbeitsgestaltung können Mentoren-Programme darstellen, bei denen erfahrene Projektmitarbeitende die Berufseinsteiger z. B. bei der Promotion unterstützen. Auch Tandem-Konzepte, bei denen ein Berufseinsteiger und ein erfahrener Projektmitarbeiter ein Projekt gemeinsam bearbeiten, bieten Potenziale zur Beanspruchungsminderung und Kompetenzentwicklung für die jüngeren und älteren Projektmitarbeitenden.

Um eine nachhaltige Lebensphasenorientierung im Unternehmen implementieren zu können, ist es unerlässlich, entsprechende Arbeitskulturen zu etablieren. Das kann nur gelingen, wenn Regelungen zur besseren Bewältigung von anspruchsvollen Arbeits- und Lebensepisoden für alle Beschäftigtengruppen wirksam sind und nicht lediglich *Zumutungen* verschoben werden. Gerade im Hinblick auf Überlastungsprobleme kommt der

Prävention eine wichtige und bisher häufig unterschätzte Bedeutung zu: Statt Belastungen zu verschieben oder Qualifikationsmöglichkeiten zu selektieren, kann eine große Chance von lebensphasenorientierten Personalmanagement-Konzepten darin bestehen, mit intelligenten Lösungen zur Verminderung psychischer Belastungen und mit einem Lebensphasen übergreifenden Kompetenzaufbau Arbeitskraftpotenziale in jeder Erwerbsphase zu stärken. Wie eine gesunde und innovative Entwicklung in der Erwerbsbiografie unterstützt werden kann, zeigt auch ein im Vorhaben PINOWA erstelltes Praktiker-Handbuch⁸. Für den Bereich der Technikentwicklung werden Konzepte, Befunde, Instrumente und Erfahrungsberichte für ein lebensphasenorientiertes Personalmanagement vorgestellt.

Anmerkungen

- 1 Neubecker, Nina (2014): *Die Debatte über den Fachkräftemangel*. DIW Roundup 14.01.2014. Berlin: DIW. http://www.diw.de/de/diw_01.c.434984.de/presse/diw_roundup/die_debatte_ueber_den_fachkraeftemangel.html (Stand: 19.02.2015)
- 2 Lohmann-Haislah, Andrea (2012): *Stressreport Deutschland 2012. Psychische Anforderungen, Ressourcen und Befinden*. Dortmund/Berlin/Dresden: BAuA. http://www.baua.de/de/Publikationen/Fachbeitraege/Gd68.pdf?__blob=publicationFile
- 3 Gül, Katrin; Boes, Andreas; Kämpf, Tobias (2015): *Lebensphasensensible Entwicklungs- und Karrierekonzepte: Was brauchen die Beschäftigten?* In: Gerlmaier et al. 2015, S. 143–170.
- 4 Gerlmaier, Anja (2015): *Gesund und innovativ arbeiten in jeder Lebensepisode: personalwirtschaftlicher Handlungsbedarf bei Entwicklungsberufen*. In: Gerlmaier et al. 2015, S. 35–57.
- 5 Uribe, Jaime; Strina, Giuseppe; Preuschoff, Susanne (2003): *Diversity Management – Betriebliche Integration kultureller Vielfalt*. In: Preuschoff, Susanne; Hees, Frank (Hg.): *Kulturelle Vielfalt als Ressource. Neue Nutzungspotenziale für Betriebe und ihre Kunden*. Aachen. S. 21–42.
- 6 Latniak, Erich; Gerlmaier, Anja (2015): *Lebensphasenorientiertes Personalmanagement: betriebliche Handlungsfelder erkennen mit der „Lebensphasenorientierten Potenzialanalyse“*. In: Gerlmaier et al. 2015, S. 207–220.
- 7 Lämsäalmi, Hannakaisa; Kivimäki, Mika; Elovainio, Marko (2004): *Is underutilization of knowledge, skills, and abilities a major barrier to innovation?* In: *Psychological Reports*, 94:3, 739–750.
- 8 Gerlmaier, Anja; Gül, Katrin; Hellert, Ulrike; Kämpf, Tobias; Latniak, Erich (Hg.) (2015): *Praxishandbuch lebensphasenorientiertes Personalmanagement. Fachkräftepotenziale in technischen Entwicklungsbereichen erschließen und fördern*. Wiesbaden: Springer Gabler.

Anja Gerlmaier



Anja Gerlmaier ist wissenschaftliche Mitarbeitende am Institut Arbeit und Qualifikation der Universität Duisburg-Essen und arbeitet an Fragen der Stressprävention, Arbeitsgestaltung und Personalentwicklung.

Vertrauen erhalten – Datensicherheit und Datenschutz bei modernen Fahrzeugen

Sowohl die Weiterentwicklung der Fahrzeugtechnik als auch die Vernetzung der Verkehrsteilnehmer bieten erhebliche Chancen, den Straßenverkehr sicherer, effizienter und ressourcenschonender zu gestalten. Gemeinsame Basis ist ein zuverlässiger Datenaustausch: sei es zwischen den Komponenten innerhalb eines Fahrzeugs oder zwischen einem und anderen Fahrzeugen oder Verkehrsteilnehmern oder weiteren Teilen der Verkehrsinfrastruktur. Damit stellen sich neue Aufgaben zur Wahrung der Datensicherheit und des Datenschutzes.

Damit motorisierter Straßenverkehr Realität werden konnte, hatten Fahrzeuge stets ein Mindestmaß an Sicherheitsanforderungen zu erfüllen. Im Zuge des enormen Ausbaus des Straßenverkehrs in der zweiten Hälfte des letzten Jahrhunderts erfuhr die Fahrzeugtechnik neben dem Unfallgeschehen besondere öffentliche Aufmerksamkeit zusätzlich durch die kontinuierlich ansteigende Umweltbelastung. In deren Folge wurden die Anforderungen an die technische Sicherheit um solche ergänzt, welche die Umwelt nachhaltig schützen.

Mit zunehmender Elektronifizierung der Automobile rückten in den letzten Jahren – parallel zum Umweltschutz und zur Verkehrssicherheit – Datensicherheit und Datenschutz in das Bewusstsein der Nutzer. Noch werden vornehmlich Daten innerhalb des Autos verarbeitet. Intelligentes Motormanagement reduziert Umweltbelastungen und Assistenzsysteme helfen, Unfälle zu vermeiden sowie deren Folgen zu mindern.

Heute und morgen

In den letzten Jahren haben immer mehr Assistenzfunktionen im Auto Einzug gehalten, die uns als Fahrerinnen und Fahrer unterstützen und dabei helfen, im Falle von Unaufmerksamkeit oder Fahrfehlern Unfälle zu vermeiden bzw. deren Folgen zu mindern.

Moderne Fahrzeuge sind heute neben ABS und ESP mit weiteren Systemen und Funktionen ausgestattet, die den Fahrer in seiner Wahrnehmung, Informationsverarbeitung, Entscheidungsfindung und seinem Handeln assistieren oder diese Handlungen zunehmend selbst ausführen können. In den letzten Jahren waren es die Fortschritte der Fusion von Daten, die es dem Fahrzeug ermöglichen, ein immer detailliertes Bild von der Umgebung zu erheben und in die Regelung einzubeziehen. Vom Sicherheitsgewinn durch solche Systeme sind in Deutschland neun von zehn Autofahrern überzeugt.¹

Die automobilen Welt und damit auch das Sachverständigenwesen stehen vor neuen Herausforderungen. Schon in Kürze werden neben innovativen Fahrzeugkonzepten und alternativen Antrieben insbesondere weiterentwickelte Assistenzsysteme sowie aktiv kommunizierende Sicherheitsfunktionen auf dem Markt sein.

eCall

Als erste aktiv kommunizierende Sicherheitsfunktion kommt der *Elektronische Notruf* (emergency call, eCall)² in die Fahrzeuge, er ist ab 2018 für alle neu zugelassenen Fahrzeugmodelle in Europa vorgeschrieben. eCall ermöglicht es dem Fahrzeug, eine

Kommunikationsverbindung aufzubauen. Das kann manuell durch den Fahrer geschehen oder durch ein bedeutsames Ereignis hervorgerufen werden, das – wie beispielsweise die Aktivierung eines Airbags – auf einen Unfall hindeutet. Übermittelt werden in beiden Fällen

- die Unfallzeit,
- die GPS-Koordinaten des Unfallorts,
- die Fahrtrichtung,
- die Fahrzeugidentifikationsnummer,
- der Anbieter des Notrufs sowie
- die Art, wie der Notruf ausgelöst wurde.

Optional möglich ist die Übermittlung von Daten

- zur Anzahl der Insassen und
- ob diese angegurtet waren sowie
- Daten zur Abschätzung der Schwere des Unfalls.

Alle diese Daten erhält eine Notrufzentrale. Die Datenübermittlung erfolgt bidirektional, d.h. für die Insassen wird die Datenübermittlung in Form eines Sprachanrufs aufgebaut. Soweit möglich, ermitteln die Mitarbeiter der Notrufzentrale im Gespräch mit Fahrzeuginsassen das weitere Vorgehen und halten Kontakt bis zum Eintreffen der Rettungskräfte.

Automatisierte Fahrfunktionen

In absehbarer Zukunft folgen hochautomatisierte³ Fahrfunktionen auf Basis der heutigen, weiterentwickelten Assistenzsysteme. Sie übernehmen Aufgaben wie Einparken oder Kolonnenfahrt auf der Autobahn. Folgende Anwendungsfälle stellen die aktuell diskutierten Ausbaustufen automatisierten Fahrens dar:⁴

Teilautomatisiertes Fahren im Stau: Diese Funktion steht bereits heute für Stausituationen auf Autobahnen und Kraftfahrstraßen zur Verfügung. Mit Hilfe weiterer visueller Umgebungsdaten werden in einem Geschwindigkeitsbereich zwischen 0 bis 60 km/h Längs- und Querverführung, also Beschleunigung, Abbremsung und Lenkung, vom Fahrzeug übernommen.

Hochautomatisiertes Fahren auf der Autobahn: Zukünftig wird der Fahrer in einem Geschwindigkeitsbereich zwischen 0 bis 130 km/h die Längs- und Querverführung auf Autobahnen auch über längere Distanzen abgeben können, bis er vom Fahrzeug (wieder) zur Übernahme aufgefordert wird. Sieben von zehn Autofahrern wünschen diese Funktionalitäten.^{5,6} Darüber hinaus werden Fahrzeuge miteinander vernetzt fahren, d.h. mit anderen Verkehrsteilnehmern und mit der Infrastruktur Daten austauschen.

Daneben werden die *Automatisierten Fahrfunktionen für Lkw* erweitert, welche die Fahrzeuge mittels *Elektronischer Deichsel* koppeln und Daten direkt zwischen den gekoppelten Fahrzeugen austauschen können. Konvoi-Zugführerschaft: Wird die Folgefahrt mittels Abstandsregelsystem oder Automatisierter Fahrfunktion um die Möglichkeit der direkten Datenübermittlung zwischen den Fahrzeugen erweitert, so ist der Schritt hin zur Elektronischen Deichsel gemacht. Durch die Vernetzung der Fahrzeuge ist die Echtzeitregelung der gekoppelten Fahrzeuge möglich. Bei der *Konvoi-Zugführerschaft* erklärt sich der Fahrer mit seinem Fahrzeug bereit, die Zugführerschaft für andere Fahrer und deren Fahrzeuge zu übernehmen. Zum Beenden dieser Kopplung kann der Zugführer bereits beim Koppeln angeben, bis zu welchem Ort bzw. für welche Dauer die Zugführerschaft übernommen wird; zum anderen kann durch rechtzeitige Ankündigung mehrere Minuten vor Abkoppeln der Nachfolgende informiert werden. Wegen der geringeren Abstände zwischen den Fahrzeugen lässt sich der Durchsatz an Fahrzeugen pro Straßenkilometer und dadurch die Effizienz des Straßenverkehrs deutlich steigern. Es wird möglich, den Energieverbrauch um ca. 15 % zu senken, da durch die geringen Abstände zwischen den Fahrzeugen der Luftwiderstand der Fahrzeuge sinkt.⁷

Neue Herausforderungen

Durch die Vernetzung wird das Auto Bestandteil des *Internets der Dinge*. Allerdings halten 80 % aller deutschen Internetnutzer das Internet bzw. ihre Daten im Internet für unsicher; knapp 70 % stehen derzeit staatlichen und wirtschaftlichen Stellen im Netz mit Misstrauen gegenüber.⁸

Hinzu kommt, dass die rasante technische Weiterentwicklung des Internets der Dinge in Europa leider nur zeitverzögert mitgestaltet wird: Bei diesem Wettlauf, insbesondere mit den USA, müssen starke Impulse erfolgen. Noch führen Internet-Dienstleister, deren Geschäftsmodelle darin bestehen, Nutzer- und Kundenprofile zu erstellen, um aus diesen Kenntnissen Nutzen zu ziehen. Sie sind fest entschlossen, auch die Teilnahme am Straßenverkehr für sich zu erschließen, denn Verkehrsumfeld, Fahrzeugbedienung und Verhalten im Straßenverkehr ergänzen in hervorragender Weise Persönlichkeitsprofile der Bürger. Von daher ist zu befürchten, dass neben den Grundrechten der europäischen Bürger auch die europäische Autoindustrie gefährdet ist.

Um dem Datenmissbrauch im Straßenverkehr und im Auto vorzubeugen und Misstrauen abzubauen, sind transparente Regeln für Datensicherheit und Datenschutz im und um das Auto unerlässlich. Dazu sind Fragen des zulässigen Speicherns und Übermittels von Daten, der Datensicherheit, des Datenschutzes sowie der informationellen Selbstbestimmung zu klären und rechtlich zu untermauern.

Datenspeicherung und Datenübermittlung

Wie bereits heute werden auch künftig Daten in den Fahrzeugen erhoben. Es wird weiterhin flüchtige und persistent gespeicherte Daten geben. Es wird möglich sein, Daten aus dem Fahrzeug zu senden oder abzurufen. Der *Verhältnismäßigkeitsgrundsatz* erfordert, dass bei Datenspeicherungs- und -Daten-

übermittlungsvorgängen die Grenzen, der Umfang und die Lösungsfristen für die betreffenden Daten klar und zwingend festgelegt und auch technisch durch entsprechende Voreinstellungen gewährleistet werden. Es muss klar erkennbar sein, welche Folgen eine *Einwilligung* der Betroffenen in die Erhebung, Speicherung und Übermittlung der Daten hat. Hierzu muss der Umfang dieser Daten transparent sein. Zudem muss gewährleistet werden, dass Datenübermittlungsvorgänge in jeder Hinsicht *freiwillig* erfolgen und die Betroffenen solche Systeme aktivieren und deaktivieren können.

Datensicherheit

Schließlich ist auch durch rechtliche, technische und organisatorische Regelungen und Maßnahmen zu gewährleisten, dass die Daten im Fahrzeug nicht gefälscht, manipuliert oder unbefugt verwendet werden können. Die Gefahren, die durch eine Manipulationsmöglichkeit der Datenverarbeitung für den Straßenverkehr entstehen, müssen durch einen Datensicherheitsstandard bereits bei der Fahrzeugzulassung nachprüfbar vermieden werden. Klare technische und organisatorische Maßnahmen sind in die Entwicklungs- und Herstellungsprozesse aufzunehmen. Eine besondere Herausforderung stellt in diesem Zusammenhang die Aktualisierung von Software dar – insbesondere jener, die für die Sicherheit der zu verarbeitenden Daten und Prozesse nötig ist.

Datenschutz

Die oben genannten Systeme und Funktionen, mit denen bei Unfällen automatisch Hilfe herbeigerufen werden kann, die Unfälle vermeiden oder deren Folgen mindern können, sind richtig und wichtig. Damit diese elektronischen Assistenten wie perfekte Beifahrer Hilfe rufen, vor Gefahren warnen oder in kritischen Situationen wie ein Fahrlehrer eingreifen, benötigen sie die Daten aus dem Verkehrsumfeld und aus dem Fahrzeug selbst. Von diesen Assistenten erwarten wir jedoch, dass sie ohne unsere Erlaubnis keine Informationen über Ort, Zeit, Fahrzeugzustand, Geschwindigkeit, Insassen, Regelverstöße, starkes Bremsen etc. an wen auch immer weitergeben. Fahrzeugführer und Fahrzeughalter müssen selbst entscheiden können, mit wem ihr Fahrzeug wie kommunizieren soll, und diese Entscheidung selbstständig und möglichst einfach umsetzen und ändern können. Das gilt natürlich auch für Assistenten, die vom Fahrzeughersteller oder zunehmend auch Internetanbieter für das Auto angelernt wurden:

- Wie im Berufsleben darf auch das Fahrzeug als Assistent nicht von einem geschätzten Mitarbeiter zu einem *inoffiziellen Mitarbeiter* einer anderen Firma werden.
- Genauso wenig darf sich eine zuverlässig arbeitende, automatisierte Fahrfunktion zu einem Autopiloten entwickeln oder gar als *Autospion* missbraucht werden.

Informationelle Selbstbestimmung

Alle erhobenen, gespeicherten und übermittelten Daten im Fahrzeug sind personenbezogene Daten im Sinne des § 3 Abs. 1

BDSG, da sie Einzelangaben über den konkreten Fahrer und Halter liefern oder zumindest bei bestimmten Empfängern mit anderen Daten zur Identifizierung des Betroffenen zusammengeführt werden können, sodass der Betroffene bestimmbar ist (personenbeziehbare Daten). Die Fahrdaten gehören dem Fahrzeugführer, die Fahrzeugzustandsdaten gehören dem Fahrzeughalter und ggf. auch dem Fahrzeugführer. In deren Hoheitsbereichen und Verfügungsberechtigung müssen die Daten des Fahrzeugs auch verbleiben. Die Betroffenen selbst müssen entscheiden können, wer ihre Daten erhält und wie sie gespeichert, verarbeitet oder anderweitig genutzt werden. Bei all diesen Datenverarbeitungsvorgängen besteht sonst die Gefahr eines Eingriffs in das informationelle Selbstbestimmungsrecht von Fahrer und Halter. Dabei spielt eine große Rolle, dass den Staat eine Pflicht trifft zum Schutz des unantastbaren Kernbereichs privater Lebensgestaltung vor jeder Verletzung des Rechts auf informationelle Selbstbestimmung und der Ausprägung als Recht der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Das hatte das Bundesverfassungsgericht bereits im Jahr 2008 im Urteil zur Verfassungswidrigkeit der *Online-Durchsuchung* zum Ausdruck gebracht. Ein solcher Kernbereich privater Lebensgestaltung ist bei der (privaten) Nutzung des Autos zu sehen.

Aufgrund der Reichweite eines solchen Eingriffs in das Recht auf informationelle Selbstbestimmung muss gesetzlich vorgegeben werden, welche Daten konkret übermittelt werden dürfen, wem diese Daten zur Verfügung gestellt werden und zu welchem konkreten Zweck dies geschieht. Damit die Betroffenen in der Lage sind, die Verwendung der Daten entsprechend ihrer Rolle im jeweiligen sozialen Kontext selbst zu steuern, bedarf eine Änderung dieses Zwecks stets ihrer Erlaubnis. Auch Voreinstellungen zur Löschung der Daten müssen gesetzlich festgelegt werden.

Zugriff auf diese Daten dürfen Dritte nur dann erlangen, wenn sie per Gesetz dazu berechtigt sind oder/und vom Fahrzeugführer bzw. Fahrzeughalter eine entsprechende Beauftragung erhalten. Die Beauftragung muss ohne rechtlichen oder wirtschaftlichen Zwang erfolgen.

Umsetzung von Datenschutz durch *Privacy by Design*

Autofahrer müssen die Möglichkeit erhalten, das Fahrzeug datensicher und datengeschützt zu betreiben. Diese Forderung wurde auf der Konferenz *Datenschutz und Datensicherheit im vernetzten Auto* deutlich betont.⁹ Im Folgenden werden Vorschläge anhand konkreter, praktikabler technischer Lösungen für das Kraftfahrzeug gezeigt. Mit diesen ist bereits bei der Konstruktion und Herstellung von Autos sichergestellt, dass beispielsweise der Grundsatz *Privacy by Design* erfüllt werden kann.

Grundsätzlich müssen Fahrer und/oder Fahrzeughalter selbst entscheiden können, ob und wenn ja wer welche Daten aufzeichnen und verwerten darf. Es reicht nicht aus, dass der Betroffene nur über Datenerhebungen und -übermittlungen informiert und damit vor vollendete Tatsachen gestellt wird. Vielmehr muss zumindest für bestimmte Bereiche der personenbezogenen Fahrzeugdaten die Einwilligung des Betroffenen in die Datenverarbeitung erklärt werden.

Dieses Prinzip lässt sich durch die bereits heute in den Fahrzeugen existierenden großzügigen Anzeigemöglichkeiten im Cockpit transparent umsetzen. Mit einer durchdachten Mensch-Maschine-Interaktion können Datenschutzeinstellungen rasch getroffen werden. Im Sinne von *Privacy by Default* sollten Standardeinstellungen realisiert werden, welche hohen Anforderungen des Datenschutzes genügen. Das Prinzip kann dann als erfüllt gelten, wenn bei Motorstart keine Daten außer den gesetzlich vorgeschriebenen (OBD¹⁰ und eCall) erhoben werden (Abbildung 1):

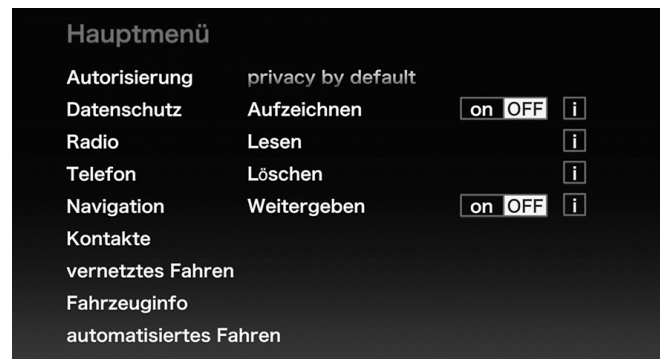


Abbildung 1: *Privacy by Default, Standardeinstellung – keine Datenerhebung außer gesetzlich vorgeschriebenen Daten*

Darüber hinaus muss jeder Fahrzeugnutzer die Freiheit haben, die Einstellungen individuell an seine Bedürfnisse anzupassen. Da Fahrzeuge von verschiedenen Fahrerinnen und Fahrern gefahren werden und sie eigene Datenschutzeinstellungen treffen können müssen, sind Überblick und Kontrolle über die auf den jeweiligen Fahrer bezogenen Daten auf einfache Art und Weise mit wenigen Bedienschritten nötig. Hierfür ist eine Anmeldung (Authentifizierung) der Person am Fahrzeug vorzusehen, nach der die gewünschten Einstellungen vorgenommen werden können (Abbildung 2). Durch geeignete Authentifizierungsverfahren kann auch die Forderung nach Anonymisierung bzw. mindestens Pseudonymisierung der folgenden Datenaufzeichnung, Datenweitergabe und Datenverarbeitung erfüllt werden.



Abbildung 2: *Authentifizierung von Fahrern zur Aktivierung individueller Einstellungen mit Datenschutzrelevanz*

Auch die Kontrolle über Aufzeichnung, Anzeige, Löschung und Weitergabe der bei den Fahrten entstandenen Daten lässt sich mit geringem Aufwand umsetzen (Abbildung 3). Ob bspw. teilweise die Aufzeichnung von Daten deaktiviert wurde, kann durch hierarchische Anzeige in den gewählten Einstellungen

leicht verständlich dargestellt werden. Welche Datenkategorie konkret deaktiviert wurde, lässt sich in gleicher Weise anzeigen.



Abbildung 3: Aktivierung, Deaktivierung und Anzeige individuell getroffener Einstellungen mit Datenschutzrelevanz

Zu jeder möglichen Einstellung muss es möglich sein, Informationen über deren Inhalt und Auswirkung zu erhalten (Abbildung 4).

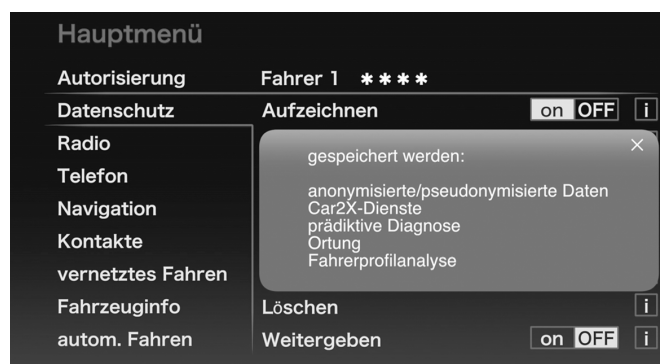


Abbildung 4: Informationsmöglichkeit über die getroffenen Einstellungen

Bevor personenbezogene Daten das Fahrzeug verlassen, muss der jeweilige Fahrer hierüber informiert werden und sich mit der Datenübermittlung einverstanden erklären. Darüber hinaus muss die Möglichkeit gegeben sein, einer Weitergabe von Daten ganz oder teilweise zu widersprechen. Dazu gehört, dass bereits aufgezeichnete Daten ganz oder teilweise gelöscht werden können (Abbildung 5).



Abbildung 5: Teilweises Löschen aufgezeichneter Daten

Der Grundsatz *Privacy by Design* beschränkt sich allerdings nicht auf die Entwicklung technischer Lösungen und deren Integration

in Systeme, sondern er verpflichtet Technologieentwickler und -hersteller bereits im Planungsprozess zur Prüfung darüber, ob und wie die Mengen personenbezogener Daten auf das absolut erforderliche Minimum beschränkt werden können. Gemäß Datenschutzgrundverordnung¹¹ muss der Datenschutz während des gesamten Lebenszyklus der Technologie gewährleistet sein: von der frühesten Entwicklungsphase über ihre endgültige Einführung und Verwendung bis zur endgültigen Inbetriebnahme. Durch transparente Prozesse, wie die hier dargestellte Fahrer-Fahrzeug-Interaktion, können zum einen die Anforderungen der zukünftigen europäischen Datenschutzgrundverordnung eingehalten und gleichzeitig das Vertrauen in Innovationen geschaffen oder erhalten werden.

Rechtlicher und wirtschaftlicher Druck

Fahrer und Halter von Fahrzeugen dürfen weder rechtlich noch wirtschaftlich dazu gezwungen werden, ein System zur Datenübermittlung zu betreiben. Ihnen muss die Möglichkeit eingeräumt werden, diese Systeme freiwillig zu aktivieren oder zu deaktivieren. Dies bedeutet, dass das System weder gesetzlich zwingend vorgeschrieben werden noch seine Verwendung als Voraussetzung für wirtschaftliche Vergünstigungen (beispielsweise Versicherungstarife) verwendet werden darf. Die Nichtnutzung der Systeme darf auch nicht durch wirtschaftliche Nachteile (beispielsweise ungünstigere Versicherungstarife) sanktioniert werden.

Rechtliche Regelungen

Die Rahmenbedingungen für die gesellschaftspolitischen und sozialen Belange, die mit dem technischen Fortschritt einhergehen müssen, wurden bisher nur unzureichend oder gar nicht angepasst. An den bekannten Beispielen ABS und ESP wird jedoch deutlich, welche automatischen Eingriffe in das Fahrverhalten bereits heute gesellschaftsfähig sind.

Um Fehlentwicklungen entgegenzutreten und gleichzeitig die Akzeptanz in technische Innovationen seitens der betroffenen Fahrzeughalter und Fahrer zu stärken, sind wirksame Regelungen für Datenschutz und -sicherheit im Auto – vergleichbar denen für Verkehrssicherheit und Umweltschutz – auf europäischer und nationaler Ebene gefordert.

Solche Maßnahmen sind aufzunehmen

- in das Wiener Übereinkommen über den Straßenverkehr (Kontrollierbarkeit der Datenverarbeitung)
- in eine horizontale Richtlinie für die UN/ECE-Regelungen für Straßenfahrzeuge
- in die EU-Verordnung über die Betriebserlaubnisse von Straßenfahrzeugen
- in die Straßenverkehrs-Zulassungs-Ordnung StVZO
- Datenschutz im Auto darf nicht durch nachträgliche Änderungen im Fahrzeug beeinträchtigt werden: „Fahrzeuge müssen in straßen- und umweltschonender sowie daten-

sicherer und datengeschützter Weise gebaut sein und in dieser erhalten werden“

- sowie in neuen Standards zu *Privacy by Design* umzusetzen.

Die Chancen zur zukünftigen Gestaltung eines sichereren, effizienteren und umweltschonenderen Straßenverkehrs bei gleichzeitig sicheren und geschützten Daten¹² sollten umgehend genutzt werden. Fahrer und Gesellschaft müssen im Fahrzeug wie im Straßenverkehr auf Datensicherheit und -schutz vertrauen können. *Datensicherheit und Datenschutz* sind zukünftig nicht nur Qualitätsmerkmale für Produkte, sondern schaffen Vertrauen in die Marktwirtschaft und sind damit eine der grundlegenden Voraussetzungen für die *automobile Demokratie* von heute und morgen.

Rolle der Sachverständigen

Kraftfahrzeugingenieure und -sachverständige sind die geeigneten Ansprechpartner, um die notwendigen Hausaufgaben transparent und gemeinsam mit der Politik zu erledigen. Gleichzeitig sind sie als neutrale Experten geeignete Ansprechpartner für die Bürger, um sie zu informieren. Die Sachverständigen sind künftig in die Lage zu versetzen, bezüglich des Datenaustauschs solcher Funktionen grundsätzlich immer auch deren Übereinstimmung mit Datensicherheits- und Datenschutzerfordernissen zu überprüfen. Dabei ist eine effektive und effiziente Integration dieser Prüfung in die Hauptuntersuchung unabdingbar. Die genannten Anforderungen sind in Zusammenarbeit zwischen Sachverständigenwesen und Fahrzeugherstellern bereits in der Fahrzeughomologation¹³ zu berücksichtigen. Auf diesem Weg kann und wird das Sachverständigenwesen wesentlich dazu beitragen, sichere, saubere und datengeschützte Mobilität zu fördern und dauerhaft zu erhalten.

Fazit

Automatisierte Fahrfunktionen haben die Besonderheit, dass sie dem Fahrer zeitweise die Verantwortung für die Fahraufgabe abnehmen können. Bei Nutzung automatisierter Fahrfunktionen

steht damit in kritischen Situationen der Fahrer als Rückfallebene zur Vermeidung von Unfällen nicht oder nur eingeschränkt zur Verfügung. Der Fahrzeugsicherheit, deren Genehmigung, Erhalt und deren regelmäßiger, unabhängiger Prüfung kommen damit noch größere Bedeutung zu. Datensicherheit und Datenschutz müssen im Auto den gleichen Stellenwert bekommen, wie heute Verkehrssicherheit und Umweltgerechtigkeit. Datensicherheit und Datenschutz sind deshalb bereits beim Design des Autos zu berücksichtigen und über dessen Betriebsdauer sicherzustellen.

Anmerkungen

- 1 Continental AG: *Continental Mobilitätsstudie 2013*, S. 14. http://www.continental-corporation.com/www/download/presseportal_com_de/themen/initiativen/ov_mobilitaetsstudien_de/ov_mobilitaetsstudie_2013/download_channel/praes_mobilitaetsstudie_de.pdf
- 2 Bundesministerium für Verkehr Bau und Stadtentwicklung (BMVBS): *Information an die EU-Kommission: IVS-Maßnahmen, die für den folgenden Fünfjahreszeitraum geplant sind*, August 2012, S. 61–63. http://www.bmvi.de/SharedDocs/DE/Anlage/VerkehrUndMobilitaet/Strasse/ivs-massnahmen.pdf?__blob=publicationFile
- 3 *Hochautomatisiertes Fahren bezeichnet eine weit gehende Automatisierung, kein voll automatisiertes Fahren.*
- 4 Bundesministerium für Verkehr und digitale Infrastruktur (BMVI): *Verkehr und Mobilität – Automatisiertes Fahren*, 2015. http://www.bmvi.de/DE/VerkehrUndMobilitaet/DigitalUndMobil/AutomatisiertesFahren/automatisiertes-fahren_node.html (Stand: 15.09.2015)
- 5 Continental, 2013, S. 26
- 6 Continental AG: *Continental-Mobilitätsstudie 2015*, S. 26. http://www.continental-corporation.com/www/download/presseportal_com_de/themen/initiativen/ov_mobilitaetsstudien_de/ov_mobilitaetsstudie2015_de/download_channel/mobistud2015_praesentation_de.pdf
- 7 Verbundprojekt KONVOI: *Entwicklung und Untersuchung des Einsatzes von elektronisch gekoppelten Lkw-Konvois. Abschlussbericht, Berichtszeitraum: 01.05.2005 bis 31.05.2009*. <https://www.tib.eu/suchen/id/TIBKAT:629521301/>
- 8 Bundesministerium der Justiz und für Verbraucherschutz (BMJV); Bundesverband Informationswirtschaft, Telekommunikation und neue Me-



Jürgen Bönninger und Udo Schüppel

Dipl.-Ing. **Jürgen Bönninger**, Studium des Maschinenbaus an der TU Dresden, 1982 verantwortlich für Typgenehmigung beim Kraftfahrzeugtechnischen Amt der dam. DDR und Lehr-tätigkeit an der Hochschule für Verkehrswesen in Dresden, 1990 stellvertretende Leitung der Technischen Prüfstelle für den Kraftfahrzeugverkehr beim DEKRA e.V., 1999 Geschäftsführer der TÜV I DEKRA-Arbeitsgemeinschaft der Technischen Prüfstellen im 21. Jahrhundert, 2004 Geschäftsführer der FSD Fahrzeugsystemdaten GmbH Dresden zur Entwicklung von Prüf-technologien für Fahrzeuge, Mitarbeit in nationalen und internationalen Fachausschüssen.

Dipl.-Psych. **Udo Schüppel**, Studium der Psychologie an der TU Dresden, seit 2008 bei der FSD Fahrzeugsystemdaten GmbH in Forschungsprojekten zur Weiterentwicklung der Kfz-Hauptuntersuchung tätig, Schwerpunkte Unfallforschung und Fahrer-Fahrzeug-Interaktion.

- dien e. V. (BITKOM): Gemeinsame Presseinformation „Sicherheit im Internet erhöhen“, Berlin, 11.02.2014. <https://www.bitkom.org/Presse/Anhaenge-an-Pls/2014/Februar/Presseinfo-BITKOM-BMJV-Safer-Internet-Day-11-02-2014.pdf> mit Anhang „Charts PK Safer Internet Day“, S. 2–3. <https://www.bitkom.org/Presse/Anhaenge-an-Pls/2014/Februar/BITKOM-Charts-PK-Safer-Internet-Day-11-02-2014.pdf>
- 9 Heiko Maas: „Wohin geht die Fahrt? Datenschutz und Datensicherheit im vernetzten Auto“. Bundesministerium der Justiz und für Verbraucherschutz (BMJV), Rede des Ministers zum Safer Internet Day 2015, Berlin, 10.02.2015. http://www.bmju.de/SharedDocs/Reden/DE/2015/02102015_Safer_Internet_Day_2015.html
- 10 OBD ist die Schnittstelle, über die sämtliche Daten ausgelesen werden.
- 11 Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, tritt voraussichtlich 2018 in Kraft
- 12 Vgl. z. B. Artikel 10 der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates: Richtlinie zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern. <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32010L0040&from=EN>
- 13 Verfahren der Zulassung eines neuen Fahrzeugtyps für den Verkehr in einem Staat oder einer Gruppe von Staaten



Beate Blättner, Elisabeth Hintz, Werner Winzerling

Erprobung eines sozialen Netzwerkes für die Unterstützung von Familien

Bisher gelten digitale Medien in der Präventionsforschung primär als Risikofaktoren, da sie körperliche Inaktivität unterstützen und gesundheitsfördernde Kommunikationsstrukturen in Familien stören. Gleichzeitig werden jedoch zunehmend Menschen, die „mit dem Internet groß geworden sind“, jetzt Familie. Da liegt es nahe, das Potenzial der digitalen Medien für die Familienarbeit¹ zu untersuchen.

Das Projekt FamTIME² war Preisträger des AOK-Leonardo-Förderpreises für digitale Prävention 2012 und wurde an der Hochschule Fulda im Zeitraum 2012–2014 in einer Kooperation der Fachbereiche Pflege und Gesundheit sowie Angewandte Informatik bearbeitet.

rungen Familien tatsächlich eine Unterstützung durch digitale Medien benötigen. Aus den Ergebnissen der Interviews wurde eine prototypische Web-Anwendung entwickelt und wiederum in Familien evaluiert.

Zielstellung und Herangehensweise

Um die Anforderungen an neu zu entwickelnde digitale Produkte zu analysieren, kann zunächst die Zielgruppe befragt werden. Neben den offensichtlichen Vorteilen hat dieses Vorgehen bei qualitativ neuen Produkten jedoch einen entscheidenden Nachteil, auf den u. a. der Apple-Gründer Steve Jobs hingewiesen hat:

Es ist wirklich schwer, Produkte nach Fokusgruppen zu gestalten. Oft wissen Menschen nicht, was sie wollen, bis du es ihnen zeigst.³

Ein alternatives Vorgehen besteht darin, der Fokusgruppe gleich ein neu entwickeltes Produktkonzept vorzustellen und deren Meinung dazu einzuholen.

In FamTIME wurden beide Herangehensweisen kombiniert und bei der Produktkonzeption abwechselnd angewendet. Dazu arbeiteten Sozial- und Gesundheitswissenschaftlerinnen (in diesem Fall tatsächlich nur Frauen) eng mit Informatikerinnen und Informatikern zusammen.

Zunächst wurde aus der Kenntnis typischer Anforderungen der Familienarbeit ein Interviewleitfaden entwickelt, auf dessen Basis eine Befragung in Familien erfolgte. Damit wurde sichergestellt, dass bei der Befragung alle in der aktuellen Theorie bekannten wichtigen Problembereiche der Familienarbeit Berücksichtigung finden. In den Interviews erfolgte dann ein Abgleich, für welche dieser (in der Theorie bekannten) Anforder-

Interviews

Die Entwicklung des Interviewleitfadens orientierte sich an dem SPSS⁴-Prinzip von Helfferich⁵. Durch vorgegebene Nachfragen wird sichergestellt, dass alle zuvor als relevant identifizierten Themen in den Interviews angesprochen werden, so z. B. zur Mediennutzung, zur Beschreibung des Familienalltags oder zum wahrgenommenen Weiterentwicklungspotenzial digitaler Medien im familiären Kontext.

Die Auswahl der Interviewpartner orientierte sich am *theoretical sampling* der *Grounded Theory*⁶, wonach solange neue Interviewpartner nach dem Prinzip möglichst großer Kontraste ausgewählt werden, bis eine theoretische Sättigung eintritt. Die Datenerhebung und die Datenauswertung stehen in einem permanenten Wechselprozess. Es wurden 14 Interviews mit 34 Personen geführt, die sich u. a. in den Kriterien soziale Lage (z. B. Migrationshintergrund, Bildungsstand und Einkommen), Struktur des Wohnumfeldes (Stadt/Land, Ost/West), Familienform (u. a. Alleinerziehende, Pendlerfamilien, nicht verheiratete Paare, Kinderzahl) und Medienkompetenz unterschieden.

Wesentliche Ergebnisse

Familiale Arbeit wird in den Interviews in vier Formen expliziert, die miteinander verbunden sind:

- In der Gestaltung des Alltags der familialen Gemeinschaft
- im Entwickeln und Ausüben von Ritualen, die eine Sonderrolle im Alltag einnehmen

- in der Planung und Ausübung gemeinsamer Aktivitäten und
- dem In-Kontakt-Bleiben (trotz räumlicher Distanz).

Familienzeit ist die Voraussetzung für familiäre Arbeit. Jedes Familienmitglied muss Zeit investieren, damit der Handlungsplan familiärer Arbeit erreicht werden kann. Die Interviews zeigen, dass es Familien schwer fällt, gemeinsame freie Zeit zu identifizieren, als solche wahrzunehmen und gemeinsam zu nutzen.

Familiäre Arbeit steht mit anderen Arbeitslinien der Familienmitglieder in Konkurrenz um die zur Verfügung stehende Zeit. In den Interviews werden insbesondere die Erwerbsarbeit der Erwachsenen und die Arbeit des Kompetenzerwerbs der Kinder in Schule und Freizeit als Arbeitslinien sichtbar, die Zeit kosten und gemeinsame Zeitfenster rar machen. Die Entgrenzung von Erwerbsarbeit ändert die Konstellation, unter denen familiäre Arbeit geleistet werden kann und wie Freizeit erlebt wird.

Gemeinsame Zeitfenster für kopräesente familiäre Arbeit sind entsprechend mühevoll zu recherchieren, der Organisationsaufwand dafür ist hoch. Wand- und Küchenkalender, digitale Kalender einzelner Familienmitglieder, Zettel oder Pinnwände sollen die Familienmitglieder dabei unterstützen, alle Termine und Verpflichtungen rechtzeitig wahrzunehmen.

Werden mit hohem Organisationsaufwand dann doch gemeinsame Zeitfenster gefunden, fällt es den Familien mitunter schwer, diese mit Inhalt zu füllen. Die Interessen der Familienmitglieder gehen dabei oft auseinander. Soll dann doch etwas gemeinsam unternommen werden, fehlen oftmals Kenntnisse über Angebote, die alle interessieren könnten.

Das Mobiltelefon ist eines der wichtigsten digitalen Medien im Familienalltag, fungiert als multifunktionales Organisationsmedium und steht meist in einem direkten Zusammenhang mit Planungs- und Koordinationsaufgaben.

Überwiegend nutzen die interviewten Familien den Computer als Zugang zum Internet. Sie recherchieren Informationen, tätigen Onlinebanking, kontrollieren E-Mails, ersteigern Gegenstände oder suchen bestimmte Produkte. Neben diesen Möglichkeiten nutzen die Familien Funktionen, die speziell das Web 2.0 auszeichnen, wie soziale Netzwerke, Austauschforen oder Chatkommunikationen (Abbildung 1).

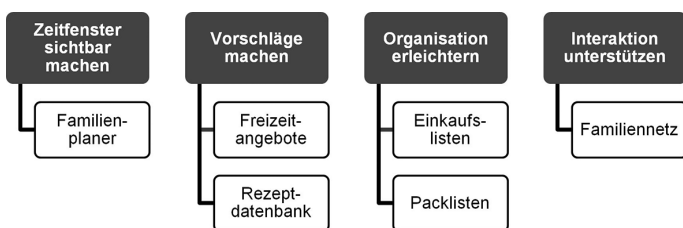


Abbildung 1: Im Projekt unterstützte Bereiche familiärer Arbeit

Die Vorteile der Kommunikation über soziale Netzwerke werden von den Familien in der Einfachheit der Kontaktaufnahme sowie in der zeitlichen und räumlichen Flexibilität der Kommunikation gesehen. Zusammenfassend zeigt sich, dass digitale Medien gut

geeignet sind, familiäre Arbeit durch Koordination, Organisation und Kommunikation zu unterstützen.

Ableitung der Anforderungen

Auf der Basis der aus den Interviews gewonnenen Erkenntnisse wurde eine interaktive Web-Anwendung konzipiert. Um hierfür eine möglichst breite Ideenbasis zu schaffen, nutzte das Projektteam eine gemeinsame Projektlehrveranstaltung mit Studierenden aus den Studiengängen *Gesundheitsförderung* und *Digitale Medien*. In interdisziplinären Kleingruppen planten die Studierenden Funktionen und stellten diese modellbasiert dar. Die Annäherung an die konkrete Ausgestaltung der Funktionen erfolgte wechselseitig durch Überführung der digitalen Funktionen in den realen Kontext und Überführung der realen Situationen in den digitalen Kontext.

In einem zweiten Arbeitsschritt wurden Funktionsvorschläge ausgewählt, die im Projektteam sowohl inhaltlich als auch visuell weiterentwickelt und konkretisiert wurden (Abbildung 2).

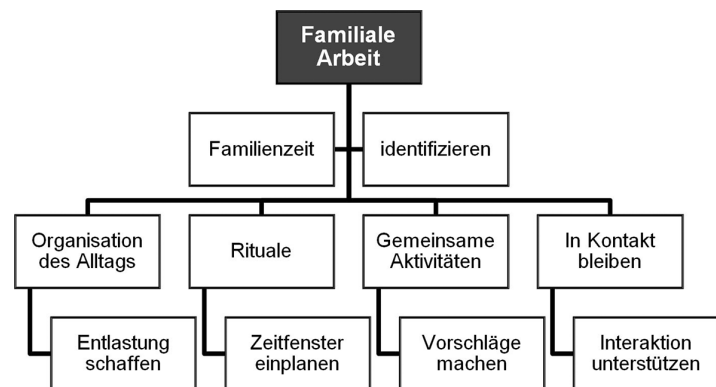


Abbildung 2: Für den Prototyp abgeleitete Funktionen

Gesundheitsbezogene Funktionen

Entsprechend der gesundheitsfördernden Zielsetzung von *FamTIME* wurden für den Prototyp die Funktionen *Freizeitangebote* und *Rezeptdatenbank* beispielhaft umgesetzt und exemplarisch mit Inhalten gefüllt.

Aus inhaltlichen (Partizipation) sowie pragmatischen Gründen (Reduktion des Pflegeaufwandes) werden die Nutzer in die Pflege der Freizeitdatenbank einbezogen. Nutzer bekommen so die Möglichkeit, neue Freizeitangebote einzutragen, vorhandene Freizeitangebote mit Schlagwörtern zu versehen, zu bewerten und zu kommentieren.

Vor Beginn der Recherche wurden Kriterien zur Beurteilung der Freizeitangebote definiert. Neben körperlichen Aktivitäten, die dem physischen und auch mentalen Wohlbefinden dienen, wird das soziale Wohlbefinden mit Freizeitangeboten positiv unterstützt, bei denen das Erleben als Gemeinschaft im Mittelpunkt steht.

Bei der Erstellung der Rezeptdatenbank lag der Fokus noch stärker auf der zu entwickelnden Struktur als bei der Freizeitdaten-

bank. Die Inhalte sollten hier in noch größerem Umfang von den Nutzern selbst erzeugt werden.

Prototyp

Für den *FamTIME*-Prototyp wurden die wesentlichen Anforderungen aus dem Pflichtenheft als interaktive Webanwendung implementiert. Der Prototyp ermöglicht auch die Anbindung anderer Geräte wie Smartphones, Tablets und Smart-TVs.

Die serverseitige Anwendung wurde mit der Java Platform Enterprise Edition (JavaEE) auf Basis einer MySQL-Datenbank entwickelt. Auf der Client-Seite wurde HTML5 und die Bibliothek Backbone.js genutzt (Abbildung 3).

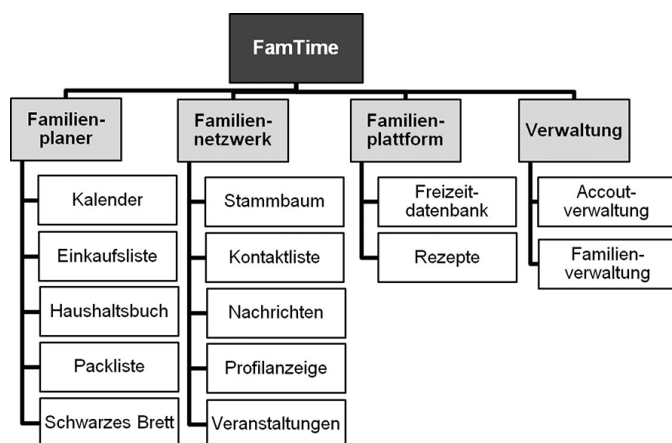


Abbildung 3: Funktionen des *FamTIME*-Prototyps

Evaluation

In einem letzten Schritt wurde der *FamTIME*-Prototyp evaluiert. Dazu wurden zwei Evaluationsmethoden kombiniert:

- das aus der Software-Evaluation stammende *Thinking Aloud* und
- das aus der empirischen Sozialforschung stammende *leitfadengestützte Interview*.

Es wurden 13 Testfamilien ausgewählt. Die Familienmitglieder wurden zu Beginn der Testphase gebeten, die Web-Anwendung zunächst nach eigenen Vorstellungen auszuprobieren. Durch einen visuellen Mitschnitt der Computeroberfläche und die parallel dazu erfolgte Tonaufnahme des Thinking Aloud konnten in der nachfolgenden Datenauswertung die Aktionen der Familienmitglieder nachvollzogen werden. Dann wurden die Familienmitglieder gebeten, konkrete Aufgaben auszuführen. Diese Phase der Evaluation diente dazu, Anfangsschwierigkeiten in der Bedienbarkeit des Programms aufzudecken.

Darauf folgte eine 7- bis 10-tägige freie Nutzungsphase, in der es den Familienmitgliedern selbst überlassen war, *FamTIME* auf verschiedenen Endgeräten zu nutzen. Nach dem Ablauf der freien Testung wurde erneut ein Thinking-Aloud-Test durchge-

führt. Hiermit sollten Probleme aufgedeckt werden, die bei der Bedienbarkeit auch nach einer längeren Aneignungsphase noch bestehen.

Ergänzend wurde wieder ein leitfadengestütztes Interview mit den Familien durchgeführt. Die Familienmitglieder wurden so zu einer offenen Erzählung über ihre Erfahrungen mit der Anwendung angeregt.

„Unfertiger“ Prototyp

Durch einen verspäteten Projektstart sowie durch Schwierigkeiten bei der Implementierung musste die bereits vorher terminierte Evaluation in den Testfamilien mit einem geringeren Funktionsumfang als geplant durchgeführt werden. Dies führte einerseits dazu, dass sich bei der anschließenden Befragung der Familien ein Teil der Hinweise auf die noch fertig zu stellenden Funktionen bezogen. Andererseits unterbreiteten die Familien auch eine Reihe sehr nützlicher Hinweise und Anregungen zur Verbesserung und Weiterentwicklung von *FamTIME*.

Möglicherweise ist dies auf einen auch anderswo beobachteten interessanten Effekt bei der Software-Evaluation zurückzuführen.⁷ Gerade „unfertig“ erscheinende Software-Produkte werden von Testern freimütiger beurteilt als bereits allzu perfekt erscheinende Prototypen. Vermutlich hat gerade der (unfreiwillig) „unfertige“ Entwicklungsstand des Prototyps dazu beigetragen, dass die Testfamilien umfangreiche Hinweise zur Weiterentwicklung gegeben haben.

Ergebnisse

Bei der Evaluation stellte sich heraus, dass eine der wesentlichen Erwartungen der Familien die Möglichkeit der Individualisierung von *FamTIME* ist. Die Familien nehmen sich selbst als individuell wahr. Dies führt zu der Anforderung, die Funktionen innerhalb von *FamTIME* individuell anpassen zu können.

Durch den Einsatz von *FamTIME* erwarten die Familien im Familienalltag eine positive Veränderung, insbesondere durch eine leichtere Koordinierung der Familienzeit, so dass beispielsweise wieder mehr gemeinsame Aktivitäten unternommen werden können. Außerdem erhoffen sich die Familien eine Erleichterung bei der Kontaktpflege mit Familienmitgliedern, die nicht im Haushalt leben.

Gleichzeitig deuten die Ergebnisse darauf hin, dass die Aussicht auf eine positive Veränderung im Familienalltag eine der größten Motivationen für die Familien sein kann, eine Anwendung wie *FamTIME* zu nutzen. Die gesundheitsbezogene Funktion, die von den meisten Familien positiv hervorgehoben wurde, war die Suche nach Freizeitangeboten. Sie wird als potentiell sehr hilfreich empfunden. Auch die Funktion der Rezeptsuche wird als sinnvoll eingeschätzt.

Vor allem den Eltern ist es wichtig, dass ein sicherer Umgang mit dem digitalen Produkt gewährleistet wird. Lediglich Familienmitglieder oder enge Bekannte sollen sich hierüber vernetzen

können, um auch Kindern den sicheren Umgang mit *FamTIME* zu ermöglichen.

Software-Auslegung nach dem Grundsatz *Privacy by Design*⁸ eine zusätzliche Akzeptanz für das Produkt erreicht werden.

Nächste Schritte

Vermarktung

Die Konkurrenzproduktanalyse zeigt, dass es bereits Familienplattformen unterschiedlicher Qualität gibt und dass digitale Familienplaner existieren, die eine Ermittlung von gemeinsamen Freizeitphasen unterstützen. Parallel dazu steht die wachsende Zahl sozialer Netzwerke. Der Vergleich zeigt jedoch, dass die bestehenden Produkte (noch) nicht optimal auf die Bedürfnisse von Familien ausgerichtet sind und dass Gesundheitsaspekte keine bzw. nur eine untergeordnete Rolle spielen.

Für eine Marktreife von *FamTIME* sind noch erhebliche Aufwendungen erforderlich. Einem Bezahlmodell in nennenswertem Umfang steht jedoch entgegen, dass *FamTIME* für breite Schichten der Bevölkerung zugänglich sein soll. Ebenfalls nicht direkt nutzbar sind andere, bei sozialen Netzwerken übliche Finanzierungsmodelle, wie die Nutzung (Verkauf) der in *FamTIME* generierten Daten oder ein anwendungsspezifisches Marketing. Ein geeignetes Geschäftsmodell muss demzufolge noch gefunden werden.

Weitere Forschungsansätze

Da Nutzer in *FamTIME* sehr viele private familiäre Informationen teilen, sind ein (sehr) hohes Datenschutz-Niveau sowie die Sicherstellung einer höchstmöglichen Privatheit (*privacy*) von entscheidender Bedeutung. So könnte mit einer konsequenten

Anmerkungen

- 1 Unter Familienarbeit wird hier die „Herstellung von Familie“ (*doing family*) in einer selbst definierten sozialen Gemeinschaft mit Kindern unter 18 Jahren verstanden. Dazu gehören z.B. die Herstellung eines Gefühls von Zugehörigkeit, Erziehungsarbeit und die Organisation des familiären Alltags.
- 2 Blättner, B.; Winzerling, W.; Hintz, E.; Ludolph, M.; Rudloff, M. (2014): *FamTIME – Echtzeit für Familien. Schlussbericht, Forschungsvorhaben im BMBF-Programm IKT 2020, Förderkennzeichen 16SV5958*
- 3 Reinhardt, A. (1998): *Steve Jobs: There's sanity returning (Interview)*. In: *BusinessWeek*, Issue 3579, 25 May 1998, p. 62
- 4 Sammeln, Prüfen, Sortieren und Subsumieren
- 5 Helfferich, C. (2009): *Die Qualität qualitativer Daten. Manual für die Durchführung qualitativer Interviews*. 3. Aufl. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 178 ff.
- 6 Strauss, A. L. (1991): *Grundlagen qualitativer Sozialforschung. Datenanalyse und Theoriebildung in der empirischen und soziologischen Forschung*. München: Fink
- 7 Wong, Y. Y. (1992): *Rough and ready prototypes: lessons from graphic design*. CHI '92, SIGCHI Conference on Human Factors in Computing Systems, p. 83–84
- 8 European Union Agency for Network and Information Security (2014): *Privacy and Data Protection by Design*



Beate Blättner, Elisabeth Hintz und Werner Winzerling

Beate Blättner ist seit 2003 Professorin für Gesundheitsförderung an der Hochschule Fulda und im Vorstand der Deutschen Gesellschaft für Public Health. Nach einem Studium in Pädagogik war sie 12 Jahre in der Gesundheitsbildung und Gesundheitsförderung tätig und promovierte zum Dr. phil.
Kontakt: Prof. Dr. Beate Blättner, Hochschule Fulda, Fachbereich Pflege und Gesundheit, Leipzigerstr. 123, 36037 Fulda

Elisabeth Hintz ist Doktorandin und seit 2009 in Forschung und Lehre in der Hochschule Fulda tätig. Zuvor absolvierte sie ein Masterstudium in Public Health und ein Bachelorstudium in Gesundheitskommunikation.
Kontakt: Elisabeth Hintz, Hochschule Fulda, Fachbereich Pflege und Gesundheit, Leipziger Straße 123, 36027 Fulda

Werner Winzerling ist Informatik-Professor an der Hochschule Fulda. Er hat in Dresden studiert und in Magdeburg promoviert. Vor seiner Berufung war er mehrere Jahre als Projektmanager im IT-Bereich der Deutschen Telekom AG tätig.
Kontakt: Prof. Dr. Werner Winzerling, Hochschule Fulda, Fachbereich Angewandte Informatik, Leipziger Str. 123, 36037 Fulda

forum

Paul-Olivier Dehaye

aus dem Englischen von Birgit Ahlmann, Nils Erik Flick und Eberhard Zehendner, mit einem Nachwort von Nils Erik Flick

Wie ich einen Blick auf die persönlichen Daten werfen durfte, die ein milliardenschweres Unternehmen über mich besitzt

Turn, Inc. ist ein Retargeting-Unternehmen. Es sammelt Online-Datenspuren und nutzt diese Information, um das Privileg zu versteigern, Ihnen Werbeanzeigen einzublenden. Neben anderen Techniken verwendet es Browsercookies und Canvas-Fingerprinting¹, um Ihren Browser – und damit letztlich sogar Ihre Identität – eindeutig zu identifizieren.

Das Safe-Harbor-Abkommen² gibt allen Bürgern und Einwohnern der EU das Recht, die eigenen persönlichen Daten bei Unternehmen wie Turn einzusehen.³ Im April 2015 bat ich Turns damaligen Anwalt Max Ochoa⁴ (erreichbar über privacy@turn.com), mir alle Daten zu übermitteln, die bei Turn vorgehalten werden und zu meinen Gerätekennungen (etwa Cookies und Apple-Werbekennungen,⁵ siehe unten) gehören. Turn stellte sich zunächst gegen dieses Ansinnen, gab aber schnell nach, als ich es zu verklagen begann. Damit sollte es jetzt jede.r leichter haben, an die eigenen Daten zu kommen. Weiter unten erkläre ich, wie es gemacht wird.

Anfängliche Anfragen per E-Mail

Obwohl er mir versicherte, Turn nähme die Privatsphäre von Verbrauchern ernst, erhob Ochoa drei Einwände, um Turns gesetzlichen Verpflichtungen nicht nachkommen zu müssen.

Sein erster Einwand war im Grunde eine Irreführung: „Turn liefert maßgeschneiderte Werbung unter Verwendung ausschließlich nicht persönlich identifizierbarer Information und sammelt keine persönlich identifizierbare Information (PII) als Teil dieses Prozesses.“ Das Konzept der persönlich identifizierbaren Information entspringt der US-Gesetzgebung und soll Identifizieren des von Nichtidentifizierendem sauber abgrenzen; es ist zudem branchenspezifisch zu interpretieren. Eigentlich war der Begriff bereits überholt, als er ins Gesetz geschrieben wurde. Er wies Anwälten und Technologie-Experten nämlich, so wie sich die Technologie entwickelte, einen sicheren Weg, die im Gesetz festgelegten Schranken zu umgehen: Cookies sind im Web bessere Identifikationsmerkmale als die meisten Vor- und Nachnamenskombinationen. Aus europäischer Sicht ist das Konzept ohnehin reine Fiktion, da die EU-Bestimmungen zum Schutz persönlicher Daten keine bestimmten Identifizierungsmethoden angeben.

Ochoas zweite Abwehr bestand darin, mir anzubieten, aus Turns Tracking durch ein Opt-out auszusteigen. Natürlich habe ich nicht angebissen.

Seine dritte Antwort war, Turn könne nicht sicher sein, dass die Kennung mir gehöre. Ich bot viele Wege an nachzuweisen, dass ich tatsächlich Besitzer dieser Geräte war: ein Bild mit meinem Gesicht nahe der Geräte, Originalrechnungen, sogar Tausende von Meilen bis zu Turns Büros in Redwood City zu reisen (ich plante ohnehin einen Trip in die Bay Area). Nichts davon verfiel.

Schließlich kündigte ich Ochoa im September 2015 meinen nächsten Schritt an: eine formale Beschwerde. Er antwortete mir ziemlich zuversichtlich:

Paul-Olivier, es ist natürlich Ihr gutes Recht, das zu tun. Aber wie bereits erklärt haben wir, wenn uns eine Person eine Kennung schickt, keine Möglichkeit zu validieren, dass diese von einem Gerät dieser Person kommt. Es könnte eine nicht rechtmäßig erlangte Kennung von einem anderen Gerät sein. Wir berücksichtigen daher nur Anfragen von Strafverfolgungsbehörden gemäß einem gültigen Gerichtsbeschluss. Viele Grüße, Max⁶

Ich muss zugeben, dass ich ein wenig schockiert war. Ochoa deutete damit an, dass ich ein Dieb sein könnte, und dass Turn lieber mit Strafverfolgungsbehörden zusammenarbeitet als einen Ausgleich für seine Fähigkeiten zur Datensammlung zu schaffen, etwa durch Bemühungen um Transparenz.

Ist Turn noch an Safe Harbor gebunden?

Ende September 2015 reichte ich meine Beschwerde beim Better Business Bureau ein.⁷ Das ist ein privates Schiedsgericht, das von Turn beauftragt ist, derartige Beschwerden zu klären. Dieses Verfahren ist für Privatpersonen kostenfrei (Turn bezahlt) und stellt die erste Instanz im Rahmen der vom Safe-Harbor-Abkommen vorgesehenen Selbstregulierung dar.

Am 6. Oktober 2015 erklärte der Europäische Gerichtshof (EuGH) im Zuge eines von dem österreichischen Staatsbürger Max Schrems angestregten Verfahrens⁸ die Entscheidung der EU-Kommission für ungültig, der rechtliche Rahmen von Safe Harbor böte den glei-

Paul-Olivier Dehaye

Paul-Olivier Dehaye, SNSF (Swiss National Science Foundation) Professor am Institut für Mathematik der Universität Zürich, publizierte den englischen Originaltext dieses Beitrags in seinem Blog.¹⁶ Sowohl seine Originalveröffentlichung als auch Übersetzung und Nachwort stehen unter CC-BY-SA-Lizenz (Attribution-ShareAlike).

chen Schutz wie EU-Datenschutzbestimmungen.⁹ Dies störte erst einmal den Vorgang, den ich gerade angestoßen hatte: das *Better Business Bureau* schien willens, die Sache völlig fallenzulassen.

Allerdings müssen Privatunternehmen auf US-Seite im Rahmen von Safe Harbor jährlich Verpflichtungen gegenüber ihren Kunden eingehen. Die EU-Entscheidung hat daran nichts geändert, und entsprechend kündigte die FTC (Federal Trade Commission)¹⁰ auf ihrer Website die Fortsetzung des Programmvollzugs an. Als ich darauf hinwies, erklärte sich das *Better Business Bureau* nach ein paar Wochen bereit, ein Verfahren zu eröffnen.

Das Safe-Harbor-Verfahren gegen Turn

Sobald das Verfahren erst einmal ernsthaft in Gang gekommen war, erwies sich der Mediator als äußerst professionell. Es wurde sehr schnell klar, dass *Turn* rechtlich keinen guten Stand hatte. *Turn* fragte an, ob ich bereit sei, eine eidesstattliche Erklärung zu unterzeichnen, der gemäß mir die Geräte gehörten, deren Kennungen ich ihnen geschickt hatte. Ich stimmte bereitwillig zu (rückblickend wäre es natürlich geschickter gewesen, diesen Schritt bereits vor Monaten selbst zu unternehmen). Als *Turn* die Erklärung übersandt hatte, zeigte sich, dass sie eine zusätzliche Klausel eingebaut hatten:

Gemäß den Regeln des vom Council of Better Business Bureaus, Inc., verwalteten Better-Business-Bureau-EU-Safe-Harbor-Streitbelegungsverfahrens stimme ich zu, die Existenz dieser Erklärung und jegliche Information, die ich von Turn Inc. bezogen auf [meine] Kennungen erhalte, vertraulich zu behandeln.

Die Verfahrensregeln des *Council of Better Business Bureaus* enthalten aber keine derartige Klausel.¹¹ Sie verlangen von den Teilnehmern lediglich, ein laufendes Verfahren vertraulich zu behandeln. Ich schickte postwendend eine Antwort, in der ich anmahnte, dies würde mehrere meiner anderen Grundrechte (Recht auf ein faires und öffentliches Verfahren, etc.) verletzen, und unterschrieb die Erklärung einfach, nachdem ich die zusätzliche Klausel durchgestrichen hatte. Scheint geklappt zu haben.

Party when the Case is closed.

8.4 Parties' Treatment of Information Received During the Procedure

The Parties agree that during the course of the Procedure they will treat any information provided to them by the CBBB as information provided exclusively for the purpose of furthering the Procedure, and that they will not disseminate such information to anyone other than those persons directly involved in the handling of the Case. If a Party violates this agreement, the CBBB may refuse to continue processing the Complaint. The purpose of this protection is to maintain a professional, unbiased atmosphere to facilitate a timely and lasting resolution to a Case. If the Party violating the agreement is a Respondent, the CBBB may refer the matter to the appropriate government agency.

8.5 When Information May Be Treated as Proprietary

A Complainant or Respondent may submit information to the CBBB with the request that such information be treated as Proprietary Information and not made available to the other Party. A Party

Nach einigen weiteren Wochen (!) Wartezeit erhielt ich schließlich im Januar 2016 Einblick in meine persönlichen Daten. Also? Was war das große Geheimnis? Eigentlich nicht viel ... *Turn* hat Verträge mit mindestens einem der Unternehmen *Le Figaro*, *Huffington Post*, *Scout24.ch* und *AfriZap* (die Datenflüsse zwischen diesen sind nicht klar, aber ich werde *Turn* um zusätzliche Erläuterungen bitten). Ich scheine einige Male auf diesen Websites auf *Clickbait*s hereingefallen zu sein, einmal auf meiner Arbeitsstelle. Alles in allem nicht weltbewegend. Aber nachdem ich *Turn* zur Herausgabe meiner Daten veranlasst habe, kann nun jeder dasselbe tun – und sollte es dabei leichter haben. Ich ermu-

tige Sie, dies auch zu tun. Wer weiß, vielleicht wird *Turn* später einmal dem Beispiel seines Konkurrenten *Criteo* folgen, der solche Anfragen sehr viel leichter zu machen versucht.¹²

Wie man *Turn* um seine persönlichen Daten bittet

Muster-Schreiben (Originalfassung, da für die USA bestimmt)

Affidavit of ownership of identifiers

I, XXXXXX, hereby solemnly affirm and certify under penalty of perjury as follows:

1. I am citizen of EUROPEAN COUNTRY, and I currently reside in WHEREVER. [Nur eines von beiden braucht ein EU-Land (oder die Schweiz) zu sein.]
2. I am the owner and controller of Apple mobile devices associated with the following Identifiers for Advertisers ("IDFAs"): [Auflisten, siehe unten.]
3. I am the owner and controller of Android mobile devices associated with the following Google Advertising IDs: [Auflisten, siehe unten.]
4. I am the owner and controller of computers running web browsers associated with the following "uid" cookie values set by the turn.com domain: [Auflisten.]

I solemnly affirm and certify under penalty of perjury that the foregoing is true and correct.

DATE – NAME – SIGNATURE

1. Legen Sie eine Sammlung möglichst vieler Ihrer persönlichen Kennungen an: Ihre *turn.com*-Browsercookies (das ist nicht schwer, suchen Sie im Web nach einer Anleitung für Ihren Browser), IDFAs unter iOS (siehe unten),⁵ Google Advertising IDs unter Android (siehe unten). Jede dieser Kennungen sollte eine lange alphanumerische Zeichenkette sein.
2. Unterschreiben Sie eine eidesstattliche Erklärung, dass diese Bezeichner zu Ihren Geräten gehören, und scannen Sie sie ein (siehe oben stehendes Muster).
3. Schicken Sie eine E-Mail mit der ausdrücklichen Bitte um die zu diesen Kennungen gehörenden Daten an *privacy@turn.com*, und fügen Sie den Scan eines amtlichen Ausweises und Ihre eidesstattliche Erklärung bei.
4. Erinnern Sie *Turn* ggf. nach 30 Tagen an seine Verpflichtungen.
5. Hoffentlich hat *Turn* jetzt seine Lektion gelernt und ist seiner Auskunftspflicht nachgekommen. Wenn nicht, legen Sie Beschwerde beim *Better Business Bureau*¹³ oder bei der *FTC*¹⁴ ein (denn in diesem Fall liegt augenscheinlich fortgesetztes pflichtwidriges Verhalten vor).

Tipps für die Praxis

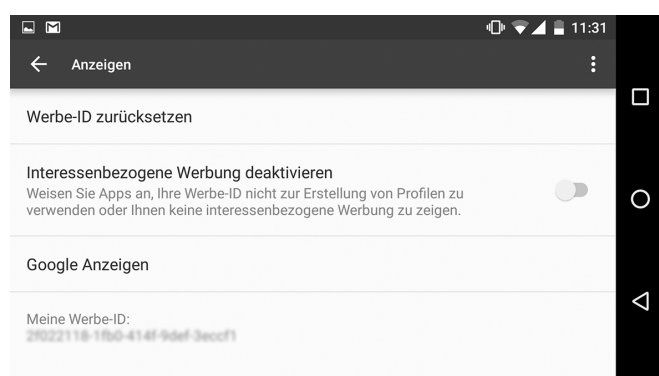
IDFAs ermitteln (iOS)

Installieren Sie die Anwendung „The Identifiers“¹⁵ und schauen Sie unter „Advertising identifier“ nach. (Falls Sie eine bessere Lösung kennen, teilen Sie mir diese bitte mit.)

Google Advertising ID ermitteln (Android)

Schauen Sie auf Ihrem Android-Gerät unter „Google Settings“ > „Ads“ > „Your advertising ID“ nach.

[Deutsche Variante: „Google Einstellungen“ > „Anzeigen“ > „Meine Werbe-ID“]



Die Standard-Einstellungen bei Android 6.0.1

Anmerkungen

- ¹ https://en.wikipedia.org/wiki/Canvas_fingerprinting
- ² https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles
- ³ <https://github.com/pdehaye/safe-harbor>
- ⁴ <https://www.crunchbase.com/person/max-ocha%23/entity>
- ⁵ <https://apsalar.com/blog/2015/06/all-about-idfa/>
- ⁶ Anmerkung: Im Original ist die Rede von "requests from law enforcement authorities pursuant to valid subpoenas". Eine subpoena zwingt im US-Recht eine Person, vor Gericht zu erscheinen und Auskünfte oder Beweismittel herauszugeben. Diese (echte oder juristische) Person braucht nicht Zeuge zu sein.
- ⁷ <https://www.auto.bbb.org/EU-Safe-Harbor-Complaint-Form/>
- ⁸ <http://schrems.eu>
- ⁹ <https://europeanlawblog.eu/?p=2931>
- ¹⁰ <https://safeharbor.export.gov/list.aspx>
- ¹¹ <http://www.bbb.org/council/eusafeharbor/about/rules/>
- ¹² <http://info.criteo.com/mycriteoid>
- ¹³ <http://www.bbb.org/council/eusafeharbor/bbb-eu-safe-harbor-dispute-resolution-program/>
- ¹⁴ <https://www.ftc.gov/faq/consumer-protection/submit-consumer-complaint-ftc>
- ¹⁵ <https://itunes.apple.com/us/app/the-identifiers/id564618183>
- ¹⁶ Paul-Olivier Dehaye: How I peeked at the personal data a billion dollar company holds about me. <https://medium.com/@pdehaye/how-i-peeked-at-the-personal-data-a-billion-dollar-company-holds-about-me-61a446642cd9> (Stand: 19.01.2016)

Nachwort von Nils Erik Flick

Soweit der Erfahrungsbericht von Paul-Olivier Dehaye. Das Vorhandensein von Menüpunkten wie „Advertising ID“ bringt eines auf den Punkt: Das Problem sind nicht allein opportunistische Datensammler, sondern auch schädliche Default-Einstellungen und ausspähungsfördernde Mechanismen in den Systemen, die wir mehrheitlich nutzen. Das Problem betrifft uns jedoch alle, unabhängig von der Computernutzung – der entfesselte Überwachungskapitalismus lässt sich nicht auf das Web beschränken, sondern dringt durch die Digitalisierung des Alltags mehr und mehr in Bereiche vor, in denen selbst wachsamste Verbraucher innen schutzlos sind.

Das Recht bleibt hinter dieser rasanten Entwicklung zurück, auch weil die einzelnen Angriffe auf die informationelle Selbstbestimmung unterschwellig oder diffus sind und daher zu wenige Beschwerden aufkommen – und sicher auch, weil man eine milliarden schwere Industrie nicht abwürgen mag, so unmoralisch sie auch sein mag: *Datenreichtum*.

Das Ironische und Traurige an den existierenden Auskunftsrechten ist: Wer Unternehmen damit Arbeit und Kosten machen will, muss selbst Zeit und Mühe investieren. Wer Datenschutz einfordern will, muss erst einmal bestätigen, dass die Daten richtig sind, und er oder sie stellt damit den Personenbezug erst her (und muss diese sensiblen Daten, die es eigentlich zu schützen galt, womöglich unverschlüsselt übermitteln). Ein Schelm, wer einen *Catch-22*¹ darin wittert! Ähnliches gilt bei dem theoretisch vom Bundesdatenschutzgesetz zugesicherten Recht, sogar Videoaufnahmen aus privaten Überwachungskameras anfordern zu können, auf denen man zu sehen ist – nach § 34 besteht theoretisch ein derart weitreichendes Auskunftsrecht. Doch eine Mitarbeiterin eines Landesdatenschutzamtes deutete mir gegenüber an, ich müsse dem Unternehmen unter Umständen ein Foto zukommen lassen. Na toll!

Trotzdem ist das Schaffen einer Gegentransparenz eine nicht gering zu schätzende Taktik in der Bekämpfung des Daten-Kapitalismus. Wer ein genaues Bild von den Mitteln der Industrie – sowie detaillierte und verbrieft Antworten – hat, kann besser dagegen vorgehen.

Anmerkungen

- ¹ *Catch 22, also Falle 22 oder Trick 22* – das ist die ebenso irrsinnige wie ausweglose Dienstanweisung für das amerikanische Bombengeschwader, der zufolge Bomberpilot Yossarian nur dann von weiteren Einsätzen verschont bleibt, wenn er als verrückt anerkannt wird. Roman von Joseph Heller, 1955

Nils Erik Flick ist Doktorand in der Informatik an der Carl von Ossietzky Universität Oldenburg und seit 2011 FIF-Mitglied. Seine Forschungsschwerpunkte sind Software-Verifikation und formale Sprachen, seine Interessengebiete u. a. Computer-Sicherheit und Kryptologie.

Kontakt: flick@informatik.uni-oldenburg.de



Bericht über das Kolloquium *Emergente Systeme, Information und Gesellschaft*

Die Leibniz-Sozietät der Wissenschaften zu Berlin e. V. ist eine ehrwürdige Organisation, die an die von Gottfried Wilhelm Leibniz im Jahre 1700 gegründete Brandenburgische Sozietät der Wissenschaften anknüpft. Sie bietet Wissenschaftlerinnen und Wissenschaftlern aller Disziplinen ein Forum des Austauschs auf der Basis politischer Unabhängigkeit, weltanschaulicher Pluralität, Interdisziplinarität und Internationalität.

Aus Sicht des FlfF ist besonders interessant, dass im Rahmen der Leibniz-Sozietät im vorigen Juni auf Anregung von Klaus Fuchs-Kittowski ein Arbeitskreis *Emergente Systeme, Information und Gesellschaft* gegründet wurde, der Systemtheorie einerseits und Informatik und Gesellschaft andererseits zusammenbringt. Der Arbeitskreis wird von Wolfgang Hofkirchner (TU Wien), der die systemtheoretische Seite repräsentiert, und mir für den Komplex von Informatik und Gesellschaft geleitet.

Dieser Arbeitskreis wurde am 10. Dezember 2015 in einem eintägigen Kolloquium mit dem Langtitel *Theoria cum praxi et commune bonum: Emergente Systeme. Information und Gesellschaft. Problemstrukturen und Lösungsansätze* im Rathaus Berlin-Tiergarten mit über 60 Teilnehmerinnen und Teilnehmern vorgestellt.

Das Programm war in drei thematische Blöcke mit je drei Vorträgen aufgeteilt, wobei sich am Ende jeden Blocks eine Diskussion anschloss:

I. Die Gestaltung der Informationsgesellschaft im Gesamtzusammenhang

1. Wolfgang Hofkirchner: Eine Informatik für eine globale nachhaltige Informationsgesellschaft
2. Rainer Zimmermann: System, Materie, Information. Probleme der Grundlegung ihrer Begriffe
3. Tomáš Sigmund: Informationsethik – Probleme, Risiken und provisorische Lösungen

II. Entropie – Information – soziotechnische Systeme

4. Werner Ebeling: Entropie – ein Begriff der Physik, der universelle Bedeutung gewinnt
5. Klaus Fuchs-Kittowski: Entstehung und Erhaltung der Information in lebendiger Organisation
6. Peter Brödner: »Information« – allgegenwärtig, doch ungeklärt

III. Probleme der Gestaltung soziotechnischer Systeme

7. Werner Zorn: Über die Schwierigkeit mit Hierarchien
8. Christian Stary: Systeme von Systemen
9. Hans-Jörg Kreowski: Autonomie in technischen Systemen

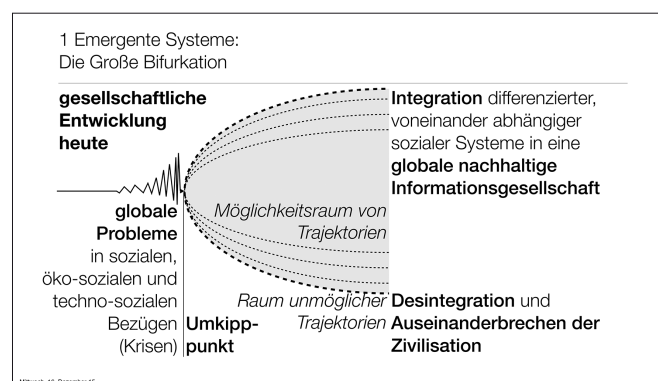
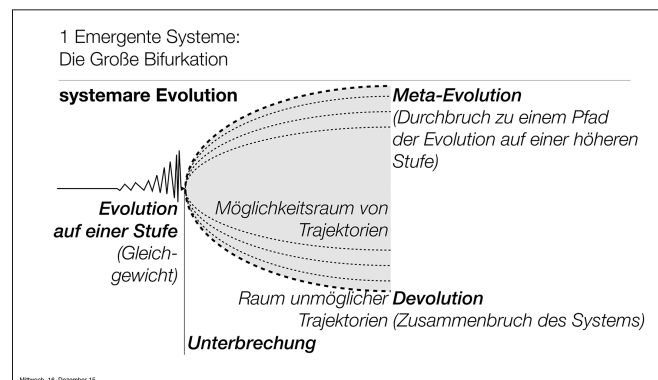
Auf der Webseite der Leibniz-Sozietät findet man unter <http://leibnizsozietat.de/dezember-klassensitzung-emergente-systeme-bericht/>

die Kurzfassungen der Vorträge, die Vortragsfolien und einen ausführlichen Bericht, in dem auch die Diskussionen skizziert sind. Ich werde sicherlich von Zeit zu Zeit über weitere Aktivitä-



H.-J. Kreowski (MLS) und W. Hofkirchner (MLS),
Kovorsitzende des AK „Emergente Systeme“, Foto: D. Linke

ten des Arbeitskreises berichten. Denn eine systemtheoretische Sicht auf das Gebiet Informatik und Gesellschaft kann befruchtend wirken.



Folien aus dem Vortrag von Wolfgang Hofkirchner:
Eine Informatik für eine globale nachhaltige Informationsgesellschaft



Offener Brief für die Beibehaltung von Bargeld

Sehr geehrter Herr Bundesminister Schäuble,

das geplante Verbot von Bargeldtransaktionen über 5.000 Euro sehen wir als den Einstieg in die Abschaffung des Bargelds. Dabei wird mit der Einschränkung von baren Zahlungsmitteln das Ziel der Verbrechensbekämpfung nicht erreicht. Mit Einschränkungen des Bargeldverkehrs verlieren die Bürgerinnen und Bürger Deutschlands schrittweise wichtige Persönlichkeits- und Freiheitsrechte.

Darum fordern wir Sie auf, von einem Verbot von Bargeldtransaktionen über 5.000 Euro abzusehen.

Kernargumente gegen das Vorhaben:

- Euro-Bargeld ist das einzige Zahlungsmittel, das niemand zur Erfüllung einer Geldforderung ablehnen kann, ohne rechtliche Nachteile zu erleiden. Im Euroraum ist Euro-Bargeld das gesetzliche Zahlungsmittel. In Deutschland sind auf Euro lautende Banknoten das einzige unbeschränkte gesetzliche Zahlungsmittel (neben den auf 50 Stück oder im Wert auf 200 Euro beschränkten Münzen).
- Nach Berechnungen von Schattenwirtschaftsfachmann Friedrich Schneider von der Universität Linz hätten die Abschaffung großer Banknoten und das Verbot großer Barzahlungen „nur minimale senkende Effekte auf die Schwarzarbeit oder die Kriminalität“. Die beabsichtigte gesetzliche Beschränkung wäre also nicht verhältnismäßig.
- „Für die Bürgerinnen und Bürger bedeutet jede Einschränkung der Bargeldnutzung einen Verlust an persönlicher wirtschaftlicher Freiheit.“ (Bundesbank-Vorstand Carl-Ludwig Thiele)
- „Die Anonymität des Bargelds ermöglicht es den Bürgern, auch den gesetzestreuen, einen Rest Privatsphäre zu bewahren, der nicht der vollständigen Überwachung oder Überwachbarkeit unterliegt.“ (Handelsblatt)
- Beim privaten Kauf und Verkauf von Gebrauchsgütern sowie auf Märkten ist die Barzahlung essenziell. Auch Musikgruppen werden in der Regel bar aus der Abendkasse bezahlt.
- Elektronische Zahlungsmittel schließen bestimmte Personenkreise aus und sind wegen Transaktionslimits oder technischer Probleme nicht immer einsetzbar.
- Im Sparstrumpf der Bürgerinnen und Bürger befindet sich meist Bargeld, zumal dieses vor Negativzinsen oder Bankenpleiten geschützt ist.
- „Der Bürger soll selbst entscheiden können, ob er lieber Bargeld nutzen oder bargeldlos bezahlen möchte.“ (Bundesbankpräsident Jens Weidmann)

Wir fordern Sie auf, von Begrenzungen von Bargeldzahlungen abzusehen – um die Freiheitsrechte und das Grundrecht auf Privatsphäre aller Bürgerinnen und Bürger zu wahren.

Mit freundlichem Gruß

Rena Tangens

Digitalcourage e.V.

Der offene Brief geht auf eine Initiative auf dem AKtiVCongreZ am 4.-7. Februar 2016 in Hattingen zurück.

Den Brief haben unterzeichnet:

- Digitalcourage e.V.
- Verbraucherzentrale Bundesverband (vzbv) e.V.
- Deutsche Vereinigung für Datenschutz (DVD) e.V.
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FlFF) e.V.
- quintessenz – Verein zur Wiederherstellung der Bürgerrechte im Informationszeitalter
- Arbeitskreis gegen Vorratsdatenspeicherung (AKV)
- dieDatenschützer Rhein-Main

Datenschützer schockiert über sogenannten „Datenschutzschild“

1. März 2016 – Die am 29. Februar von der EU-Kommission vorgestellten Dokumente zum sogenannten EU-U.S.-Privacy Shield (Datenschutzschild) sind in der Deutschen Vereinigung für Datenschutz e. V. (DVD) auf ungläubige Irritation gestoßen. Nach Ansicht der DVD ist der Versuch, die US-Regierung zu Zugeständnissen zu veranlassen, die mit den Anforderungen des Europäischen Gerichtshofs (EuGH) in Bezug auf personenbezogene Datenübermittlungen von Europa in die USA in Einklang stehen, rundherum gescheitert. Am 6. Oktober 2015 hatte der EuGH die Safe-Harbor-Entscheidung der EU-Kommission aus dem Jahr 2000 aufgehoben, weil dabei die Grundrechte auf Privatsphäre und Datenschutz ignoriert werden. Nach einer Analyse der (bisher nur in englischer Sprache vorliegenden) umfangreichen Dokumente zeigte sich der Vorstand der DVD schockiert.

Vorstandsvorsitzender Frank Spaeing: „Es ist für uns nicht nachvollziehbar, wie die EU-Kommissare Anspic und Jouravá die Behauptung aufstellen können, das Datenschutzschild entspräche den Anforderungen des EuGH in Sachen Grundrechtsschutz und Rechtsschutzmöglichkeit. Aus den Dokumenten ergeben sich nicht im Ansatz effektive Begrenzungen der Massenüberwachung durch Sicherheitsbehörden wie die NSA und ebenso keine wirksamen Datenschutzinstrumente gegenüber US-Firmen.“

Ergänzend Vorstandsmitglied Thilo Weichert: „Die materiellrechtlichen Vorgaben des aufgehobenen Safe-Harbors unterscheiden sich nur unwesentlich vom jetzt geplanten Schild. Wer Transparenz sucht, muss – wie bisher bei Safe Harbor – einen Hindernislauf absolvieren, bei dem absehbar das Ziel – die Sicherung eines Grundrechts – nicht erreicht wird. Anstelle von unabhängigen Datenschutzkontrolleuren sollen es das US-Wirtschaftsministerium, die Federal Trade Commission und ein 20-köpfiges „Privacy Shield Panel“ richten, das von der EU-Kommission und dem US-Ministerium besetzt werden soll. Die für die Geheimdienstkontrolle vorgesehene Ombudsperson soll nicht wirklich unabhängig, sondern keinen Weisungen der Geheimdienst-Community unterworfen sein. Eine unabhängige Rechtskontrolle, wie sie Art. 47 der Europäischen Grundrechtecharta fordert, sieht anders aus.“

Die DVD fordert das Europaparlament, die Artikel-29-Arbeitsgruppe der europäischen Datenschutzbehörden und den Europäischen Datenschutzbeauftragten auf, unzweifelhaft klarzustellen, dass wegen der dann weiter andauernden digitalen Grundrechtsverstöße bei Datenübermittlungen in die USA die geplante Angemessenheitsentscheidung der EU-Kommission nicht akzeptiert wird.

Liga protestiert zusammen mit weltweitem Menschenrechtsverband gegen Antiterror-Notstandspolitik Frankreichs

Öffentlicher Protestbrief der FIDH an Staatspräsident François Hollande

29. Februar 2016 – Die *Internationale Liga für Menschenrechte* (Berlin) als eine von 178 Mitgliedsorganisationen des weltweiten Menschenrechtsverbandes FIDH (*Fédération internationale des ligues des droits de l'Homme*, Paris: <http://www.fidh.org/>) ist Mitträgerin eines öffentlichen Protestbriefs vom 26. Februar 2016 an den französischen Staatspräsidenten François Hollande. Der Protest richtet sich gegen die Antiterror-Notstandspolitik der französischen Regierung, besonders gegen die Fortführung des Ausnahmezustands und die weitgehend bürgerrechtswidrigen Maßnahmen, die als Antwort auf die Terroranschläge in Paris im vorigen Jahr ergriffen worden sind.

Die FIDH und mehr als 60 ihrer Mitgliedsorganisationen in aller Welt erklären, dass der Kampf gegen den Terrorismus unbedingt im Rahmen der Menschenrechte geführt werden muss, weil er anderenfalls die Grundlagen der Demokratie und des Rechtsstaats beschädigt. Das würde die Ziele derjenigen befördern, die Terroranschläge gegen unschuldige Menschen verüben, um Angst und Gegenterror zu provozieren. Jede Maßnahme, die die bürgerlichen Freiheitsrechte und damit die Bürgerrechte des Einzelnen in ihrem Kern antastet, kann nur als Verstoß gegen internationale Verpflichtungen Frankreichs, dem europäischen Ursprungsland der Erklärung der Menschenrechte, gewertet werden.

Die Liga teilt diese Einschätzung der FIDH und besonders auch ihre tiefe Besorgnis angesichts der Verlängerung des Ausnahmezustandes und seiner geplanten Verankerung in der französischen Verfassung, denn dies bedeutet eine zeitweise Suspendierung von verfassungsrechtlich garantierten Grund- und Bürgerrechten. Bisherige Informationen und Erkenntnisse deuten darauf hin, dass es bei den fast 3.400 Hausdurchsuchungen und Razzien, die ohne richterliche Genehmigung durchgeführt wurden, zu unangemessener und unnötiger Gewaltanwendung sowie zu gravierenden Fehlentscheidungen kam. Im Zuge des Ausnahmezustandes verhängten die Präfekten etwa 400 Hausarreste gegen einzelne Verdächtige – und zwar auch auf der Grundlage nicht dokumentierter Verdachtsmomente.

Solche Maßnahmen, die die Bewegungsfreiheit der Betroffenen dramatisch einschränken, betrafen – über den engen Rahmen der Terrorismusbekämpfung hinausgehend – zum Beispiel auch Umweltaktivisten. Fast alle diese schwerwiegenden Eingriffe in die Freiheits- und Grundrechte haben Verwaltungsgerichte später bestätigt, deren nachträgliche Kontrolle sich insbesondere bei Razzien und Hausdurchsuchungen unter Bedingungen des Ausnahmezustands als weitgehend ungenügend, ja unwirksam erwiesen hat.

Die Liga kommt in Übereinstimmung mit der FIDH zu dem Schluss, dass die Mittel und Methoden des bestehenden allgemeinen Rechts der aktuellen Situation genügen und dass es daher keines problematischen Antiterror-Sonderrechts bedarf.

Der Verfassungsreform-Entwurf zum Ausnahmezustand und zur Aberkennung der französischen Staatsangehörigkeit für Bürger, die u. a. wegen Tattaten verurteilt wurden, sowie auch der Entwurf zur Reform des Strafverfahrensrechts – die zum Überwachungsgesetz und zu dreißig Jahren Antiterror-Gesetzgebung noch hinzukommen – bergen enorme Gefahren für Menschenrechte und Rechtsstaat. Falls diese Reformvorschläge der Regierung Hollande tatsächlich durchkommen sollten, wird Frankreich eines der wenigen Länder sein, deren Verfassung drei Ausnahmezustandsregelungen vorsieht sowie die Aberkennung der Staatsbürgerschaft. Es steht zu befürchten, dass diese Regelungen in der Bevölkerung und besonders bei den am meisten verletzlichen Menschen ein Gefühl von Willkür und Rechtsunsicherheit verstärken; sie sind geeignet, Stigmatisierung und Diskriminierung zu befördern sowie den sozialen Zusammenhalt in Frankreich noch stärker als bisher schon zu beschädigen.

Die Liga ruft zusammen mit der FIDH dazu auf, den Ausnahmezustand keinesfalls zu erneuern, die Verfassungsreformen unverzüglich zurückzunehmen und den strikten Rahmen der Menschenrechte bei jeder Reform und auch bezüglich der französischen Außen- und Militärpolitik im Zusammenhang mit Terrorismusbekämpfung zu wahren.

Die Liga begrüßt die von der FIDH geplante internationale Untersuchungskommission, die zum Ziel haben soll, die Antiterrormaßnahmen und ihre Auswirkungen auf Menschenrechte und demokratischen Rechtsstaat zu untersuchen und aufzuarbeiten.

Referenz

<https://www.fidh.org/fr/regions/europe-asie-centrale/france/60-organisations-de-la-fidh-appellent-francois-hollande-a-etre>

Wissenschaft & Frieden 1/2016 „Forschen für den Frieden“ mit Dossier „Deutsche Rüstungsexporte – Skandale und Reförmchen“

Friedensbewegte Menschen nutzen zur Information, Diskussion und Argumentation häufig Texte oder Konzepte, die das Ergebnis langen wissenschaftlichen Forschens und Nachdenkens sind. Auch Politiker:innen greifen auf die Expertise von Friedens- und Konfliktforscher:innen zurück, rezipieren deren Texte, laden sie von Zeit zu Zeit zu Anhörungen ein oder geben Studien in Auftrag. Doch darüber, was Friedens- und Konfliktforschung (FuK)

eigentlich ist, wem sie dient, gehen die Meinungen weit auseinander. W&F lud Autor:innen ein, das Thema für Heft 1/2016 zu beleuchten.

Unter dem Titel *Für den Frieden forschen* beziehen in gesonderten Beiträgen Beatrix Austin, Konstanze Jüngling, Mathias Krams und Götz Neuneck Position. Weiter schreiben: Lisa Borgers, Stefan Bösch und Christoph Weller:



Politik, Protest, Forschung – Wie die Friedensforschung entstand; Volker Franke und Lina Tuschling: *Ein bisschen Frieden*; Maria Cardenas: *Mainstreaming Decolonialism? – Zum Mehrwert einer dekolonialen FuK*; FONAS: *Naturwissenschaftliche Friedensforschung in Deutschland*. Unter dem Thema *Konzepte vom Frieden – Vier Friedensinstitute, vier Ansätze* stellt Christoph Marischka die Informationsstelle Militarisierung (IMI) vor, Kathrin Jeske das Institut für Theologie und Frieden (ithf), Chris-

tine Schweitzer das Institut für Friedensarbeit und gewaltfreie Konfliktaustragung (IFGK), J. Christopher Cohrs und Gert Sommer das Forum Friedenspsychologie. In einem fiktiven Streitgespräch beleuchtet das Organisationsteam der *Konferenz von unten* am Zentrum für Konfliktforschung der Marburger Universität die Probleme der Friedens- und Konfliktforschung.

Weitere Themen in W&F: Die Würde des Menschen in schwierigen Zeiten, Streiflichter und Anregungen zur Debatte um die Ukraine, die Forderung nach einem Ökologischen Weltbürgergericht und eine kommentierte Presseschau *Die teure Truppe*, 13 Milliarden € mehr für die Beschaffung und Ausstattung der Bundeswehr.

Deutsche Rüstungsexporte – Skandale und Reförmchen ist der Titel des W&F beiliegenden Dossiers. Jürgen Grässlin, Alexander Lurz und Kerstin Seifert schildern, wie die Ausfuhr von Rüstungsgütern aus Deutschland allzu oft geprägt ist von skandalösen Praktiken und dem fehlenden Willen der zuständigen PolitikerInnen und Behörden, daran etwas zu ändern.

Wissenschaft & Frieden 1/2016 „Forschen für den Frieden“, 7,50€ plus Porto.

W&F erscheint vierteljährlich. Jahresabo 30€, ermäßigt 20€, Ausland 35€, ermäßigt 25€, 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



Andreas Sachs

Smart-TVs im Fokus der Datenschutzaufsichtsbehörden

Das Internet hat viele Bereiche des Alltags bereits durchdrungen und wird von vielen Bürgern als nützlich und selbstverständlich angesehen. Es gibt allerdings noch einen Bereich, der sich lange gegen die Vernetzung „gewehrt“ hat und als DAS Medium der Informationsbeschaffung angesehen wird oder zumindest wurde: der Fernseher.

Konvergenz der Medien

Durch maßgeblich zwei Faktoren hat sich dieser Sachverhalt mittlerweile grundlegend verändert. So besitzen heute die meisten Bürger einen Breitband-Internetanschluss (oder zumindest das, was mit viel Phantasie darunter verstanden werden kann). Gepaart mit einem Flatrate-Preismodell können beliebige Endgeräte dauerhaft mit dem Internet verbunden bleiben. Dies sind die Smartphones, die regelmäßig große Datenmengen mit den angebundenen Cloud-Speichern synchronisieren, die private Cloud zuhause, die einen Zugriff auf die letzten Urlaubsfotos von überall erlaubt oder die Spielekonsolen, die ohne Internetanbindung einen erheblichen Verlust des Spaßfaktors mit sich bringen. Was liegt also näher, als noch ein weiteres Endgerät mit wenigen Klicks über den WLAN-Anschluss des Haushaltes mit der großen weiten Welt zu verbinden. Der zweite Faktor sind die vielen kleinen Anwendungen, die Apps, die bereits die Smartphones so erfolgreich gemacht haben. Für jede Lebenslage, seien es Online-Banking, Shopping, Nachrichten, Soziale Netzwerke, Kochrezepte, Spiele, Liebeskummer, Bewertung von anderen Autofahrern, ... gibt es mittlerweile kleine Helferlein. Manche davon sind derart erfolgreich geworden, dass diese eine millionenfache Verbreitung mit einem Stammkundenkreis gefunden haben. Was liegt also näher, als das Lieblingsspiel oder die soziale Kommunikation nicht mehr auf einem 5-Zoll-Mini-Display, sondern auf einem 40-Zoll-4K-Boliden mit Surround-Sound zu genießen.

Wer sich heute (oder in Bälde im Hinblick auf die Fußball-Europameisterschaft) ein neues Fernsehgerät kaufen möchte, wird feststellen, dass neben der Bildschirmdiagonale und der Bildqualität weitere Features zum Kauf genau eines bestimmten Geräts verführen sollen: Smart-TV, HbbTV, Spracherkennung, Skype, EPG, ... Doch was versteckt sich hinter diesen Begriffen und was bedeutet dies bezüglich des Einsatzes eines technischen Gerätes, das bis jetzt für die anonyme Informationsbeschaffung (und gelegentlich für leichte Kost wie Gesangs- und Schönheitswettbewerbe oder Überlebenstrainings im Dschungel) stand.

Datenschutzaufsichtsbehörde

An dieser Stelle kommt nicht nur, aber auch der Begriff Datenschutz ins Spiel. Dieser ist heute sicherlich für jeden sehr ge-

läufig, zumindest wenn die eigene Daten betroffen sind. Die einen verstehen darunter den Schutz des Rechts auf informationelle Selbstbestimmung, andere ein Relikt aus analogen Zeiten, weitere den ausschließlich technischen Schutz von Daten. Würde man die Frage nach dem Stellenwert für den Bürger stellen, dann könnte möglicherweise folgendes Dilemma festgestellt werden: Den Datenschutz finden viele sehr wichtig – irgendwie. Es soll keine Werbung zugestellt werden, der Staat soll keine Daten (z.B. das Einkommen, die Haushaltsgröße, ...) erheben, die eigenen Daten sollen vor „Hackern“ geschützt werden und wenn der eigene Name gegoogelt wird, sollen am besten keine Treffer erscheinen. Auf der anderen Seite soll es möglich sein, an allen tollen technischen Entwicklungen teilzuhaben – und das kostenlos (oder zumindest sehr günstig): Die Nachrichtenportale im Internet, die sozialen Medien, die Kommunikation mit Freunden und Familie, der Genuss von Musik und Filmen, ... Klappt dies nicht so wie gewünscht, dann kann der Kontakt mit einer Behörde gesucht werden, die sich um den Datenschutz „kümmert“. Nach ein wenig Recherche wird schnell klar, dass dieser offizielle Schritt zuerst ein bisschen komplizierter erscheint, da die Datenschutzaufsicht in Deutschland föderal geregelt ist. Dies bedeutet, dass jedes Bundesland eine eigene Datenschutzaufsichtsbehörde besitzt. Der Freistaat Bayern hat sich hier sogar für eine spezialisiertere Organisation entschieden und die Aufsichtsbehörde in einen öffentlichen Teil (für die Kontrolle des Staates) und einen nicht-öffentlichen Teil (für die Kontrolle der Wirtschaft) geteilt. So kompliziert wie sich das Konstrukt der Aufsichtsbehörden auf den ersten Blick anfühlt, ist es dann aber in der Praxis nicht. Sollte eine Behörde „nicht zuständig“ sein, so wird beispielsweise eine Beschwerde unbürokratisch an die zuständige Aufsichtsbehörde weitergeleitet. Da den Datenschutzaufsichtsbehörden Begriffe wie E-Mail und PGP auch geläufig sind, geht dies (mitunter) auch recht zügig und sicher.

Rechtliche Regelungen für Smart-TVs

Wenn eine Datenschutzaufsichtsbehörde sich einer Aufgabenstellung (z.B. Beschwerde oder Beratungsanfrage) annimmt, dann geschieht dies nicht auf beliebiger Basis oder Sichtweise, sondern immer auf Grundlage von Gesetzen. Diese regeln (mehr oder weniger spezifisch) die Art und Weise, ob und wie die Verarbeitung personenbezogener Daten erfolgen darf. In Deutschland gilt diesbezüglich der Grundsatz „Verbot mit Er-

laubnisvorbehalt“, was bedeutet, dass personenbezogene Daten entweder auf Basis eines konkreten Paragraphen eines Datenschutzgesetzes (hauptsächlich Bundesdatenschutzgesetz und Telemediengesetz) verarbeitet werden oder, indem der Bürger um Erlaubnis für diese Verarbeitung gebeten wird. Die Regelungen unterscheiden auch zwischen dem Verhältnis zweier „Verantwortlicher Stellen“, z.B. Unternehmen, untereinander (wie dies beispielsweise beim Outsourcing an einen Cloud-Anbieter zum Tragen kommt) einerseits und dem Verhältnis zwischen dem Bürger (auch als Betroffener bezeichnet) und einer Verantwortlichen Stelle, z.B. einem Smart-TV-Hersteller, andererseits.

Nutzungsbedingungen

Soll nun ein (neues) Smart-TV angeschafft werden, dann stellt sich auch die Frage, inwiefern eine Verarbeitung personenbezogener Daten stattfindet und wie diese im ersten Schritt auch rechtlich geregelt wird. Mittel der Wahl ist bei Smart-TVs ein zivilrechtlicher Vertrag, auch Allgemeine Geschäftsbedingungen genannt, der auch eine Rechtsgrundlage für eine Verarbeitung personenbezogener Daten darstellen kann. Bei diesem sollte Transparenz das oberste Gebot sein, da dies die Grundlage dafür ist, eine Entscheidung über die Nutzung eines Smart-TV zu treffen. Dass dies in der Praxis nicht zwangsläufig zutrifft, ist auch den Datenschutzaufsichtsbehörden bekannt. Auch stellte sich die grundsätzliche Frage nach den rechtlichen Anforderungen eines Smart-TV in Deutschland. Deshalb haben sich die Datenschutzaufsichtsbehörden in Deutschland, die in ihrem Bundesland einen Hersteller von Smart-TVs (oder eine Niederlassung) haben, entschieden, ein Prüfprojekt zu starten, das zwei aufeinander aufbauende Ziele hatte: Zuerst sollten aktuelle Smart-TVs technisch besser verstanden werden. Darauf aufbauend sollten dann technische und rechtliche Anforderungen an Smart-TVs formuliert werden, die auf Basis der deutschen Datenschutzgesetze eine Richtschnur und eine rote Linie für einen beanstandungsfreien Einsatz von Smart-TVs in Deutschland darstellen sollen.

Das Prüfprojekt

Unter Federführung des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA) wurde ein technisches Prüflabor aufgebaut (bzw. das bestehende Labor an die Smart-TV Prüfung angepasst) und eine Prüfmethodik entwickelt, um vergleichbare Ergebnisse bei mehreren Smart-TVs zu erhalten.

Bei Smart-TVs stellte sich zuerst die Frage, was denn technisch überhaupt geprüft werden soll und kann. Da es bei diesen keine standardisierten Plattformen gibt (auch wenn viele auf einem Linux-Kern aufbauen) und sie zusätzlich als geschlossene Systeme fungieren (ein Zugriff auf das Filesystem bzw. auf eine Shell ist nicht möglich – zumindest wenn keine Sicherheitslücke ausgenutzt werden kann), wurde entschieden, eine dynamische Analyse der Datenflüsse des Smart-TV bei dessen Nutzung durchzuführen. Dazu wird ein Endgerät mittels WLAN an einen Standard-PC angeschlossen, der als Router fungiert. Dies bedeutet, dass sämtliche Kommunikation des Smart-TV mit beliebigen Servern, die über das Internet-Protokoll IP abgewickelt

wird, über die Netzwerkkarte dieses Rechners geht. Durch den Einsatz des Netzwerkanalysetools Wireshark kann so festgestellt werden,

- mit **welchen Servern** (Domainname oder IP-Adresse) **wann** kommuniziert wird, sowie
- **welche Daten** dabei übermittelt werden (sofern nicht verschlüsselt).

Kommuniziert ein Smart-TV verschlüsselt über das SSL/TLS-Protokoll mit einem Server, dann stellt dies ein Problem der technischen Prüffransparenz dar, da die Inhaltsdaten der Internetkommunikation verborgen sind. Dies ist zwar beim Einsatz der Betroffenen aus Gründen der Vertraulichkeit löblich (und auch notwendig), für einen Laboraufbau aber sehr hinderlich. Bei den Analysen wurde auch ein Web-Proxy (BurpSuite Pro) eingesetzt, der als Man-in-the-Middle die verschlüsselte HTTPS-Kommunikation „knacken“ sollte – funktioniert hat dies allerdings bei den aktuellen Smart-TV-Geräten nicht (mehr), da diese wohl aus den Fehlern der Vergangenheit gelernt haben und die Überprüfung der Serverzertifikate nun korrekt implementieren. Da ein Smart-TV im Gegensatz zu einem Smartphone es nicht zulässt, dass eigene selbstsignierte SSL-Zertifikate installiert werden können, beschränkt dieser Sicherheitsmechanismus die Möglichkeiten eines Prüfers. Abbildung 1 zeigt das kleine Prüflabor beim BayLDA.



Abbildung 1: Prüflabor für Smart-TVs beim BayLDA

Die Datenschutzprüfung

Zur Durchführung der Prüfung wurden aktuelle Smart-TV-Geräte benötigt. Dazu wurden die Hersteller von Smart-TVs über die beabsichtigte Prüfung informiert und um ein aktuelles Leihgerät gebeten. Dieser Bitte sind alle 13 Unternehmen nachgekommen und haben auch das Angebot des BayLDA angenommen, bei der Durchführung der Prüfung anwesend zu sein. Die Hersteller wurden so ausgewählt, dass ca. 90 % Marktabdeckung (der Hersteller, nicht des Gerätemodells) erreicht wurden. Die Teilnahme von Vertretern der Hersteller hatte auch den Vorteil, dass bei der Prüfung auftretende Fragen teils schnell geklärt werden konnten sowie dass die transparente und unvoreingenommene Prüfung auch so an diese kommuniziert werden konnte.



Abbildung 2: Die ersten Testgeräte sind eingetroffen

Nachdem die ersten Testgeräte beim BayLDA eingetroffen waren (Abbildung 2) konnte die systematische Prüfung beginnen:

1. Ausgepackt und eingesteckt

Dieses Prüfzenario hatte die Transparenz der Informationen vor Nutzung eines Smart-TV im Fokus. Diese ist auch insofern wichtig, da auf Grund dieser eine Entscheidung über die Verwendung eines Gerätes getroffen werden soll(te). Die Ergebnisse waren allerdings ernüchternd, da nur knapp die Hälfte der Geräte nach Inbetriebnahme überhaupt eine Datenschutzerklärung anbot (Abbildung 3).



Abbildung 3: Kein Betrieb ohne Datenschutzerklärung!

Weniger zurückhaltend war die Verteilung der Geräte, die noch vor Lesen der Datenschutzbestimmungen im Hintergrund eine Internetkommunikation mit dem Hersteller aufgenommen haben (Abbildung 4).

2. Ende des anonymen Fernsehens: HbbTV

Wird ein Smart-TV an das Internet angeschlossen, dann erscheint es noch so, als würde sich beim reinen Anschauen von Filmen und Sendungen nichts geändert haben. Das Smart-TV könnte als kontrollierte Nutzung von Apps oder der Mediathek verstanden werden. Dass dies nicht so ist, liegt auch an einer neueren technischen Entwicklung, die unter dem Namen „Hybrid Broadcast Broadband TV“ (HbbTV) standardisiert wurde. Dies stellt einen Paradigmenwechsel bei der Programmnutzung dar. War es bis jetzt so, dass das Fernsehprogramm als unidirek-

tionaler Empfang des Rundfunksignals eine vollständig anonyme Nutzung zwangsläufig technisch mit sich brachte, ändert HbbTV dies nun vollständig. Es wird ein sogenannter Rückkanal zur Verfügung gestellt, über den das Fernsehgerät aktiv mit beliebigen Servern kommunizieren kann. Technisch ist dies so umgesetzt, dass neben dem Rundfunksignal digitale Zusatzinformationen übertragen werden, die auch eine URL beinhalten. Wie bei Webbrowsern üblich, kann damit auch der Smart-TV über das HbbTV-Protokoll eine Webseite laden, die spezielle Rahmenbedingungen für den Einsatz mit HbbTV umsetzen muss, ansonsten aber mit HTML5, CSS und JavaScript wie bei Webseiten bekannte Entwicklungen ermöglicht. Eine davon ist der Einsatz von Tracking-Verfahren, die es z. B. durch den Einsatz von Cookies ermöglichen, das Nutzungsverhalten eines konkreten Smart-TV zu ermitteln. Dabei greifen wie bei Browsern zwar auch Schutzmechanismen wie die Same-Origin-Policy, die einen Zugriff auf Cookies fremder Domänen unterbinden. Bei den Tests wurde aber trotzdem ein senderübergreifendes Tracking (innerhalb einer Senderkette) festgestellt, bei dem periodisch (ca. jede Minute) ein Aufruf an den Tracking-Server erfolgte und damit die Verweildauer auf einem Sender (zu einer Uhrzeit) sowie der Wechsel zu einem anderen Sender (der Sendergruppe) festgestellt werden konnte. Möglich machen dies wie sonst im Web auch die sogenannten Third-Party-Cookies – nur bei Smart-TVs können diese meist nicht gelöscht werden.

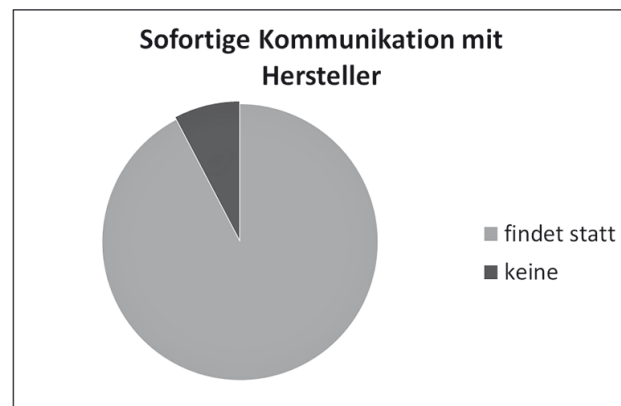


Abbildung 4: T. V. nach Hause telefonieren ...

Wer jetzt der Meinung sein sollte, dies dürfte doch nicht zulässig sein, dem darf die Kurzantwort sehr häufiger und sehr juristischer Diskussionen zu diesem Thema gegeben werden: Es ist unklar. Es gibt das eine Argument, das sagt, dass ein Smart-TV nichts anderes als einen mit dem Internet verbundenen PC darstellt (der auch noch TV kann). Unter dieser Prämisse wären dann die gleichen rechtlichen Anforderungen wie beim Tracking von Webseiten zu stellen. Dies würde bedeuten, dass über den Einsatz von Trackingverfahren informiert werden sowie eine Widerspruchsmöglichkeit vorhanden sein muss. Dass letztere technisch auch bei Webseiten meist nicht funktioniert, da nach einem sogenannten Opt-out weiterhin HTTP-Requests an den Tracking-Anbieter (mit einem kleinen Opt-out-Flag) gehen, sei nur am Rande erwähnt. Das andere Argument sagt, dass ein Anschluss eines Smart-TV, der ja nicht nur HbbTV kann, nicht unmittelbar mit einem PC gleichzusetzen ist. So ist es vorstellbar, dass (per WLAN) nur auf die lokale Filmdatenbank zugegriffen oder ausschließlich YouTube als „smarte“ Applikation verwendet werden soll. In diesem Fall wäre vor dem Aufbau eines internetbasierten Rückkanals, der auch immer IP-Adressen be-

inhaltet, um Erlaubnis zu fragen. Bei der Analyse von zehn Sendern (fünf privat, fünf öffentlich-rechtlich) wurde festgestellt, dass immerhin acht auch eine Datenschutzerklärung hatten, die über den Einsatz von Tracking-Verfahren informierte. Sieben der zehn analysierten Sender setzen Tracking-Verfahren schon ein, bevor die speziellen Möglichkeiten einer HbbTV-Seite (durch Drücken des „Red Buttons“ auf der Fernbedienung) überhaupt genutzt werden. Die Zielsetzung der Trackingverfahren ist offensichtlich: Zum einen soll das Einschaltverhalten ermittelt werden – damit gehören die GfK-Panels, die eine Basis für die Verteilung der Werbeeinnahmen darstellen, bald der Vergangenheit an. Zum anderen ermöglicht HbbTV die Einblendung individueller Werbung auf Basis der Nutzung des Smart-TV. So können passend zur Kochsendung geeignete Weine oder zur Sendung über Bandscheibenvorfälle passende Reha-Maßnahmen beworben werden. Schützen wird sich der Normalanwender davor kaum können, ist doch die Technik intransparent und die geeignete Konfiguration einer Gateway-Firewall im eigenen Hausnetz doch eher etwas für Technik-Enthusiasten.

Ob HbbTV in dieser Form weiterbetrieben werden kann, hängt von der weiteren rechtlichen Bewertung der komplizierten Rahmenbedingungen sowie der Zurückhaltung des Tracking-Verhaltens von Seiten der Fernsehsender ab, die bei einem exzessiven Einsatz einen Vollzug von Seiten der Aufsichtsbehörden geradezu erzwingen würden.

3. Apps bei Smart-TV

Wie bei Smartphones und Tablets gibt es auch bei Smart-TVs Apps, die genutzt, oder moderner ausgedrückt, für ein besseres Nutzererlebnis verwendet werden können. Diese kommen (noch) nicht von Google oder Apple Stores, sondern sind von der Basis so vielfältig wie die technischen Plattformen, auf denen Smart-TVs betrieben werden. Entsprechend unterscheidet sich die Anzahl der Apps, die von wenigen vorinstallierten bis zu Hunderten von Anwendungen reichen. Heruntergeladen werden diese über das Smart-TV-Gerät, aber nicht zwingend vom Smart-TV-Hersteller. So gibt es einen Akteur „App-Store-Betreiber“, der eine eigene verantwortliche Stelle sein kann und in Eigenmächtigkeit Apps für den Download bereitstellt sowie evtl. auch eine Registrierung der Nutzer durchführt.

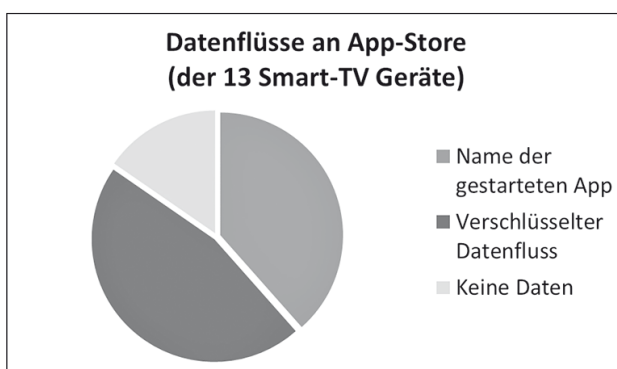


Abbildung 5: Datenschutz verletzt: der App-Store hört mit

Technisch sind die meisten Apps als Web-App umgesetzt (obwohl bei manchen Plattformen auch native Apps möglich sind). Der Start erfolgt dann durch den Aufruf einer der installierten

App zugeordneten URL. Mit dieser findet eine Kommunikation mit dem App-Hersteller, der selbst für den Datenschutz bei seiner App verantwortlich ist, statt. In der Prüfung wurde allerdings bei knapp der Hälfte der Testgeräte festgestellt, dass auch an den App-Store der Start einer App, verbunden mit einer geräte- oder installationseindeutigen ID, übermittelt wurde (Abbildung 5). Damit werden Profile der App-Nutzungen erhoben, die anhand des App-Namens, der Häufigkeit und des Zeitpunkts durchaus nicht uninteressante Aussagen ableiten lassen, beispielsweise die Nutzungshäufigkeit von YouTube oder eines Spieles mit wilden Vögeln.

4. USB-Medien

Smart-TV-Geräte bieten auch umfangreiche Möglichkeiten der Medienwiedergabe aus USB-Datenträgern an. Dies können heruntergeladene Videodateien, MP3-Sammlungen oder die letzten Urlaubsfotos sein. Dazu wird das USB-Medium in einen Slot am Gerät gesteckt, und die Verarbeitung erfolgt lokal am Gerät. Umso überraschender war es, dass bei vier Geräten beim Einstecken und Nutzen der lokalen Mediendateien Datenflüsse stattfanden (Abbildung 6).

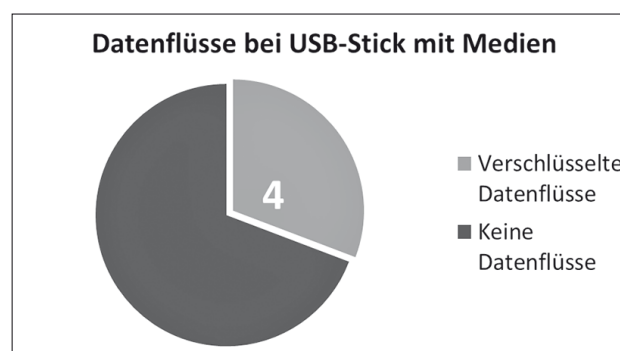


Abbildung 6: Smart-TV beim Ausplaudern erwischt ...

Da diese allerdings mit HTTPS verschlüsselt und Man-In-the-Middle-Methoden mangels Möglichkeit einer Einspielung von eigenen Test-Serverzertifikaten nicht möglich waren, konnten nur heuristische Prüfverfahren angewandt werden, um den Inhalt der Übermittlungen zu erhellen. In der Prüfung wurden beispielsweise viele Grafikdateien mit sehr langen Dateinamen auf einem USB-Stick erzeugt und die Größe der verschlüsselten Datenpakete mit der Größe verglichen, wenn die gleiche Anzahl Dateien mit sehr kurzen Dateinamen auf einem Stick enthalten war. Selbiges wurde mit unterschiedlich großen Mediendateien durchgeführt. Indizien dafür, dass Dateinamen und Inhalte der USB-Medien das Smart-TV verlassen haben, wurden nicht gefunden, da die Größe der verschlüsselten Pakete gleich groß war. Bei einem Hersteller (der übrigens seinen Sitz nicht in Bayern hatte) wurden mit einem mobilen Prüflabor bei dessen Firmensitz die Tests wiederholt – allerdings hatten wir dort das echte Server-Zertifikat erhalten (und nach der Prüfung wieder gelöscht). Damit war es uns möglich, einen Einblick in die HTTPS-Verbindungen zu nehmen (leicht zu machen mit der Burp-Suite). Festgestellt haben wir in diesem Fall, dass statistische Nutzungsdaten des Medienplayers (z. B. Stick ein, Foto ausgewählt, Video ausgewählt), nicht aber Dateinamen oder Inhalte übertragen wurden.

5. Aufnahmen von Fernsehsendungen

Fast alle Smart-TVs haben die Möglichkeit, Fernsehsendungen auf internen oder externen Festplatten aufzuzeichnen. Wie bei den USB-Medien würde man hier nicht zwingend Datenflüsse an Dritte erwarten. Bei sieben Geräten fanden diese dennoch statt, wobei fast alle davon ebenfalls HTTPS-verschlüsselt erfolgten.

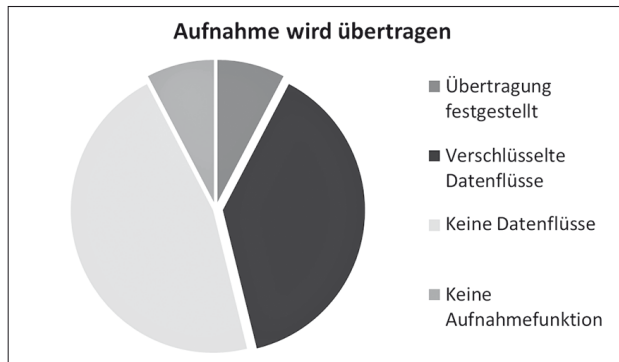


Abbildung 7: Auch Mitschnitt und Wiedergabe kommen ans Licht

Anders als bei den USB-Medien ist in diesen detektivische Spurensuche schwierig, da die Größe der verschlüsselten Datenpakete keinen Rückschluss darüber ableiten lässt, ob die aktuelle Sendung enthalten ist. Bei dem einen Hersteller, bei dem wir mittels des mobilen Prüflabors einen Einblick in die verschlüsselte HTTPS-Verbindung nehmen konnten, wurde festgestellt, dass sowohl die Aufnahme (Sender, Zeitpunkt) als auch die Wiedergabe gepaart mit einer eindeutigen ID an den Hersteller übertragen wurde (Abbildung 7).

Security

Datenschutz ist der Schutz des Persönlichkeitsrechts eines sogenannten Betroffenen – also auch eines Smart-TV-Nutzers. Dazu gehört neben der Frage, ob und welche Daten überhaupt an Hersteller, Fernsehsender, App-Store-Betreiber, ... übermittelt werden dürfen, auch, ob die Sicherheit im Sinne von *Security* ausreichend ist. Bei Smart-TVs ist dieses Themenfeld sehr abhängig vom Hersteller, der Modellversion und natürlich vom aktuellen Softwarestand der Firmware. Systematische Tests der Sicherheit waren aus Ressourcengründen im Rahmen des Smart-TV-Prüfprojekts nicht möglich. Aufgefallen sind allerdings doch einige Punkte:

- Die HTTPS-Verschlüsselung ist bei den aktuellen Geräten zumindest insofern korrekt implementiert, als die Server-Zertifikate auf die Gültigkeit (bezüglich des Ausstellers) überprüft werden. Die Konfiguration der HTTPS-Endpunkte an den Servern ließ allerdings teils zu wünschen übrig. So war Perfect Forward Secrecy (PFS) nicht immer vorhanden. Sogar SSL3 kam teilweise zum Einsatz.
- Bei Portscans an die Smart-TVs waren einige Ports vorhanden und offen, deren Funktion nicht ganz klar war. Bei einigen waren hier Debug-/Test-Zugänge vorhanden, auf die auch bei Produktivversionen innerhalb des lokalen Netzes zugegriffen werden kann. Inwiefern hier Risiken vorhanden sind, wäre noch zu klären.
- Die HbbTV-Seiten, die automatisch und auch ohne aktive Nutzung eines Betroffenen von den Fernsehsendern auf den Smart-TV geladen werden, basieren im Großen und Ganzen auf HTML5, CSS und JavaScript. Würde ein Angreifer eine solche Seite übernehmen, dann hätte dieser Zugriff auf das Smart-TV mit den Schnittstellen, die der HbbTV-Standard definiert. Während ein Ausschalten eines Smart-TV aus der Ferne beim Endspiel der Fußball-Europameisterschaft nur sehr ärgerlich wäre (für manche auch mehr als das), wird es sehr kritisch, wenn über proprietäre Schnittstellen auf diese Weise auf die Kamera und das Mikrophon zugegriffen wird. Dass dies unter realistischen Rahmenbedingungen schon heute möglich ist, wurde im Rahmen einer Reportage über Smart-TVs sogar schon im Fernseher gezeigt (<http://www.swr.de/marktcheck/smart-tv-spione/-/id=100834/did=15300884/nid=100834/1ncw4pz/>).
- Dass Softwaresysteme Schwachstellen enthalten, lässt sich (zumindest praktisch) nicht verhindern. Deswegen kommt der Einspielung von Sicherheitsupdates eine zentrale Rolle zu. Da dies vom Smart-TV-Hersteller gemacht werden muss, besteht die Gefahr, dass – ähnlich wie bei „alten“ Android-Smartphones – Sicherheitslücken nicht immer geschlossen werden können.
- Die meisten Plattformen der Smart-TV-Geräte haben noch keine ausreichende Sicherheitsarchitektur. So gibt es Hersteller, bei denen alle Apps immer mit Root-Rechten laufen. Die Sicherheit soll über die korrekte Nutzung von APIs sichergestellt werden. Dass dies nur schlecht funktioniert, wird mittlerweile regelmäßig auf IT-Sicherheitskonferenzen dargestellt, bei denen Smart-TVs gehackt werden.



Andreas Sachs

Andreas Sachs ist Informatiker und leitet das technische Referat beim Bayerischen Landesamt für Datenschutzaufsicht in Ansbach. Zu seinen Aufgaben gehören die Beratung und Kontrolle von in Bayern ansässigen Unternehmen in den Bereichen IT-Sicherheit und technischem Datenschutz.

Wie geht es weiter?

Nach Durchführung der Prüfung der dreizehn Testgeräte wurden vom BayLDA technische Prüfberichte erstellt und an die beteiligten Datenschutzaufsichtsbehörden und die Hersteller versandt. Ziel war, wie bei anderen Datenschutzprüfungen auch, bei den technisch festgestellten Gegebenheiten (hier: Datenflüsse) ein gemeinsames Verständnis mit allen Beteiligten zu haben. Auf dieses kann dann eine rechtliche Bewertung aufgebaut werden. Dies hat auch stattgefunden und wurde in Form einer sogenannten Orientierungshilfe niedergeschrieben, in der die deutschen Datenschutzaufsichtsbehörden eine abgestimmte technische und/oder rechtliche Auffassung zu einem Themengebiet veröffentlichen. Die Orientierungshilfe „Datenschutzanforderungen an Smart-TV-Dienste“ kann unter <http://www.lida.bayern.de/de/orientierungshilfen.html> heruntergeladen werden. Diese wird von den Datenschutzaufsichtsbehörden für den aufsichtlichen Vollzug verwendet, sollte ein Smart-TV sich nicht an die deutschen Datenschutzgesetze halten.

Fazit

Das anonyme Fernsehen wurde faktisch abgeschafft. Der Weg, den Smart-TV nicht mit dem Internet zu verbinden, bleibt natürlich bestehen, nur ist dann auch das „Smart“ nicht mehr nutzbar. Dies wird allerdings zukünftig nur für informierte Konsumenten, die für den Datenschutz auch bereit sind, Einschränkungen bei der Nutzung neuer Technologien auf sich zu nehmen, ein Weg sein. Experten für Netzwerkanalyse und Firewalls können auch zuhause die eigenen Systeme, samt Smart-TV, versuchen abzuschotten – ohne Garantie, ob dann die smarten Dienste auch weiterhin voll funktionsfähig sein werden. Es bleibt zu hoffen, dass die rechtlichen Instrumente (auch im Hinblick auf das neue Datenschutzgesetz, die EU-Datenschutzgrundverordnung, die ab Mitte 2018 gelten wird) ein exzessives Erheben von Nutzungsprofilen und deren Verarbeitung mit Big-Data-Methoden regeln können. Die Macht der Konsumenten bleibt natürlich erhalten – die Frage, ob Datenschutz für Hersteller von Smart-TVs ein Wettbewerbsvorteil sein kann, der möglicherweise auch höhere Kosten rechtfertigt und transparente Allgemeine Geschäftsbedingungen belohnt, wird die Zeit beantworten.



Sebastian Jekutsch

Fairere Computer

Dass IT-Produkte nicht fair produziert werden, etwa im Sinne des Fair Trade, hat viele Gründe, wie wir immer wieder in Artikeln aus der AG Faire Computer des FfF erfahren konnten. Dennoch ist zu beobachten: Sie werden immer etwas fairer. Im Beitrag zur FfFKon 2015, der ausführlich bebildert und verlinkt im Blog Faire Computer zu finden ist, legen wir dar, wie dies tatsächlich geschieht: Durch investigative Aufdeckung von Unfairness, aufgrund derer negative Presseberichte folgen, reagieren die gebrandmarkten Unternehmen mit Korrekturmaßnahmen. Das Blog zeigt drei Beispiele aus Indonesien, Malaysia und der D.R. Kongo. Manchmal entstehen auch Pionierprojekte daraus, die mehr Fairness als Hauptziel haben. Wir stellen sie vor. Und manchmal entstehen sogar Gesetze daraus, und dies ist ohne Zweifel die nachhaltigste Form der Verbesserung.

Der Beitrag ist zu finden unter <http://blog.faire-computer.de/fairere-computer>.



Faire Computer

Suchen

Für eine sozialverträgliche IT-Produktion






[Startseite](#)
['Faire Computer'](#)
[Termine](#)
[Aktiv werden](#)
[Was kaufen?](#)
[Petitionen](#)
[Bildungsmaterial](#)
[Impressum](#)

Sebastian Jekutsch

Sebastian Jekutsch recherchiert und informiert seit nun fünf Jahren über sozialverträgliche IT-Produktion. Er ist Sprecher der AG Faire Computer des FfF und Initiator des blog.faire-computer.de.

FlfF-Konferenz 2015: Gedichte

Wie auch schon früher bei anderen Gelegenheiten habe ich während des Konferenzdiners der FlfKon 2015 drei Gedichte mit FlfF-Bezug vorgetragen als ein Dankeschön an die Organisatorinnen und Organisatoren.

Das erste Gedicht zielt auf die Regierungspolitik, die ja häufig Anlässe für FlfF-Aktivitäten liefert.

Verben 2015

gabrielen: Panzer an Katar liefern

vonderleyen: bewaffnete Drohnen kaufen

seehofern: Flüchtlinge auf der Grenze stehen lassen

demaiziëren: Frauen und Kinder von Flüchtlingen nicht nachziehen lassen

merkeln: schaffen ohne Plan

... und was ist **FlfFen** und **Cyberpeacen**?

Das dritte Gedicht ist in seiner endgültigen Form erst vor Ort entstanden. Zehn Freiwillige haben je ein Adjektiv aufgeschrieben, die danach gemischt und an die Freiwilligen wieder verteilt wurden. Die haben sich in eine Reihe gestellt und ihr jeweiliges Adjektiv an einen vorgegebenen Satzanfang gehängt. In dieser Reihenfolge vorgelesen, hat sich folgendes Gedicht ergeben:

Cyberpeace und FlfF in Erlangen

Cyberpeace ist streitend

FlfF ist demokratisch

Erlangen ist wohlschmeckend

Cyberpeace ist schön

FlfF ist froh

Erlangen ist begehrenswert

Cyberpeace ist nachdrücklich

FlfF ist laut

Erlangen ist blümerant

Cyberpeace ist bunt

Das zweite Gedicht geht auf die Kritik ein, dass 14 Cyberpeace-Forderungen zu viele sind. Wenn man sie zu Gedichtzeilen verkürzt, geht es doch. Der Refrain „Cyber – Peace“ soll dabei interaktiv eingesetzt werden. Entweder ruft die oder der Vortragende „Cyber“ und die Zuhörenden antworten mit „Peace“, oder die Zuhörenden werden in zwei Gruppen aufgeteilt, so dass die eine Gruppe „Cyber“ ruft und die andere mit „Peace“ antwortet.

Cyberpeace-Forderungen

Keine Erstschläge
ausschließlich defensiv

Cyber – Peace

Abrüstung
keine konventionelle Antwort
Genfer Cyberkonvention

Cyber – Peace

Übernahme in Regierungspolitik
demokratische Kontrolle
Online-Protest kein Angriff
demilitarisierte Sprache

Cyber – Peace

Schwachstellen offenlegen
Schutz kritischer Infrastrukturen
Cybersicherheit sicherstellen

Cyber – Peace

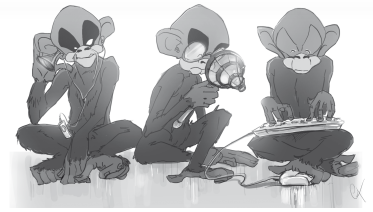
Junge IT-ExpertInnen fördern
freie und offene Software



Hans-Jörg Kreowski

Prof. Dr. **Hans-Jörg Kreowski** war bis 2015 Leiter der Forschungsgruppe *Theoretische Informatik* an der Universität Bremen. Von 2003 bis 2009 war er Vorsitzender des FlfF.

FfF-Studienpreis 2015



FfF-Studienpreis 2015
1. Preis

Christian Ricardo Kühne

Zur Idee herrschaftsfreier kooperativer Internetdienste

Eine Übung im utopischen Denken

Als Lenin sich auf seine letzten Jahre der beschränkten Macht der Bolschewiki bewusst wurde und der Sozialismus nicht von heute auf morgen zu erreichen war, schreibt Slavoj Žižek, sah er die einzige Möglichkeit für sozialen Fortschritt darin, eine moderate Politik des Staatskapitalismus mit einer intensiven kulturellen Schulung der trägen Masse der Bauern zu verbinden, bis die materiellen Bedingungen für den Sozialismus geschaffen wären.¹ Aus der Leninschen Idee einer beschränkten Anwendung der kapitalistischen Produktivkraft lässt sich vielleicht mit Blick auf die Geschichte des Internets die folgende unorthodoxe Lehre ziehen: Am Ende des NSFNET-Projekts – als letztem großen Ausläufer des ARPANET-Projekts – wurde nicht nur die Zweckbindung an Bildung und Forschung fallen gelassen, sondern auch die Werte der Offenheit und Inklusion, die maßgeblich zur Ausbreitung des Internets bis 1995 beigetragen haben.² Die darauf folgenden Jahre der Liberalisierung des Internets sorgten für einen massiven Anstieg von Internet-Nutzer:innen, und mit den Wechselwirkungen zwischen Internet und Gesellschaft überschlugen sich die Innovationszyklen; auf die bekannten E-Mail- oder Chat-Dienste folgten unter anderem internet-basierte Finanzdienstleistungen, Online-Händler, soziale Netzwerke und sogenannte Cloud-Dienste. Ein gedeihliches Jahrzehnt ging vorüber, bis die ersten Krisenerscheinungen auftraten: Mit der ungebändigten Produktivkraft der kapitalistischen Wirtschaftsordnung wurden nicht nur die anfänglich dezentralen Strukturen schrittweise zentralistisch überformt,³ sondern immer mehr Kommunikationen und Daten in die Warenform überführt und öffentliche Räume unter privatwirtschaftlicher Herrschaft in die Abhängigkeit getrieben. Vielleicht wird es Zeit, mit Lenin die Koffer zu packen und das Experiment der Liberalisierung des Internets allmählich zu verlassen ...

An einer Stelle gilt es jedoch eine historische Besonderheit hervorzuheben: Als in den 70er- und 80er-Jahren die ersten Internetdienste wie das Telnet, das File Transfer Protokoll oder E-Mail sich als sozial nützlich erwiesen hatten, war es gang und gäbe, Ressourcen zu teilen, indem ein ARPANET-Host sowohl als Server als auch als Client betrieben wurde.⁴ Diese und andere Peer-to-Peer-Ansätze in der Folge waren die Voraussetzung für den Aufbau und die Gestaltung einer kleinen Netzgemeinde, die bereits starke Anzeichen des Politischen an sich trug. Es entwickelte sich eine einmalige kooperative Praxis unter den Ingenieuren, Wissenschaftlern und Studierenden, welche die anfängliche Entwurfsentscheidung eines verteilten Systems mit gleichberechtigten Peers aufgriffen und daraus eine Basis für einen fruchtbaren Wissensaustausch und technische Experimente schufen. Ich möchte gerne an die Ideen offener P2P-Ansätze anknüpfen, die zwischenzeitlich durch das Filesharing in P2P-Netzwerken seit den 2000er-Jahren zwar neu aufgelebt sind, denen es aber meines Erachtens entschieden an einer wahrhaft politischen Dimension mangelt. Ich behaupte nämlich, dass ein nicht unerheblicher Teil der heutigen Problematik einer aus den Fugen geratenen Informationsmacht durch eine politisch reformulierte P2P-Idee in Angriff genommen werden kann. Mein Vorschlag hierfür ist die begrifflich weiterentwickelte Idee des herrschaftsfreien kooperativen Internetdienstes (HKI). Um diese These zu untermauern, werde ich zuerst erläutern, was sich hinter diesem Begriff verbirgt und welches normative Problem damit zusammenhängt. Anschließend sollen am Beispiel des GUNet-Filesharing-Dienstes einige konkrete Aspekte eines HKI veranschaulicht werden. Zuletzt werde ich auch auf Grenzen dieses Ansatzes eingehen.



Christian Kühne bei Entgegennahme des Studienpreises
Foto: Kai Nothdurft

Was sind herrschaftsfreie kooperative Internetdienste?

Kooperative Internetdienste machen sich die im Netz verbundenen, frei verfügbaren Ressourcen der Computer zunutze. Erst durch das kooperative, sich ergänzende Zusammenwirken der teilnehmenden Computer als Netzwerkknoten entfaltet dieser Typ von Internetdiensten sein eigentliches Potential. Die Ressourcen, die ein vernetzter Computer an sich besitzt, umfassen im Allgemeinen Rechenleistung, Speicherkapazität und die Durchsatzrate der Netzanbindung (fälschlicherweise auch als „Bandbreite“ bezeichnet). Die Tatsache, dass diese Ressour-



cen die meiste Zeit über ungenutzt bleiben, wird jedoch kaum zur Kenntnis genommen. Zwar verzeichnen wir einen steigenden Trend bei der Verbreitung von tragbaren Computern wie *Smartphones* mit vergleichsweise geringer Rechenleistung und einem kleinen Energiespeicher, gleichzeitig werden aber auch im Zuge der Informatisierung verschiedener Lebensbereiche an anderer Stelle leistungsfähigere Computer eingeführt. So werden in immer mehr Berufen Arbeitsplätze mit Computern ausgestattet, die einen durchgängigen Betrieb mit Netzanbindung für die Arbeit voraussetzen.

Die Grundlage für einen kooperativen Dienst ist ein bestimmtes interkommunikatives Rollenmodell, das sich im Netzwerkprotokoll und der Programmlogik niederschlägt. Jedes Gerät, das einen kooperativen Dienst betreibt, verhält sich als Peer gegenüber den anderen Peers als (nahezu) gleichberechtigtes Mitglied in dem teilnehmenden Netzwerk. Dies geschieht auf eine Weise, bei der jeder Peer die gleiche Rolle hinsichtlich einer bestimmten Netzwerkfunktion ausübt, ausgestattet mit den gleichen Rechten und Pflichten, die es bedarf, um einen kooperativen Dienst „ins Leben zu rufen“ und „am Leben zu erhalten“. Einige beispielhafte Rechte umfassen Zugriffsrechte auf Dateien, Verteilrechte für Datenreplikation oder Abfragerechte für Suchanfragen, während das Weiterleiten von Anfragen oder das Routen von Datenpaketen zum Kanon der Pflichten gehören kann, die sich aus dem Gebrauch der Rechte gegenüber anderen ergeben. Die Einhaltung der Rechte und Pflichten wird über das Netzwerkprotokoll wechselseitig vermittelt, wer das Protokoll verletzt, muss mit „Einschränkungen“ seiner Rechte rechnen.

Die Vernetzungsart spielt bei HKIs eine untergeordnete Rolle, daher sind neben dem Internet auch Ad-hoc-Netzwerke zwischen physisch nahestehenden Geräten, LANs oder drahtlose Maschennetzwerke in der Stadt wie auf dem Lande tauglich, denn selbst ein sogenannter *Netsplit*, wie man ihn aus IRC-Zeiten mit Wehen erinnert, macht einem gut entworfenen Internetdienst dieser Art wenig aus. Aus einem ganz anderen Blickwinkel erweist sich dies sogar als recht vernünftig: Die fehlende Internetkonnektivität darf nicht dazu führen, dass den Menschen in räumlicher bzw. regionaler Nähe ein Austausch von Informationen wie zum Beispiel über Filesharing oder Instant Messaging verwehrt ist.

Damit ist bereits auf eine weitere Eigenschaft kooperativer Dienste verwiesen, nämlich die Selbstorganisation. Die Automatisierbarkeit von Kommunikations- und Informationsverarbeitungsprozessen durch Computer hält uns dazu an, den Gebrauch und die Bereitstellung von Netzwerkressourcen selbstorganisierend zu gestalten. Nach dem Anschalten eines Gerätes sucht es automatisch nach anderen Geräten in der Nähe, um Kontakt aufzunehmen und seine Teilnahme an einem kooperativen Internetdienst (bspw. mittels Flooding) zu verkünden.

Herrschaftsfreie kooperative Internetdienste sind in erster Linie reine P2P-Dienste – mit einigen besonderen Eigenschaften. Weder gibt es Server noch privilegierte Super-Knoten oder irgendeine Art hierarchisch organisierter Strukturen zwischen den Knoten. Dahinter steckt der Gedanke, dass soziale Privilegien, die von Anfang an durch die Technik bestimmt sind, vermieden werden.⁵ Historisch treten weitere Aspekte der Herrschaftsfreiheit hinzu. Die Codebasis des Internetdienstes muss freie Soft-

ware sein, nicht nur um ihre freie Nutzung zu gewährleisten, sondern auch um den Code verschiedenen Prüfverfahren unterziehen zu können und eine stetige Verbesserung als Lernprozess zu ermöglichen. Die Offenheit des Kommunikationsprotokolls fördert eine freie und nicht kommerzielle Teilnahme am Internetdienst, die der kulturellen Teilhabe am gesellschaftlichen Leben entspricht. Die sogenannten *Cloud*-Dienste weisen genau in die entgegengesetzte Richtung, denn dort kommen zwar P2P-Technologien im Inneren zum Einsatz, aber nach außen hin wird *Access* als Ware vermarktet.⁶ Sicherheit und Fehlertoleranz sind vielleicht die letzten beiden Aspekte eines herrschaftsfreien Dienstes, denn bei beiden geht es erneut um die Vermeidung außerordentlicher Machtausübung auf die Peers und ihre Dienste. Die Fehlertoleranz eines HKI bemisst sich daran, wie gut er äußere und innere Störungen bewältigen oder abwehren kann, ohne dass die Funktionstüchtigkeit des Dienstes dadurch gefährdet wird. Die Sicherheit sowohl des Netzwerks als auch eines Peers beinhaltet die Schutzziele der Integrität, Vertraulichkeit und Verfügbarkeit gegen äußere und innere Angriffe. Alle genannten Aspekte, die sich in den Mechanismen und Strategien gegen einen autoritären Einfluss widerspiegeln, und auch der institutionelle Charakter, wie er durch die verstetigte Nutzung von P2P-Diensten in Erscheinung tritt, begründen die begriffliche Wahl eines herrschaftsfreien kooperativen Internetdienstes.

Welches (gesellschaftliche) Problem nehmen HKIs eigentlich in Angriff?

Herrschaftsfreie kooperative Internetdienste, wie ich sie oben skizziert habe, setzen dort an, wo Informations- und Kommunikationstechniken durch Organisationen ein zusätzliches, verstärkendes Machtgefälle aufbauen. Das anfängliche Problem mit der organisierten automatischen Datenverarbeitung hat nicht abgenommen, sondern zugenommen, während gleichzeitig die Verkettungsrisiken durch die Verbreitung des Internets dieses Problem noch einmal verschärft haben.⁷ Dieser technisch-organisatorische Zustand, an den ein zunehmender Teil gesellschaftlicher Praktiken gebunden ist, ermöglichte in verschiedenen Bereichen der Gesellschaft autoritäre Herrschaftsformen, die westliche Demokratien (allen voran die Bürgerrechtsbewegungen) unter anderem durch das Prinzip der Gewaltenteilung zu bekämpfen suchten. Ich bezeichne diesen Gesamtzusammenhang als das gesellschaftliche Problem einer aus den Fugen geratenen Informationsmacht.

Diese Problemstellung lässt sich aufgrund ihrer genetisch-materiellen Bedingungen von anderen artverwandten Problemstellungen unterscheiden. So lässt sich seit J.J. Rousseau von einer gesellschaftlichen Macht sprechen, als klar wurde, dass die Individuen bzw. Minderheiten einer sozialen Übermacht in den Städten nichts entgegenzusetzen hatten. Von einer Wirtschaftsmacht ließ sich spätestens seit K. Marx sprechen, der wie kein anderer den Konflikt zwischen Kapitalisten und Lohnarbeitern hinsichtlich der Produktionsmittel auf sozialkritische Weise thematisierte. Eindrücklich ist auch die Finanzmacht der Banken und Investoren im Hinblick auf die Geldmittel, die bereits auf verschiedenen Märkten die Realwirtschaft und das Gemeinwesen in ihrer Funktionsweise bedroht oder gestört haben. Informationsmacht als gesellschaftlich relevantes, aber bedingungs-



loses Machtverhältnis neuen Typs wurde jedoch erst mit der Verbreitung und Rationalisierung von Informations- und Kommunikationsmitteln immer sinnfälliger. Sowohl das Aufkommen von Datenverarbeitungszentren in Verwaltung und Wirtschaft als auch der Telekommunikationsanbieter vergrößerten die Gemengelage der Problemscheinungen und führten dazu, die Problembeschreibung einer aus den Fugen geratenen Informationsmacht zu vervollständigen, die noch bis in die zweite Hälfte des 20. Jahrhunderts diffus und unbestimmt war. Die Ersten, die angetreten waren, diesen neuen Typ von Macht systematisch zu theoretisieren und unter Bedingungen zu stellen, waren die Datenschützer der ersten Generation in den 1960er-Jahren.⁸ Die von ihnen eingebrachte neue gesellschaftliche Rationalität, die, theoriegeleitet und verfassungsrechtlich begründet, auf die sozialen Pathologien zu reagieren versuchte, sollte sich im kodifizierten Recht und in neuen Institutionen wie dem Datenschutzbeauftragten niederschlagen.

Während es dort aber um die „Konditionierung von Macht“ ging,⁹ vermögen HKIs das Problem der Informationsmacht in einigen Fällen durch eine Form der radikalen Gewaltenteilung anzugreifen. Die P2P-Struktur von HKIs bewirkt eine Machtzergliederung, die bis zur Mikroebene hinunter reicht. Die Informationsverarbeitung geschieht hier arbeitsteilig zwischen den Peers, während persönliche Kommunikationsvorgänge vertraulich und verkettungssicher¹⁰ unter der Kontrolle der kommunizierenden Peers bleibt.¹¹ Wie eine solche Umsetzung konkret aussehen kann, erläutere ich im nächsten Abschnitt am Beispiel des GUNets.

Beispiel GUNet und Informationsmacht

Das GUNet ist eine sicherheitsorientierte, dezentrale P2P-Netzwerktechnologie mit ausgesprochen ethisch-politischem Charakter.¹² Sie ist meines Erachtens Ausdruck einer (wissenschaftlich praktizierten) technischen Fundamentalkritik an den derzeit weit verbreiteten Internetdiensten, von denen große Teile der Weltgesellschaft Gebrauch machen. Anhand des Filesharing-Dienstes aus der Reihe der GUNet-Dienste möchte ich kurz skizzieren, wie das Paradigma eines HKIs prototypisch umgesetzt wurde und welche Wirkungen dieses auf das informationelle Machtgefüge haben kann.

Der GUNet-Filesharing-Dienst (GUNet-FS) verwirklicht die Idee der Herrschaftsfreiheit auf unterschiedliche Weise. Das besondere Codierungsschema ECRS zerteilt eine Datei, die mit Suchbegriffen in das System gespeist wurde, in viele kleine gleich große Blöcke, die verschlüsselt und auf unterschiedliche Peers verteilt und repliziert werden. Nur wenn die damit verknüpften Suchbegriffe bekannt sind, lässt sich die Datei rekonstruieren,

denn die Fragmente sind allein kryptographisch adressierbar. Einem Zensor wird damit die Arbeit ungemein erschwert, denn weder lassen sich die Suchbegriffe noch die Datei an einer zentralen Stelle sperren oder löschen. (Die Replikationsmechanismen sorgen zudem dafür, dass einzelne Kopien verloren gehen können.) Das Anonymisierungsprotokoll GAP erschwert zudem, dass der Initiator einer veröffentlichten Datei mit dieser in Beziehung gebracht werden kann. Im Unterschied dazu stellen die restlichen Peers des Netzwerks den Speicherplatz bereit, ohne zu wissen, welche (fragmentarischen) Inhalte sie eigentlich aufbewahren. Die so gewonnene Möglichkeit, das Wissen um den „Besitz“ dieser Informationen plausibel abstreiten zu können, verringert das Risiko von persönlichen Sanktionen. Zuletzt sind auch die eingebauten Schutzmechanismen gegen Angriffe auf das Gesamtsystem zu nennen, auf die ich hier aber nicht weiter eingehen werde.¹³ Die spezifische Idee der Herrschaftsfreiheit wird also aufgrund der Architektur dieses Dienstes verwirklicht, welche den inneren und äußeren Akteuren keine zureichenden technischen Mittel an die Hand gibt, um auf die Menschen und ihr demokratisches Anrecht auf freien Informationsaustausch Einfluss zu nehmen.¹⁴

Dieser Form der herrschaftsfreien Technikgestaltung wohnt aber auch ein inhärenter kooperativer Charakter inne. In dem gleichen Maße, wie der Dienst technisch verteilt wird, werden Mechanismen und Protokolle notwendig, die einer guten Praxis der Kooperation gleichkommen. Die normative Bezugnahme auf das Gute bezieht sich auch hier wieder auf Probleme und Lernprozesse im historischen Kontext: Das Phänomen des Free-loadings/Leechings führte das Problem vor Augen, dass kooperativ konzipierte Dienste einseitig (aus)genutzt wurden. Im GUNet-FS kommt daher ein integriertes Reputationssystem zum Tragen, das einen fairen Umgang auf Basis der zur Verfügung stehenden ökonomischen Ressourcen organisiert. Ressourcen-Überschuss in Bandbreite und Rechenleistung ist die Quelle für die Reputation eines unbekannten Peers.¹⁵ Werden bs pw. Suchanfragen gestellt, reduziert sich der zahlenmäßige Wert der Reputation. Dieser kann jedoch niemals negativ werden bzw. in Gering-schätzung übergehen. Die Folge ist eine Form der Kooperation, die auf Inklusion und einer Wertschätzung von freigegebenen und unbenutzten Ressourcen aufbaut.

Wo sind Grenzen herrschaftsfreier kooperativer Internetdienste?

Freilich wäre es weit gefehlt, HKIs als allgemeines Heilmittel anzusehen. Ich behaupte, dass es zwei wesentliche Einzugsgebiete gibt, in denen HKIs gesellschaftlich wirksam sein könnten. Ihr größtes Veränderungspotential entfalten sie zum einen dort, wo vollständig berechenbare Internetdienste (also in Algorithmen

Christian Ricardo Kühne

Christian Ricardo Kühne hat Informatik, Philosophie und Sozialwissenschaften studiert. Zurzeit forscht er im Bereich der Kritischen Informatik über *emanzipatorische Informations- und Kommunikationstechnologien*. Nebenbei arbeitet er im *Secushare-Projekt* mit, in dem ein erster Prototyp für soziale Interaktion auf Basis des GUNets entwickelt wird.

vergegenständlichte Handlungs- und Arbeitsfunktionen) die asymmetrischen Machtverhältnisse zwischen den verschiedenen sozialen Akteuren maßgeblich herbeiführen und durch funktionsähnliche HKIs ersetzt werden können. Ein interessantes Beispiel ist Amazon. Die Idee eines virtuellen Marktplatzes, an dem Händler ihre Waren tauschen oder verkaufen, lässt sich auch als verteiltes System im Sinne eines HKI konzipieren. Die Entscheidung darüber, was angeboten oder verkauft werden soll, liegt idealerweise bei den Händlern, Käufern und Tauschpartnern, also bei den Peers und nicht beim Dienst selbst! Im Kern geht es also darum, die Informationsverarbeitung unter gänzlich neue Bedingungen zu stellen.

Zum anderen sind Veränderungspotenziale dort zu erwarten, wo durch Telekommunikationsdienste eine hauptsächlich vermittelnde Funktion durchgeführt wird. Hier wirken HKIs durch verkettungssichere und vertrauliche Kommunikation darauf hin, dass Telekommunikationsdienstleister auf die banale Funktion der agnostischen Paketvermittlung reduziert werden.

Allerdings gibt es Dienste, deren konstitutive Handlungs- und Arbeitsfunktionen nicht vollständig berechenbar sind oder von denen wir zumindest erwarten, dass beispielsweise menschliche Abwägungen ein Teil des Prozesses bilden sollten. Die Annahme oder Ablehnung eines behördlichen Antrags darf eben keine Frage der Berechenbarkeit sein, auch wenn der Behördengang selbst elektronisch vonstattengeht. Zusätzlich zu dieser dritten Klasse gibt es eine vierte, nämlich digitale Infrastrukturdienste einschließlich ihrer Terminals, die als abgeschlossene Systeme vermachtet und infolgedessen ebenfalls keinen Machtverschiebungen des HKI unterziehbar sind. Beispielhaft hierfür wäre das Informations- und Kommunikationssystem der Deutschen Bahn AG, bestehend aus Servern, Datennetzen und Bahnautomaten. Mit den beiden letztgenannten Dienstklassen wird klar, dass die Idee des Datenschutzes sachlich nach wie vor nichts an Aktualität und politischer Bedeutung verloren hat. Die von Organisationen betriebenen Dienste, von denen angenommen wird, dass sie einen gesellschaftlichen Nutzen bringen, müssen unter politische Bedingungen gestellt werden, indem Organisationen gegenüber demokratisch legitimierten Datenschutzbeauftragten sowie Betroffenen nachweisen, dass die personenbezogenen Verfahren fair, beherrschbar und sicher sind.¹⁶

Schluss

Wie sich gezeigt hat, ist die Idee der herrschaftsfreien kooperativen Internetdienste höchst anspruchsvoll, nicht nur aufgrund der technischen Kriterien, die ein guter HKI erfüllen sollte. Es sind vor allem die politisch-ethischen Ansprüche wie Selbstbestimmung, Freiheit oder Solidarität, die moderne Gesellschaften an die Technik stellen. Zurzeit lässt sich jedoch beobachten, wie immer mehr Funktionen und soziale Interaktionen in Cloud-Plattformen übergehen, indem Computer- und Netzwerkreisourcen zentralisiert werden und nur noch über Client/Server-Schnittstellen zur Verfügung stehen. Von Social Networking Services bis zum Document Sharing wird die Kontrolle über Daten und Algorithmen an große Organisationen mit transnationaler Reichweite abgegeben. Mit Morpheus lässt sich ironisch fragen: "Do you think that's air you're breathing now?"

Anmerkungen

- 1 *Nicht durch kommunistische Propaganda und staatlichen Terror, wie sie durch seinen heftigsten Opponenten Josef W. Stalin einige Jahre später zur Anwendung kamen, sondern „durch geduldige, allmähliche Etablierung gängiger Standards der Zivilisation“.* Vgl. Žižek, Slavoj (2012): *Die Revolution steht bevor. Dreizehn Versuche über Lenin.* Frankfurt am Main: Suhrkamp, S. 14.
- 2 Aspray, William und Paul E. Ceruzzi (Hg.) (2008): *The Internet and American Business (History of Computing).* MIT Press, S. 33.
- 3 *Einige Indikatoren hierfür sind die zunehmende Monopolbildung bei den Internet-Organisationen, die Einführung dynamischer IP-Adressen oder der Network Address Translation (NAT) durch die Telekommunikationsanbieter oder der starke Trend, Internet-Dienste nach dem Client/Server-Modell zu entwickeln und die Informationsverarbeitung hauptsächlich in die „Clouds“ zu verlagern.*
- 4 Vgl. Coy, Wolfgang (2008): *Market and Agora: Community Building by Internet.* In: William Aspray und Paul E. Ceruzzi (Hg.): *The Internet and American Business (History of Computing).* MIT Press, S. 543.
- 5 *An der Geschichte von Skype lässt sich dies gut nachvollziehen. Ursprünglich als P2P-Dienst mit einigen Super-Peers konzipiert, wurde es von Microsoft übernommen und in einen Client/Server-Dienst umgebaut. Dies war möglich, weil die Super-Peers eine besondere Rolle bei der Vermittlung von P2P-Kommunikation besaßen.*
- 6 *Zur Access-Ökonomie vergleiche Rifkin, Jeremy (2000): Access. Das Verschwinden des Eigentums. Warum wir weniger besitzen und mehr ausgeben werden.* Frankfurt am Main: Campus Verlag.
- 7 Rost, Martin (2008): *Gegen große Feuer helfen große Gegenfeuer. Datenschutz als Wächter funktionaler Differenzierung. Vorgänge, 184:15–25.*
- 8 Pohle, Jörg (2014): *Die immer noch aktuellen Grundfragen des Datenschutzes.* In: Hansjürgen Garstka, Wolfgang Coy (Hg.): *Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten. Wilhelm Steinmüller zum Gedächtnis.* Helmholtz-Zentrum für Kulturtechnik, Humboldt-Universität zu Berlin, S. 45–58.
- 9 Vgl. Rost, Martin (2013): *Neun Thesen zum Datenschutz.* In: Jörg Pohle und Andrea Knaut (Hg.): *Foundationes I: Geschichte und Theorie des Datenschutzes.* Münster: Monsenstein und Vannerdat.
- 10 *Verkettungssicherheit korrespondiert mit der Idee der Anonymität aus dem Bereich der PETs. Neuere Überlegungen formulieren dies als „kombinierter Metadatenschutz mit Ende-zu-Ende-authentisierter Vertraulichkeit“.* Siehe auch Rost, Martin (2004): *Verkettbarkeit als Grundbegriff des Datenschutzes? Identitätsmanagement soziologisch betrachtet.* In: Johann Bizer, Albert von Mutius, Thomas B. Petri und Thilo Weichert (Hg.): *Innovativer Datenschutz 1992–2004. Wünsche, Wege, Wirklichkeit. Für Helmut Bäumler. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, S. 315–334.*
- 11 *Siehe zum Beispiel von Loesch, Carlo; Gabor Toth und Mathias Baumann (2011): Scalability & Paranoia in a Decentralized Social Network.*
- 12 Vgl. Kühne, Christian Ricardo (2015): *GNUnet und Informationsmacht: Analyse einer P2P-Technologie und ihrer sozialen Wirkung.* Diplomarbeit, Humboldt-Universität zu Berlin, S. 49. Im Internet: https://crook.de/docs/gnunet_und_informationsmacht.pdf
- 13 *Der Filesharing-Dienst setzt z. B. auf den Routing-Dienst R5N, der Sybil-Angriffe überstehen kann.*
- 14 *Ebd., S. 50–66.*
- 15 *Ebd., S. 39.*
- 16 Rost, Martin (2012): *Faire, beherrschbare und sichere Verfahren.* In: Falk Peters, Heinrich Kersten und Klaus-Dieter Wolfenstetter (Hg.): *Innovativer Datenschutz.* Berlin: Duncker & Humblot. S. 17 ff.

Techno-Politics as Network(ed) Struggles

The Politics of Internet Surveillance

An dieser Stelle möchte ich mich gerne ganz herzlich beim FfF für die Verleihung des Studienpreises bedanken, und ebenso für die Einladung zur Preisverleihung im Rahmen der FfF-Konferenz, die im November 2015 in Erlangen stattfand. Mein besonderer Dank gilt Sylvia Johnigk und Kai Nothdurft, die mich auf die Bewerbung zum Preis aufmerksam gemacht haben, sowie Professorin Britta Schinzel für ihre Laudatio meiner Arbeit. Des Weiteren bedanke ich mich sehr herzlich bei meinen Professoren Michael Nagenborg und Peter-Paul Verbeek von der Universität Twente, ohne deren intensive Betreuung und Input diese Masterarbeit nicht möglich gewesen wäre!

Schwerpunkt



Einleitung

Wie kann staatliche Überwachung im Sinne der von Edward Snowden enthüllten Dokumente als politisches Mittel verstanden werden? In diesem Artikel möchte ich gerne einen Ansatz zur Beantwortung dieser Frage vorstellen, an welchem ich im Rahmen meiner Masterarbeit in *Philosophy of Science, Technology and Society* an der Universität Twente in den Niederlanden gearbeitet habe. Während dieses Essay die wesentlichen Punkte der Arbeit herausstellt und in den größeren Kontext setzt, kann die Vollversion der Arbeit unter <http://essay.utwente.nl/66530/> heruntergeladen werden.

Im Folgenden setze ich die Arbeit zuerst in Bezug zu den den FfF-Leser:innen vermutlich durchaus schon bekannten Snowden-Enthüllungen, durch welche wir tieferen Einblick in das System staatlicher (Internet-)Überwachung gewinnen konnten. Anschließend diskutiere ich die Frage, was Infrastruktur mit Politik zu tun hat und stelle die techno-politischen Dimensionen der Internet-Infrastruktur dar. Innerhalb dieses Rahmens fasse ich anschließend meine Analyse der NSA-Überwachungsmethoden und deren Implikationen zusammen. Abschließend gebe ich meine kurze Antwort auf die Frage, ob staatliche Überwachung tatsächlich nur eine Frage von Privatsphäre und Sicherheit ist.

Die Snowden-Enthüllungen und deren Konsequenzen

Im Juni 2013 trat Edward Snowden in Hongkong zum ersten Mal vor die Kamera von Laura Poitras und stellte sich den Fragen der Journalisten Glenn Greenwald und Ewen MacAskill.¹ Was daraufhin folgte, war wohl eines der größten Medienereignisse in der Geschichte des Whistleblowings. Die detaillierten Einsichten in die Methoden eines internationalen Netzwerkes staatlicher Überwachungsorgane, die wir dank Edward Snowden gewinnen konnten, haben wohl unser Verhältnis zum Internet und unser Verständnis von Online-Privatsphäre entscheidend mitgeprägt. Obwohl bereits seit längerer Zeit bekannt war, dass die NSA in großem Stile überwacht, schlugen die Veröffentlichungen weitreichende Wellen und prägten gar eine ganze Epoche der „Post-Snowden-Ära“, gaben Anlass zu Büchern und zahlreichen Panels sowie Talkrunden in Politik, Fernsehen, Universitäten und in der Technikbranche selbst. Insbesondere in Amerika führten die „Snowden disclosures“ zu Unmut, da klar wurde, dass die amerikanischen Überwachungsorgane in ihrem präventiven Generalverdacht durchaus keinen großen Unterschied zwischen amerikanischen und nicht-amerikanischen Staatsbürger.



Laura Fichtner, Foto: Kai Nothdurft

innen machen, was letztendlich nur noch die knallharten Verfechter:innen der „Nothing-to-Hide, Nothing-to-Fear“-Doktrin kalt lassen konnte.

Aber was der internationalen Internetcommunity, die sich ja schon lange mit den technischen und gesellschaftlichen Fragen des Datenschutzes, der IT-Sicherheit, Privatsphäre und, zumindest in jüngerer Vergangenheit, der *Big Data* beschäftigt, einen besonderen Dienst erwies, war der Umfang der gewonnenen Einsichten sowie die Details, die aus den klassifizierten schriftlichen Dokumenten entnommen werden können und somit etwaigen politischen, ethischen oder technischen Forderungen Nachdruck verleihen konnten. Die gewonnenen Einblicke ermöglichten dann letztendlich auch für mich das Verfassen einer technisch und empirisch wohlinformierten *Techno-Politics as Network(ed) Struggles*². In der Arbeit konzeptualisierte ich den Begriff der *techno-politics*, welcher eine Form der Politik beschreibt, die durch technische Kanäle ausgeführt wird. In diesen techno-politics verschmelzen das Technische und das Politische miteinander – sie beschreiben die Technisierung des Politischen und die Politisierung des Technischen: technische Herausforderungen werden zum Gegenstand politischer Ambitionen, und politische Ambitionen werden durch technische Mittel verfolgt.

Was hat Infrastruktur mit Politik zu tun?

Die Frage, die ich mir in meiner Arbeit stellte, war nicht die Frage, inwiefern die NSA-Überwachung rechtliche Grenzen überschreitet oder gegen Verfassungen verstößt, oder etwa inwieweit die Gewährung innerer Sicherheit gegen die Bewahrung der Privat-

sphäre abzuwägen sei. Vielmehr konzentrierte ich mich darauf, zu verstehen, wie sich die ausgeprägte Form der NSA-Überwachung, oder allgemeiner jedwede Form der zentralisierten Internet-Überwachung, durch ein Macht- und/oder Marktmonopol, auswirkt auf die politischen Strukturen der globalen Öffentlichkeit, die durch das Internet und seine Infrastruktur entstanden ist.

In meiner Arbeit baute ich auf einen Begriff des Politischen und Demokratischen auf, der vom Amerikaner und Demokratie-Idealisten John Dewey bereits in den 20er-Jahren des letzten Jahrhunderts entwickelt worden ist.³ Für Dewey besteht die Aufgabe der Politik vor allem darin, die Interaktionen und den Austausch innerhalb einer Gesellschaft im Sinne aller Beteiligten verlässlich und vernünftig zu regulieren. Er sieht diese Aufgabe dann in einer Demokratie erfüllt von den demokratisch gewählten Repräsentanten der *public*, der politischen Gemeinschaft oder Öffentlichkeit.⁴ Diese sollen gemäß ihrer Aufgabe im Interesse dieser Öffentlichkeit handeln und ihre Entscheidungen auf Grundlage eines Austausches mit den Bürgern im öffentlichen und rationalen Diskurs fällen. Für Dewey ist eine solche politische Gemeinschaft oder Öffentlichkeit allerdings kein statisches Gebilde, und sie ist schon gar nicht festgelegt durch die Grenzen unserer heutigen Staatenlandschaft. Stattdessen wird sie vielmehr bestimmt durch eben jenen gesellschaftlichen Austausch, den Politik zu regulieren sucht.⁵

Auf Grundlage dieses Politikverständnisses werden technische Infrastrukturen dann zum zentralen Bestandteil der Politik und politischer Bestrebungen, da sie neue Kanäle eröffnen, über welche der gesellschaftliche Austausch verschiedener Güter oder Informationen erfolgen kann. Das Internet zum Beispiel schafft solche neuen Kanäle, und konsequenterweise entsteht dann eine neue politische Öffentlichkeit, die aus all jenen besteht, welche über diese Kanäle interagieren und so ein Interesse an deren Regulierung haben. So wird die Infrastruktur dann zum Gegenstand politischer Bestrebungen.

Im Zusammenhang hierzu steht die Arbeit des Medientheoretikers Alexander Galloway, der es sich in *Protocol* einmal zur Aufgabe gemacht hat, die Kontrollstrukturen, die sich in der ansonsten transparenten Internet-Infrastruktur verbergen, sichtbar zu machen.⁶ Er unterscheidet hier zentralisierte, dezentralisierte und verteilte Netzwerkstrukturen, die sich vor allem darin unterscheiden, wie sie 1. die Flüsse, die durch das Netzwerk und seine Infrastruktur ermöglicht werden, gestalten, 2. auf welche Weise Kontrollmechanismen und -instanzen implementiert werden und 3. wie sie die Machtverhältnisse zwischen den verschiedenen Netzwerkteilnehmer:innen gestalten.⁷

In einem zentralisierten Netzwerk, so Galloway, gibt es eine kontrollierende Instanz, einen Mittelpunkt, an den alle anderen anknüpfen. Dieser, als einziger Hauptknotenpunkt, hat das Recht, anderen den Zugang zum Netzwerk zu verwehren, und muss immer um Erlaubnis gefragt werden: dieser Mittelpunkt übersieht alle Flüsse im Netzwerk und kann Kommunikation zwischen anderen Netzwerkteilnehmern herbeiführen oder unterbinden.

Ein dezentralisiertes Netzwerk ist dann die Verbindung mehrerer zentralisierter Netzwerke: hier gibt es einige Hauptknotenpunkte, die sich auf einer hierarchischen Ebene befinden und miteinander gleichberechtigt agieren können. Diese haben allerdings ihre eigenen untergeordneten Instanzen, über welche sie wie im zentralisierten Netzwerk verfügen können. Als anschauliches Beispiel könnte man hier ans internationale Flugsystem denken. Auch dort gibt es einige Hauptknotenpunkte, beispielsweise New York, Frankfurt oder Amsterdam, die alle gleichberechtigte Verbindungen zueinander pflegen, allerdings die Kontrolle über provinzielle Ziele haben – wer in eine kleine Stadt in der Provinz in den USA möchte, ist immer darauf angewiesen, erst einen großen Knotenpunkt anzusteuern.

Und dann gibt es letztendlich noch das anarchistische, das verteilte, Netzwerk, in dem man keinerlei Hierarchien zwischen verschiedenen Netzwerkteilnehmern entdecken kann. Stattdessen befinden sich alle auf gleicher Ebene und jeder Knoten kann beliebig mit jedem anderen Knoten im Netzwerk interagieren. In einem solchen Netzwerk gewinnen die Protokolle, also die allgemein gültigen Regeln, nach welchen man am Netzwerk teilnehmen und mit anderen interagieren kann, größte Bedeutung, da sie als allgemein verbindliche Standards die Funktionsfähigkeit der Netzwerkstruktur garantieren.

Was können uns nun aber die konzeptionellen Arbeiten von Dewey und Galloway über den NSA-Skandal und die politischen und sozialen Implikationen von Massenüberwachung durch staatliche Geheimdienste sagen? Meiner Meinung nach liegt hier eine große Bereicherung vor allem auf der strukturellen Ebene. Wenn wir diese konzeptuellen Arbeiten in Verbindung setzen mit einer konkreten empirischen Analyse, wie Überwachungstechnologien auf infrastruktureller Ebene operieren und technische Realitäten schaffen, können wir den NSA-Skandal nicht nur als Bestrebung, Individuen und deren Gedanken und Taten so detailliert wie möglich zu überwachen, verstehen, sondern als politisches Mittel, das durch Technik sozio-politische Strukturen zu schaffen und Machtpositionen zu erschaffen versucht.

Wenn wir uns nun weiter unten anschauen, wie die NSA-Überwachung tatsächlich funktioniert, sehen wir, dass sie erstens auf



Laura Fichtner

Laura Fichtner hat Elektro- und Informationstechnik in Karlsruhe und Philosophy of Science, Technology and Society in den Niederlanden studiert. Die hier vorgestellte Arbeit ist im Rahmen ihres Masters entstanden. Zurzeit forscht Laura zum Thema Überwachung und Cybersecurity im Internet der Dinge. Das nebenstehende Logo der Arbeit stammt von Eva Müller.

der Grundlage eines geopolitischen Machtvorteils operiert und diesen zweitens durch das von ihr angelegte Schattennetzwerk und zum Trotz anderweitiger Bestrebungen der *Open Source Community* weiter auszubauen versucht.

Doch die Idee, die Ursprung und Entstehung des Internets letztendlich geleitet hat, war eigentlich die Idee einer dezentralen Infrastruktur, die in ihrer Funktionsweise einem zentralisierten Angriff trotzen könnte. Diese Idee trieb *World-Wide-Web*-Begründer Berners-Lee dann weiter vorwärts.⁸ Die Entwicklung der *Hypertext Markup Language* (HTML) und der Internetprotokolle transformierten das Netzwerk der Netzwerke dann vollends zu einem verteilten Netzwerk, das jedem Teilnehmer gleiche Rechte eingesteht und die gleichen Regeln auferlegt, und das es so jedem gleichermaßen ermöglicht, mit jedem anderen beliebigen Netzwerkteilnehmer privat und Ende-zu-Ende zu kommunizieren oder Informationen für jeden zugänglich zu veröffentlichen.



Wie gestaltet sich eigentlich die Internet-Infrastruktur?

Wie bereits erwähnt, ist diese verteilte Netzwerkstruktur vor allem in den Protokollen des Internets eingebettet, zum Beispiel in der TCP/IP-Protocol-Suite. Diese Protokoll-Ebene ist eine logische Ebene, die die Regeln beschreibt, nach welchen der Austausch von Informationen zwischen zwei Netzwerkteilnehmern über das Internet erfolgen kann. Zu diesem Zweck bekommt jeder Netzwerkteilnehmer, das heißt jedes am Internet angeschlossene Gerät, eine eindeutig identifizierbare Adresse zugeschrieben, die wohlbekannte IP. Wenn nun ein Gerät eine Nachricht an ein anderes Gerät schicken möchte, so muss es diese Nachricht mit der Adresse des Empfängers kennzeichnen, ähnlich der Adresse auf einem Briefumschlag.

Das TCP (*Transmission Control Protocol*)-Routing-Protokoll legt dann fest, wie die Nachricht zum Empfänger kommt, nämlich indem sie von Router zu Router hüpf – jeder Router, jeder Knotenpunkt schaut sich die Adresse der Nachricht an und leitet diese weiter in die richtige Richtung. Das können wir uns wieder so ähnlich vorstellen wie bei der Post: zuerst wird auf den Ländercode geschaut, dann auf das Bundesland, die Gemeinde, den Ortsteil und schließlich Straße und Hausnummer. Durch diese Routingprotokolle wird die Idee des verteilten Netzwerkes, in dem jeder mit jedem gleichermaßen und nach den gleichen Regeln kommunizieren kann, dann zur Realität.⁹

Damit dieses verteilte Netzwerk allerdings technisch wirklich funktionieren kann, braucht das Internet neben diesen logischen Protokollen eben auch noch eine physisch-materielle Infrastruktur, die Informationen in Form von elektrischen oder optischen Signalen übertragen kann, genauso wie unsere verteilte postalische Kommunikation die Infrastruktur der Post, ihre Außenstellen, Sammelstellen und Verteilungszentren, LKWs und deren Autobahnen benötigt. Das Beispiel mit der Post zeigt uns indes auch gleich noch einen weiteren wichtigen Punkt: obwohl sich die logische, die Protokoll-Ebene, die es jedem erlaubt, eine Adresse zu haben und frei mit jeder anderen Adresse zu kommunizieren, als verteiltes Netzwerk gestaltet, kann es auf einer anderen Ebene der kommunikationstechnischen Infrastruktur durchaus zur Bildung zentralisierender Netzwerkstrukturen kommen.

Genauso verhält es sich auch mit der Internet-Infrastruktur. Wenn wir uns anschauen, wie Daten nach den Protokoll-Regeln übertragen werden und als Signale durch eine globale Infrastruktur an ihr Ziel huschen, können wir durchaus andere, dezentralisierte Netzwerkstrukturen entdecken. Da sind zum Beispiel die großen Unterseekabel, die es ermöglichen, Daten über Kontinente hinweg zu übermitteln und auszutauschen.¹⁰ Diese Kabel werden meist von einigen großen Firmen betrieben, und es gibt einige wenige dicke Kabel, die die meisten interkontinentalen Daten übertragen. Wenn diese das Festland erreichen, werden sie an großen Schaltstellen gebündelt und von dort aus weitergeleitet.

Dann gibt es weiterhin die großen IXPs, die *Internet Exchange Points*, von denen sich viele der wichtigsten in den USA und in Europa, also auf Boden NSA-Verbündeter, befinden.¹¹ Diese Internet Exchange Points fungieren als Hubs, an denen die meisten Internetkommunikationen zusammen geführt werden und von dort aus wieder weiter Richtung Endstation verteilt werden (ähnlich den großen Verteilungszentren der Post). Und dann gibt es natürlich noch die großen Internetriesen, Konzerne wie Google, Facebook und Microsoft, die das Marktmonopol vieler Internetservices innehaben und die Daten stellvertretend für ihre Kunden speichern.

Überwachung als Mittel einer infrastrukturellen Politik

Wenn wir uns nun einmal anschauen wollen, wie genau die Internetüberwachung der Geheimdienste überhaupt funktioniert, und das können wir mit Hilfe der Snowden-Dokumente jetzt eben auch, dann entdecken wir, dass diese vor allem auf die physische Ebene der Infrastruktur angewiesen ist, eben jene Ebene, wo es innerhalb einer dezentralisierten Dateninfrastruktur verschiedene Hauptknotenpunkte gibt. Ein kurzer Exkurs zurück zu Galloways Netzwerkdiagrammen macht klar, warum: Überwachung gestaltet sich innerhalb verteilter Netzwerke als besonders schwierig und aufwändig, da Kommunikation über eine große Anzahl beliebiger Pfade erfolgen kann – im Netzwerk gibt es keine zentralen Kontrollstellen, wo Informationsströme zusammenkommen oder von wo aus sie kontrolliert, verarbeitet oder verteilt werden.

Da ein solches Netzwerk in der Realität technisch aber schwer umzusetzen wäre, ist die physische Infrastruktur des Internets zu einer dezentralisierten Dateninfrastruktur gewachsen, wo die Knotenpunkte der Kabel- und Servicenetze sowie die IXPs wichtige Kontrollinstanzen darstellen. In solch einem dezentralisierten Netzwerk gestaltet sich Überwachung und zentralisierte Kontrolle wesentlich einfacher als in einem verteilten Netzwerk, da durch Anknüpfung an die Hauptknotenpunkte so gut wie alle Kommunikationen abgefangen werden können. Und genau hier setzt die NSA an, um ihr Schattennetzwerk der Überwachung zu errichten: da es für die NSA unmöglich wäre, alle einzelnen Internetteilnehmer an deren PC oder Server direkt anzuzapfen, abzuhören und zu überwachen, konnte sie sich die Knotenpunkte der materiellen Dateninfrastruktur des Internets zunutze machen.

So ist es kein Wunder, dass die NSA auf ihren internen Folien vermerkt, dass die meisten Internetkommunikationen durch die



USA fließen werden.¹² Korrekterweise weist sie darauf hin, dass damit auch zu rechnen sei, wenn der geographisch direkteste Weg nicht durch die USA führt: da die besten Kabel von und zu den Knotenpunkten in den USA führen, ist es für Internetprovider häufig ökonomisch günstiger, ihren ganzen Verkehr durch die USA zu schicken. Und hier kann die NSA ansetzen: da sie auf amerikanischem Boden freie Verfügungsgewalt hat, kann sie dann ganz gemächlich ihre Überwachungsgeräte an diesen Knotenpunkten installieren.

Das hat sie zum Beispiel bei AT&T in San Francisco gemacht.¹³ Wie wir vom ehemaligen Mitarbeiter Mark Klein bereits seit 2007 wissen, hatte sie dort ihren eigenen geheimen Raum beantragt, wo sie eine Kopie aller Internetkommunikationsflüsse mit einem Gerät namens Narus STA 6400 analysierte und von dort dann in ihr eigenes Überwachungsnetzwerk einspeiste. Um die geographische Bedeutung gewisser Knotenpunkte der Netzwerkinfrastruktur hervorzuheben, bildet die NSA auf einer anderen Folie als Hintergrund eine Landkarte des Verlaufes der Überseekabel ab.¹⁴ Dort weist sie dann auch ihre Mitarbeiter an, die beiden Überwachungsprogramme *Upstream* und *PRISM* parallel zu verwenden. Während *Upstream* die Daten, die vorbeifließen, direkt von den Glasfaserkabeln und der Infrastruktur sammelt, greift *PRISM* auf die Server der großen Internetkonzerne zu, die die vertraulichen Daten ihrer Kunden dort speichern. So kann die NSA mit ihren Überwachungsmethoden die großen Knotenpunkte der Infrastruktur angreifen, von wo aus sie dann eine Verbindung zu ihrer übergeordneten Kontrollstelle schafft.

Mit diesen Techniken ist es der NSA dann scheinbar erfolgreich gelungen, ein zentralisiertes Schattennetzwerk zu erschaffen, das oberhalb der normalen Infrastruktur operiert und erst einmal nicht in Datenflüsse eingreift oder sie manipuliert, sondern eigentlich „nur“ mithört. Dieses Netzwerk wird als Schattennetzwerk bezeichnet,¹⁵ da es zunächst einmal für uns als Nutzer unsichtbar bleibt und nicht in den Alltag des Internets einzugreifen scheint. Für uns Nutzer ist ja die materielle infrastrukturelle Ebene, die Ebene, die Datensignale überträgt, normalerweise eigentlich nicht Teil der Erfahrung des Cyberraums.

Was wir erfahren, ist ein verteiltes Netzwerk, in dem wir uns frei bewegen können, und in dem wir uns mit jeder anderen Teilnehmerin (prinzipiell) austauschen können. Solange die materielle Ebene nach Plan funktioniert und unsere Daten verlässlich und nach den festgelegten Regeln überträgt, müssen wir uns um sie nicht kümmern. Genauso kennen wir uns ja bei der Post eigentlich auch nicht genau aus mit der Geographie der Verteilungscenter oder -routen, und das müssen wir ja auch nicht, wenn wir einen Brief an eine beliebige Bekannte oder Unbekannte verschicken wollen. Im Gegensatz zur Post allerdings gibt es in den Internetprotokollen wesentlich weniger Regeln, die genau bestimmen, wer welche Nachricht lesen oder anschauen kann. Des Weiteren sind die digitalen Datenpakete wesentlich einfacher heimlich mitzulesen, da man diese auch samt Inhalt kopieren kann, ohne Spuren am Briefumschlag zu hinterlassen.

Allerdings heißt diese Transparenz, die die NSA-Überwachung auszeichnet, nicht, dass diese keine Auswirkungen auf uns und das Internet selbst hat – im Gegenteil! Ohne unser Wissen werden wir Teil eines zentralisierten Netzwerkes, das außerhalb un-

serer demokratisch legitimierten Ordnung operiert. In diesem Schattennetzwerk positioniert sich die NSA selbst an höchster Stelle, von wo aus sie das gesamte, globale Netzwerk übersieht und letztendlich auch kontrolliert. Zumindest in der Theorie kann die NSA so nun Informationen über jede normale Internetteilnehmerin abrufen, die Kommunikation jeder mit jeder heimlich mitlesen oder sogar Kommunikationsströme einfach abbrechen oder unbemerkt manipulieren.

Das hat sie in ihrem Programm *Quantumtheory*, welches Malware in normale Internetkommunikationen einschleust, auch getan.¹⁶ Die NSA selbst entzieht sich allerdings jeder Überwachung oder Kontrolle. Die Tatsache, dass ihr Schattennetzwerk unbemerkt und mit digitalen, also leicht und unbemerkt kopierbaren Daten operiert, unterstützt diese Dynamik zusätzlich. So werden wir als gemeinsam Überwachte im Sinne Deweys Teil einer politischen Öffentlichkeit mit all denen, die mit uns durch das Netzwerk verbunden werden und unser Schicksal teilen.

Wenn die NSA dann die Form dieses Netzwerkes bestimmt, und dort an höchster Instanz steht, dann hat sie de facto Politik im Deweyschen Sinne gemacht, denn sie hat eine gewisse Netzwerkstruktur geschaffen, die Austausch und Interaktionen innerhalb der Infrastruktur auf eine bestimmte Weise gestaltet, bestimmt und kontrolliert. Auf Grund der Geheimhaltung dieser globalen Überwachungskanäle allerdings geschieht diese Politik, diese Regulierung, nicht in einer Weise, die laut des hier beschriebenen Ansatzes als demokratisch verstanden werden kann. Zum einen findet hier keinerlei öffentlicher Diskurs statt, an welchem die betroffene Öffentlichkeit teilnehmen und somit mitentscheiden kann, oder durch welchen sie ihre Vertreter kontrollieren kann. Zweitens sehen wir hier einen nationalen Sicherheitsdienst, der im Interesse einer Nation die Gestaltung eines globalen Netzwerkes anstrebt: das heißt, dass die Politik, die die Interaktionen im Internet mitgestaltet und formt, nicht im Interesse aller Beteiligten, sondern im Interesse einer Minderheit handelt.

Die gängigen Anti-Überwachungsmaßnahmen wie Verschlüsselung und Onion-Routing versuchen diesen Tendenzen entgegenzusteuern. Indem sie Überwachung auf der infrastrukturellen Ebene durch ein unlesbar Machen der übertragenen Nachrichten erschweren, versuchen sie so dem zentralisierenden Moment der Überwachung entgegenzuwirken und ein verteiltes Netzwerk zu schaffen, in dem wir frei und ungestört kommunizieren können. Allerdings tun sie das auch nicht unbedingt immer auf eine demokratische Art und Weise, sondern schaffen, genauso wie die NSA, mit Hilfe von Applikationen technische Realitäten.

Staatliche Überwachung – nur eine Frage der IT-Sicherheit und Privatsphäre?

Solche Betrachtungen eröffnen die Möglichkeit, die NSA-Affäre nicht nur unter den Aspekten von Privatsphäre, innerer Sicherheit und Cybersecurity zu betrachten, sondern staatliche Überwachung als politisches Mittel zu begreifen, das gewisse Machtverhältnisse innerhalb einer globalen Online-Gesellschaft zu schaffen sucht. Die Analyse, die ich in meiner Arbeit gemacht habe, hat gezeigt, dass es möglich ist, in der NSA-

Affäre strukturelle Aspekte zu identifizieren, die zeigen, wie solche Überwachungsmethoden auf den strukturellen Aufbau des globalen Netzwerkes abzielen. Indem sie ein zentralisiertes Schattennetzwerk kreieren, suchen sie gewisse globale geopolitische Bestrebungen ins Internet zu übertragen und dort zu verfestigen.

Im Sinne der von mir bemühten politischen Philosophie John Deweys können diese Bestrebungen dann insofern als politische Aktivitäten verstanden werden, als sie die infrastrukturelle Form des Internets mitgestalten und somit abzielen auf eine großflächige Regulierung der Interaktionen der globalen Öffentlichkeit, welche durch das Internet erst so geschaffen wurde. Die von Galloway beschriebenen Netzwerk-Topologien helfen uns zu verstehen, wie dieses strukturelle Formen der Netzwerkcharakteristika geschehen kann. Hier nützten die Überwachungsorgane selbst die bereits vorhandenen Knotenpunkte der dezentralisierten materiellen Internet-Infrastruktur aus, um darauf ihr zentralisiertes Schattennetzwerk aufbauen zu können. Insofern geht es nicht nur um die Frage, wer auf welche Informationen über welche Individuen zugreifen oder wessen persönliche E-Mails mitlesen kann oder inwiefern Möglichkeiten zur privaten Kommunikation geschwächt werden. Vielmehr geht es auch darum, wer Kontrolle über ein Netzwerk und dessen Interaktionen ausüben kann und welche Machtstrukturen in der Internet-Infrastruktur implementiert werden.

Anmerkungen (→ Links in der online-Ausgabe abrufbar)

- 1 Frontline PBS (2014, 13. Mai). *United States of Secrets*. Video-Datei, →
- 2 Fichtner, L. (2014). *Masterarbeit Philosophy of Science, Technology and Society*. →
- 3 Dewey, J. (1927). *The public and its problems: An essay in political inquiry*. Athens, OH: Swallow Press/Ohio University Press
- 4 Dewey (1927), S. 82
- 5 Dewey (1927), S. 16, p. 27
- 6 Galloway, A. (2004). *Protocol: How control exists after decentralization*. Cambridge, MA: The MIT Press
- 7 Galloway (2004), S. 11–12, 30–31
- 8 Berners-Lee (1999). *Weaving the web: The original design and ultimate destiny of the World Wide Web by its inventor*. New York, NY: HarperCollins
- 9 Blum, A. (2012). *Tubes: A journey to the center of the internet*. New York, NY: HarperCollins
- 10 TeleGeography (2014). *Submarine Cable Map 2014*. →
- 11 TeleGeography (2012). *Global Internet Map 2012*. →
- 12 The Guardian (2013, 1. November). *NSA Prism program slides*. →
- 13 Klein, M. (2007, 15. Mai). *Spying on the home front* (Interviewer H. Smith). →
- 14 The Washington Post (2013, 6. Juni). *NSA slides explain the PRISM data-collection program*. →
- 15 Appelbaum, J.; Horchert, J.; Reißmann, O.; Rosenbach, M.; Schindler, J.; Stöcker, C. (2013, 30. Dezember). *Neue Dokumente: Der geheime Werkzeugkasten der NSA*. SPIEGEL ONLINE NETZWELT, →
- 16 SPIEGEL ONLINE (2013, 30. Dezember). *NSA-Dokumente: So übernimmt der Geheimdienst fremde Rechner*. →



Angela Meindl

Internet-Profilung – Umfang, Risiken und Schutzmaßnahmen am Beispiel Google

FIF-Studienpreis 2015
3. Preis

Einen weiteren dritten Preis des FIF-Studienpreises hat die Autorin für ihre Bachelorarbeit erhalten. Es geht darin um das Thema Datensammeln. Am Beispiel von Google wird gezeigt, wie Daten von Internetnutzer:innen unbemerkt gesammelt werden und wie diese Daten genutzt werden können. Sie befasst sich mit der Frage, welche Risiken dadurch entstehen können und welche Möglichkeiten des Schutzes bestehen. Ausführlich hat die Autorin über ihre Arbeit bereits in FIF-Kommunikation 2/2015 berichtet.¹ Wir bringen deshalb an dieser Stelle einen von der Redaktion gekürzten zusammenfassenden Bericht über ihren Inhalt.

Internet-Profilung nennt man den Vorgang, über Menschen, die sich im Internet bewegen, möglichst differenzierte Informationen zu sammeln und diese in einem Persönlichkeitsprofil zusammenzuführen. Dafür werden nicht nur die Daten gesammelt und gespeichert, die beim Ausfüllen eines Formulars absichtlich preisgegeben werden. Mit Hilfe verschiedener Techniken, die beim Besuch einer Webseite nicht unmittelbar bemerkt werden, kann der Weg der Internetnutzer:innen durch das Internet verfolgt und dokumentiert werden. Begründet wird dieses Verfahren mit gezielterem personenbezogenem Inhalt, mit einer Verbesserung der Usability, mit der Erhöhung der Effektivität von Webseiten und mit der Analyse von Werbekampagnen.

Die Arbeit geht zunächst darauf ein, mit welchen Techniken Daten gesammelt werden. Sie beschränkt sich darauf, exemplarisch die bekanntesten Dienste von Google zu untersuchen. Dort werden Daten mittels Zählpixel, Logdateien, Skripten und

Cookies gesammelt. Die Techniken werden im Einzelnen beschrieben. Mit ihrer Hilfe werden nicht nur Aktivitäten der Nutzer:innen wie Suchbegriffe, aufgerufene Webseite, Referrer und benutzte Suchmaschine, sondern auch viele Informationen über das benutzte Computersystem eingesammelt. Diese Datentypen werden in der Arbeit zusammengestellt. Aus diesen Informationen lässt sich ein *Browserfingerprint* erstellen. Nach einer Studie von Henning Tillmann² sollen Browserfingerprints mit einer Wahrscheinlichkeit von bis zu 92,57 % auf die zugehörige Person hinweisen.

Weiter geht die Arbeit auf das *Targeting* ein, das heißt, auf das Ziel der Auswertung der eingesammelten Daten. Mit *Mouse-Targeting* wird das Leseverhalten auf der Webseite analysiert. Mit *Geo-Targeting* wird der Standort des Nutzers ermittelt. Die wichtigste Rolle spielt das *Behavioural-Targeting*. Alle erhobenen Daten und die daraus gewonnenen Analyseergeb-



nisse landen ohne Wissen der Nutzer:innen in der Datenbank des Tracking-Servers. Google benutzt diese Techniken des Datensammelns für mehrere Dienste, natürlich für die Suche, aber auch für Google+, Google Analytics, Picasa und YouTube. In der Arbeit werden diese Anwendungen untersucht. Im Übrigen beschreibt Google auf seinen Hilfe-Seiten und in seinen Datenschutzrichtlinien, wie und wo von Google Daten gesammelt werden und dass sie an Dritte weitergegeben werden.³ Wie zielgenau die so gesammelten Informationen eine Person identifizieren, wird am Beispiel „Thelma Arnold“ gezeigt, das 2006 in den USA Schlagzeilen gemacht hat.

Wir Nutzer:innen haben keinerlei Kontrolle mehr über die über uns gesammelten Daten. Daraus ergeben sich vielschichtige Probleme sowohl auf politischer, auf wirtschaftlicher und insbesondere auf privater Ebene. Auf der politischen Ebene befasst sich die Arbeit vor allem mit dem Datenschutz und mit dem Problem, dass nationale Gesetze nur gelten, solange die Datenflüsse die nationale Grenze nicht überschreiten. Für Privatpersonen ergibt sich ein breites Spektrum an Gefährdungen, denn überall, wo digitale Spuren hinterlassen werden, können Andere sie nutzen – und missbrauchen.

Die Frage stellt sich, ob Profiling nicht verzichtbar ist. Sie wird in der Arbeit unter dem Aspekt der nicht gewollt zur Verfügung gestellten Daten beleuchtet. Kenntnis der technischen Ausstattung ist interessant für eine Optimierung der technischen Seitendarstellung, Kenntnis des Benutzerverhaltens dient der Optimierung der inhaltlichen. Zweifel sind angebracht, ob für alle diese Zwecke ein direkter Bezug zur Person notwendig ist. Geprüft wird in einem Test, ob es möglich ist, die für die genannten Zwecke benötigten Daten personenunabhängig zu erheben und ohne sie an Dritte weitergeben zu müssen. Zum Einsatz kamen die Open-Source-Tools *Piwik*⁴ als Alternative zu Google Analytics und *AdServer Revive*⁵ als Alternative zu Google AdWords. Beide Programme wurden auf einem lokalen Webserver ohne Internetzugang installiert, um sie auf ihre Integrität zu testen – mit positivem Ergebnis.

Die Arbeit setzt sich dann damit auseinander, wie sich Profiling mit Datenschutz verträgt. Das deutsche Datenschutzrecht gilt als das strengste der Welt. Unter der Vielzahl einzelner Gesetze und Regelungen dieses Gesetzeswerks sind die wichtigsten das Telemediengesetz, das Recht auf Informationelle Selbstbestimmung und das Gesetz zur Vorratsdatenspeicherung. Das Telemediengesetz besagt, dass personenbezogene Daten nur genutzt werden dürfen, wenn die betroffene Person vor dem Nutzungsvorgang über Art, Umfang und Zweck der Erhebung und Verwendung in verständlicher Form unterrichtet wurde, auch wenn die Daten außerhalb der EU verarbeitet werden. Die

Nutzerin muss ihre Einwilligung bewusst und eindeutig erteilt haben. Das Recht auf Informationelle Selbstbestimmung geht noch weiter, indem jede Bundesbürgerin und jeder Bundesbürger das Recht haben, selbst zu bestimmen, wem sie Informationen über sich preisgeben. Diese Rechte werden durch Profiling eindeutig verletzt. Eingeschränkt werden diese beiden Rechte außerdem durch die Vorratsdatenspeicherung, die alle Medienanbieter dazu verpflichtet, Verkehrsdaten in ihrer Infrastruktur für einen festgelegten Zeitraum zu speichern.

Das Europäische Datenschutzrecht hat bisher eher die Funktion, für alle Mitgliedstaaten einen gemeinsamen Mindeststandard zu schaffen. Anders als im deutschen und im europäischen Datenschutzrecht sieht es im US-amerikanischen Datenschutz aus. Dort setzt man auf Selbstverpflichtung. Datenschutzinformationen müssen nur korrekt und zugänglich beschrieben werden. Stellen sich Angaben als falsch heraus, droht eine Verwarnung und die Auflage, ein Pflichtenheft zum Umgang mit den Daten zu entwickeln, an das man anschließend gebunden ist. Erst nach einem Verstoß gegen das selbst entwickelte Pflichtenheft kann die Justiz tätig werden. In diesem Rahmen weist auch Google darauf hin, dass alle Daten gesammelt werden, die sie bei der Nutzung ihrer Dienste von ihren Nutzern bekommen können. Sie vernebeln dies jedoch durch umfangreiche und komplizierte Formulierungen. Auch räumt man dort das Recht auf Änderung fehlerhafter personenbezogener Daten ein, schränkt aber dessen Umsetzung ein. Daten in den Sicherungssystemen werden nie gelöscht. Google verschweigt auch nicht, dass personenbezogene Daten an „vertrauenswürdige Dritte“ zur Verarbeitung weitergegeben werden. Strafen für Verletzungen selbst der US-amerikanischen Bestimmungen halten Google nicht davor zurück.⁶ Konformität mit dem deutschen Datenschutzrecht löst Google mit dem Hinweis, dass bereits mit der Nutzung seiner Dienste die Zustimmung erteilt wird.

Die Arbeit stellt resümierend fest, dass es nicht länger akzeptiert werden darf, dass Daten von Internetnutzer:innen unbemerkt erhoben und gespeichert werden. Ohne eigentliche Notwendigkeit werden alle, die an dieser für unsere Gesellschaft mittlerweile unverzichtbaren Infrastruktur teilhaben wollen, zu einer partiellen Preisgabe ihrer Privatsphäre genötigt und einer latenten Gefährdung ausgesetzt. Auf der Seite der Akteure wird im Gegenzug an unserer Privatsphäre kräftig verdient. Als eine mögliche Gegenmaßnahme zur Wahrung der informationellen Selbstbestimmung wird in der Arbeit vorgeschlagen, u. a. für das Tracking und Profiling ein Double-Opt-in-Verfahren einzuführen, ähnlich wie es bei Newslettern schon gesetzmäßig vorgeschrieben ist. Praktische Vorschläge werden gemacht, wie das Verfahren umgesetzt werden könnte. Lehnt man z. B. das Tracking ab, könnte eine ungetrackte Version der Website geöffnet werden. Auch müsste es



Angela Meindl

Angela Meindl, B. Sc., ist Medien-Informatikerin aus Bremen
Kontakt: a.meindl@artinfakt.de

einen Link zu einer Seite geben, auf der angezeigt wird, welche Daten gespeichert werden und welche persönlichen Informationen bereits gespeichert worden sind. Dort muss eine Möglichkeit zur Korrektur fehlerhafter Angaben gegeben sein und auch das Löschen aller gespeicherten Daten inklusive der an Dritte weitergegebenen beauftragt werden können.

Eine dringende Aufgabe ist es, an einem internationalen Datenschutzrecht für das Internet zu arbeiten, das für die Anbieter von Internetseiten verbindlich sein muss. Dazu ist die Institutionalisierung einer umfassenden Kontrollinstanz sowie die Definition eines wirkungsvollen Maßnahmenkataloges gegen Verstöße notwendig, ohne diese ein solches Recht nicht durchzusetzen sein wird.

Anmerkungen (→ Links in der online-Ausgabe abrufbar)

- 1 Meindl, Angela (2015): Internet-Profiling. In: *FlFF-Kommunikation*,
2/2015, 45–49
- 2 Tillmann, Henning (2013): *Browser Fingerprinting: Tracking ohne Spu-
ren zu hinterlassen*. Diplomarbeit, Humboldt-Universität zu Berlin. ➔
- 3 Google (2016): *Google-Nutzungsbedingungen*. ➔ (Stand: 22.03.2016)
- 4 Piwik (2014): *Liberating Web Analytics*. Version 16.06.2014. ➔
- 5 Revive (2016): *About Revive Adserver*. ➔
- 6 Spiegel-Online (2012): *Datenschutz-Verstoß: Google zahlt Rekordbuß-
geld*. SPIEGEL ONLINE Netzwelt, 09.08.2012. ➔

**FIF e. V.**

Das FIF verlieht 2016 wieder den

FlfF-Studienpreis

für herausragende Abschlussarbeiten aus dem Bereich Informatik und Gesellschaft.

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

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

Wir laden dazu ein, geeignete Arbeiten bis 15. Juni 2016 einzureichen.

Das Preisgeld beträgt:

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



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

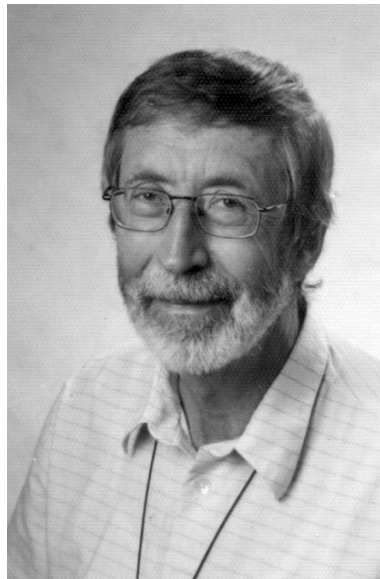
Einreichungen bitte bis zum 15. Juni 2016 an:

Fiff-Geschäftsstelle
– Studienpreis 2016 –
Goetheplatz 4
28203 Bremen
oder (vorzugsweise) per E-Mail an studienpreis@fiff.de.
Weitere Details unter <http://www.fiff.de/studienpreis>.

Der Preis wird in einer Feierstunde im Rahmen der 32. FlfF-Konferenz 2016 verliehen, die vom 25. bis 27. November in Berlin stattfindet.

Das FlfF trauert um Dirk Siefkes

* 1938 † 2016



Wenige Wochen vor seinem 78. Geburtstag verstarb Dirk Siefkes am 19. März 2016 nach schwerer Krankheit. Er war dem FlfF als Beiratsmitglied eng verbunden und hat über Jahrzehnte hinweg immer wieder Stellung zu Themen aus Informatik und Gesellschaft bezogen – insbesondere auch mit vielen Beiträgen in der *FlfF-Kommunikation*. Er studierte Theologie und später Mathematik und promovierte 1969 an der Universität Heidelberg mit einer Dissertation in mathematischer Logik.

Nach einem Forschungsaufenthalt in den USA nahm er 1973 einen Ruf der Technischen Universität Berlin auf eine Professur für Theoretische Informatik an, die er bis zu seiner Emeritierung 2003 innehatte. Über zwei Jahrzehnte lang konzentrierte sich seine Forschung auf ausgewählte Themen der Theoretischen Informatik. In den 1980er Jahren verlagerte sich sein Interesse weg von der mathematischen Fundierung hin zu einer humanwissenschaftlichen Grundlegung der Informatik. Anfangs motiviert, Lehrformen zu erproben, die mehr am Menschen als am Wissen orientiert sind, wendete er sich *kleinen Systemen* zu.

In einer Reihe von Veröffentlichungen hat er die von E. F. Schumacher entwickelte Kritik der westlichen Ökonomie, wie sie 1973 in der Essay-Sammlung *Small is Beautiful* formuliert ist, auf die Informatik übertragen. Kleine Systeme sind ein Gegenkonzept zu dem in der Informatik weit verbreiteten Hang zum Gigantismus, der in Begriffen wie „programming in the large“, „very large data bases“ und neuerdings „big data“ zum Ausdruck kommt und zu unzuverlässigen, undurchschaubaren, unbeherrschbaren und überbewerteten Informatiksystemen führt. Diese Überlegungen sind eingebettet in den umfassenderen Versuch, gemeinsam mit Wolfgang Coy, Frieder Nake, Jörg-Martin Pflüger, Arno Rolf und anderen eine *Theorie der Informatik* zu entwickeln.

Sein Hauptwerk ist die *Sozialgeschichte der Informatik*, die in einem von ihm geleiteten interdisziplinären Forschungsprojekt unter Mitarbeit von Peter Eulenhöfer, Heike Stach und Klaus Städtler entwickelt wurde. Parallel dazu leitete er in den 1990er Jahren das Studienreformprojekt *Geschichte als Zugang zur Informatik*. Mehr über seine Projekte und seine Publikationsliste findet man unter <http://tal.cs.tu-berlin.de/siefkes/>.

Dirk Siefkes gehörte zu den Persönlichkeiten, von denen es in der heutigen Wissenschaftslandschaft nicht mehr allzu viele gibt. Er bestach durch seine Aufrichtigkeit und Menschlichkeit. Er hat nicht wie so viele andere die kritische Reflexion der Jagd nach Drittmitteln, dem Konkurrenzkampf um Ruhm und Einfluss und dem Schielen nach öffentlicher Anerkennung geopfert. Er hat seine Ideen und Vorstellungen von einer kulturellen Theorie der Informatik gegen viele Widerstände und gegen das technokratische (Miss-)Verständnis der übergroßen Mehrheit in der Informatik unerschütterlich verfolgt und propagiert. Die Informatik hat eine ihrer nachdenklichen Stimmen verloren. Das FlfF wird sein Vermächtnis in Ehren halten.

Was ist so faszinierend an der Informatik?

Nach rückwärts wird in der Informatik der Blick selten gewandt, und auch nach vorwärts nicht so häufig, wie es scheint. Technik und Wissenschaft um den Computer verändern sich so rasend schnell, daß alle genug damit zu tun haben, die Füße auf dem Boden zu halten. Vergangenes ist veraltet und Zukünftiges höchstens in Visionen sichtbar; beides hat keinen echten Bezug zur Gegenwart. Im Projekt Sozialgeschichte der Informatik wollten wir aus der Untersuchung vergangener Entwicklungen die gegenwärtigen verstehen, um sie besser beeinflussen zu können und damit zu den zukünftigen beizutragen.

retrospektive

Ich habe die Arbeit des Projekts als Sprecher begleitet. Zugang zu der Thematik hatte ich von meiner langjährigen Auseinandersetzung mit Formalisierung als einem Hauptwerkzeug informatischen Tuns her. Ein evolutionäres Lernmodell, das ich aus Ansätzen in der Kybernetik gewonnen hatte (Siefkes 1991), erwies sich mir als verlässliches Hilfsmittel, die Entwicklung und die Ergebnisse des Projekts zu verstehen und für weitere theoretische Arbeit zu nutzen; erst dadurch wurde die soziale Komponente des Modells explizit. Vertraut mit *kleinen Systemen* (Siefkes 1992a) rückte ich Geschichten in das Zentrum geistiger Entwicklung (Siefkes 1994) und (kleine) Gruppen in das Zentrum sozialer, insbesondere wissenschaftlicher und technischer, Entwicklung (Siefkes 1998b). Sie sind die Sinneinheiten, in denen wir – getragen und beschränkt von starren Formen in uns und um uns – »lernen, leben und arbeiten« und dadurch diese Bedingungen und Möglichkeiten verändern (Siefkes 1997).

Auch für meine praktische Arbeit als Hochschullehrer hat das Projekt vielfältige Konsequenzen gehabt, die weiterzugeben mir wichtig ist. Die Lehre in der Informatik sehe ich als in ihrem Kanon konservativ und in ihrem aktuellen Angebot modeabhängig – beides, weil eine Standortbestimmung in der Informatik so schwierig erscheint. Eine breitere Sicht ist notwendig. Deswegen arbeite ich in meinen Lehrveranstaltungen die unterschiedlichen Sichtweisen auf den Stoff heraus, ordne ihn insbesondere in die historische Entwicklung ein. Nicht zufällig ist jetzt ein Studienreformprojekt zum Thema *Geschichte als Zugang zur Informatik* bei mir angesiedelt. In der Forschung gibt es eine gewisse Tradition, die Entwicklung nicht nur am jeweiligen technischen und wissenschaftlichen Stand festzumachen, sondern mögliche soziale und kulturelle Folgen einzubeziehen und auch darüber hinaus die Erkenntnisse anderer Disziplinen zu nutzen. Diese Tradition kann durch die Einsicht gestärkt werden, daß die Informatik nicht nur mit anderen Bereichen verflochten ist, sondern in ihrer Entwicklung von kulturellen und sozialen Strömungen getragen wird.

In der vorliegenden Arbeit ordne ich das Konzept der Hybridobjekte in diesen sozial- und erkenntnistheoretischen Rahmen ein. Die Mitarbeiter des Projekts haben es aus der Analyse informatischer Texte gewonnen und zur Rekonstruktion von Orientierungen verwendet, die in der Entwicklung der Informatik eine Rolle gespielt haben und spielen (Eulenhöfer 1998b, Stach 1998b). In Hybridobjekten sind zueinander duale und daher unverträgliche Formen, die nur in Prozessen verschmelzen können, auf versteckte Weise in eins gedacht. Das erlaubt Informatikern, zwischen unterschiedlichen Sichtweisen unversehens hin- und herzuwechseln und so gegensätzliche Weisen des Zugangs zu ihren Objekten zu kombinieren. Darin sehe ich die Faszination informatischen Arbeitens. – Ich schließe direkt an meine Arbeit (Siefkes 1998a) an, in der ich die Dualismen analysiere, die unsere Kulturgeschichte durchziehen und sich auch in der Informatik niedergeschlagen haben.

Faszination an Beweisen und Programmen

Neulich ist mir ein Beweis zusammengebrochen. Turing hat die Unentscheidbarkeit des Halteproblems schon 1936 bewiesen; aber in meiner Darstellung im Skript war ein Fehler. Ein aufmerksamer Mitarbeiter entdeckte ihn, und ich konnte ihn nicht reparieren. Ich bastelte stundenlang, wurde unleidlich, meine Familie ging auf Abstand. Am nächsten Morgen unter der kalten Dusche kam mir die rettende Idee. Ich hatte eine Kleinigkeit übersehen, eine Codierung nicht richtig verstanden. Jetzt konnte ich die Stelle berichtigen, den Beweis wieder herstellen; er wurde schöner als vorher.

Was fasziniert uns an einem mathematischen Beweis? Mathematische Gegenstände sind abstrakt, noch abstrakter als Zahlen. Mathematische Beweise sind formal, sie beziehen sich nur auf diese Abstraktionen, haben keinen Bezug zur Realität. Gefühle haben da nichts zu suchen. Der Beweis ist uralte, ich habe ihn nicht selbst geschrieben, nur einen vorgegebenen ein bißchen anders dargestellt.

Trotzdem hat mich die Geschichte so mitgenommen. Der Hinweis auf den Fehler hat mich zunächst nicht beunruhigt. Erstmal sehen. Auch als ich den Fehler selber sah, blieb ich gelassen. Das ist mir, sogar bei diesem Beweis, schon oft passiert; das kriege ich hin. Fehler finden und eliminieren ist der beste Weg zu einem tieferen Verständnis. Erst als das Problem sich als hartnäckig erwies, als alle Versuche immer wieder auf dasselbe Dilemma führten, das auf beiden Seiten nur eine Sackgasse ließ, stieg eine seltsame Mischung aus Wut (über die verlorene Zeit), Angst (»Ich krieg's nicht hin.«), trotziger Freude (»Vielleicht ist der Beweis wirklich falsch. Auch Turing kann sich irren. Dann werden wir berühmt.«) und Verzweiflung (»Ich werde zu alt für Mathematik.«) in mir hoch. Der Beweis sog mich ein, ich verschwand aus der Welt.

Der Beweis wurde mein Baby. Und wie ein krankes Kind nahm er mich ganz gefangen. Schlimmer noch: Ein Kind, das ich pflege, hat seine eigenen Stärken und Schwächen; ein Möbel, das ich baue, hat seine geraden Kanten und krummen Touren. Für meinen Beweis bin ich allein verantwortlich. Den Formalismus hat ein anderer erdacht, sogar den ursprünglichen Beweis; aber ich habe mir beide zu eigen gemacht, die Brücken nach draußen sind abgebrochen, ich habe mich selbst in dem formalen Gemäuer eingesperrt. Der Beweis ist nicht mein Baby, er ist Teil meiner selbst geworden. Der Beweis ist in mir, und ich bin im Beweis.

Programmieren absorbiert noch mehr als Beweisen. Zwar arbeite ich an einer Maschine, am »Rechner«, und diese Maschine empfinde ich als höchst widerständig. Sie übersieht keine Kleinigkeit, macht unerbittlich genau die Schritte, die ich ihr vor-

schreibe. Und wenn ich mir beim Schreiben etwas anderes gedacht habe, kommt es sofort heraus – wenn ich Glück habe; wenn ich Pech habe, erst später bei einer kritischen Anwendung. Aber die Maschine ist nur das Medium, durch das ich das Gedankengebäude kontrolliere, indem sie es realisiert und so Fehler erkennbar macht. Wie beim Beweisen habe ich mich auf einen Formalismus eingelassen, hier eine Programmiersprache, und bin allein verantwortlich, wenn mein geistiges Baby falsch läuft.

Das Laufen macht den Unterschied! Mathematische Gegenstände bewegen sich nicht; mathematische Aussagen stellen formale Sachverhalte auf, mathematische Beweise zurren sie fest. Mathematiker formalisieren; das heißt, sie gießen Flüssiges in feste Formen. Informatiker programmieren; das heißt, sie schreiben vor, wie Programme – früher für Rechnungen, heute für ganze Systeme – ablaufen sollen. Die Aufgaben und die Ergebnisse sind formal wie in der Mathematik, auch die einzelnen Schritte. Aber das Programm soll laufen, nicht stehen.

Natürlich ist das kein Gegensatz, nicht einmal ein klarer Unterschied. Rechenverfahren sind neben Beweisen der eigentliche Gegenstand der Mathematik. Und die ersten »Informatiker« – damals hießen sie nicht so – waren überwiegend Mathematiker, die daran arbeiteten, ihre immer aufwendiger werdenden Berechnungen von Maschinen durchführen zu lassen (Eulenhöfer 1998b). Aber damit entfernten sie sich zunehmend von den »reinen« Mathematikern, die zur gleichen Zeit die »moderne« Mathematik immer stärker auf Strukturen gründeten, also auf Unveränderliches.

Hybridobjekte in der Informatik

Informatiker arbeiten mit formalen Gebilden, die sich schrittweise bewegen. So klingt es zumindest in ihren Beschreibungen. John von Neumanns erster Entwurf eines Elektronenrechners »hat Organe« für Ein- und Ausgabe, für Rechnen und Speichern und für die Steuerung. Die Organe »bestehen aus Neuronen«, bilden also ein Gehirn, das selbständig entscheidet und Befehle ausführt. Gleichzeitig bilden sie eine Maschine; ausführlich diskutiert von Neumann die Probleme der technischen Realisierung. Und schaltet und waltet doch mit der organischen Geistmaschine, als wäre es ein mathematisches Konstrukt. So lese ich Heike Stachs Analyse (Stach 1998b). Von Neumann geht es wie mir, denke ich; er versetzt sich selber, den rechnenden Organismus, in die Maschine, die er entwirft. Er ist in der Maschine und die Maschine in ihm. Ein »Hybridobjekt«.

Von Neumann steht damit in der Tradition Alan Turings, der in seiner Dissertation (1936–37) einen Formalismus, in dem man alle Berechnungen darstellen kann, als eine Maschine beschreibt. Turing fängt an: »Wir können einen Mann, der gerade eine reelle Zahl berechnet, mit einer Maschine vergleichen, die ...«. Und begründet seine Definition aus den Tätigkeiten des Mathematikers und aus den Eigenschaften des menschlichen Gehirns. Die Maschine bleibt auf dem Papier, aber sie bewegt sich wie ein rechnender Mathematiker. Und bewegt damit die Herzen von Mathematikern. Der Logiker Alonzo Church hatte schon vorher die These aufgestellt, durch andere, äquivalente Formalismen seien alle Berechnungen adäquat erfaßt. Davis vermutet, erst Turings Maschine habe Gödel davon überzeugt (Davis 1982). Maschinen,

die wie Mathematiker rechnen, wirken stärker als Formalismen, in denen Rechnen durch Regeln festgelegt wird. In dem Sinn ist Turing der erste Informatiker, obwohl zweifelhaft ist, ob er die Rechnerentwicklung wirklich beeinflusst hat (Heintz 1993, Kap. 7).

Hybridobjekte ganz anderer Art entdeckt Eulenhöfer in der Entwicklung von Computern und der Entstehung der Informatik in der Bundesrepublik Deutschland (Eulenhöfer 1998b). Die neuen »Rechenautomaten« wurden als Automatisierungen der damals üblichen Rechenbüros gesehen; sie vereinigten also in sich die Fähigkeiten herkömmlicher Tischrechenmaschinen und ihrer Bedienerinnen. Zur Zähmung dieser faszinierenden Gebilde war eine neue Zunft von Mathematikern nötig, die mit ihnen umgehen konnten. Fünfzehn Jahre später konnten die Verfechter dann argumentieren, daß die Monster nicht nur Zahlen, sondern Information verarbeiteten, also von solcher allgemeinen Bedeutung seien, daß eine neue Disziplin, »Informatik«, geschaffen werden müsse (Eulenhöfer 1998a).

Ökologische Wissenschaft

Welche Vorstellung von Wissenschaft liegt dem zugrunde? Üblicherweise wird wissenschaftliches Arbeiten als Zerlegen, Klassifizieren, Hierarchisieren verstanden (Siefkes 1993b). Ich zerlege vorgefundene Sachverhalte, bis sie unter meine Begriffe passen, und setze sie neu zusammen, wie es meinem angesammelten Wissen entspricht; mache ich das mit genügender Ausdauer, erhalte ich eine Theorie, die weiteres Zerlegen und Zusammensetzen erleichtert und bestimmt. Und so weiter.

Gegenstände und Begriffe, Wissen und Theorien sind aber »Repräsentationen«: Formen, die aus Prozessen entstehen, die in früheren Formen ablaufen, und so weiter. Begriffe sind innere Repräsentationen unseres Denkens, so wie das Leben von Fischen durch die Gene, die sie in sich tragen, repräsentiert wird. Dinge und Lebewesen sind äußere Repräsentationen von Naturvorgängen und menschlichem Handeln, so wie das Leben von Fischen durch die Welt, die sie von außen trägt, repräsentiert wird. Wissen verbindet beides. Von außen betrachtet repräsentiert es unser Denken, von innen betrachtet unser Handeln.

So statisch betrachtet sind *Geist* und *Welt* zwei getrennte Bereiche, die über das Wissen durch Handeln und Wahrnehmen verbunden sind. Kommunizieren ist ein geistiger Vorgang: Mit Hilfe von Zeichen, externalisierten Verweisen auf die Welt, tauschen Geister Botschaften aus; folgen wir den Wegweisern, erfahren wir etwas übereinander und die Welt. Wer »wir« sind, bleibt unklar.

Repräsentationen sind aber dynamisch: Formen entstehen aus Prozessen und ermöglichen und bestimmen neue Prozesse. So gehen Geist und Welt auseinander hervor, aus drinnen wird draußen, aus draußen wird drinnen. Wenn wir kommunizieren, tauschen nicht Geister Repräsentationen aus, sondern verschmelzen geistige Prozesse für einen kreativen Moment. Das habe ich in langen streitbaren Auseinander- und Zusammensetzungen mit meiner Frau gelernt und oft beschrieben (z. B. Siefkes 1995): Beim Zuhören nehme ich nicht ihr Wissen auf, sondern sage lautlos die Frage, die sie gerade beantwortet. Beim Reden schiebt sie nicht Wissen über den Tisch, sondern horcht auf die Frage, die sie mich gerade stellen läßt.

In diesem ökologischen Modell von Lernen und Lehren (Siefkes 1991) sind also die Schüler nicht leere Gefäße und die Lehrer nicht volle Flaschen. (Wer hält bloß den Trichter?) Der Lehrer wird auch nicht auf das Umfeld der Schüler reduziert, dem sie sich anzupassen haben, wenn sie überleben wollen, oder das sich ihnen anzupassen hat, wenn er sein Lehrziel erreichen will. Im ökologischen Modell sind Lehrer und Schüler Menschen, die einen Weg geistig gemeinsam gehen wollen. Eine gute Lehrerin kennt viele Wege und sucht nach solchen, die für die Schüler gangbar sind. Sie weiß aber auch: Die Schüler müssen selber gehen, sehen reicht nicht; sie muß mitgehen, zeigen reicht nicht. Denn den Weg, den sie gehen können, gibt es nicht; er entsteht beim Laufen (Varela et al. 1991, Wagemann 1991, Siefkes 1998a).

Das gilt für die Wissenschaft wie für die Schule. In einer klassisch betriebenen Wissenschaft zerlegen wir das Land in Gebiete, um es dann durch Wege wieder zugänglich zu machen. Dafür müssen wir es schon kennen, es kommt wenig Neues heraus, wir bringen vor allem unsere Vorurteile hinein. In einer ökologischen Wissenschaft (Siefkes 1993a, 1998b) gehen wir von Beziehungen aus und finden dabei unsere Grenzen. Wir lassen Prozesse laufen und schaffen dabei neue Formen. Neues Wissen entsteht durch gemeinsames Suchen von Wegen, die schon unsere Spuren tragen. Wir reduzieren nicht Komplexität, sondern sind kreativ aus der Vielfalt heraus. In dem Sinn ist ökologische Wissenschaft besser als klassische: Sie erhöht die Vielfalt. Diese Wertung ist nicht absolut, aber sie trägt die kleinen Systeme, in denen wir sie betreiben. Praktisch werden wir beide Zugänge kombinieren; aber für einen Trampelpfad muß ich nicht kämpfen.

Die Einheit von Denken, Fühlen, Handeln

Noch fehlen in dem Modell die Gefühle. Unser Denken und Argumentieren ist immer emotional bestimmt. Auch in wissenschaftlichen Diskussionen, ob wir sie in der Runde mit Kollegen oder einsam am Schreibtisch führen, fühlen wir uns streitbar oder gelangweilt, suchen Ausgleich oder Versöhnung, unterwerfen uns oder triumphieren. Emotionen tragen unser Denken und Handeln. Ob wir eine wissenschaftliche Aussage annehmen oder ablehnen, hängt stark davon ab, welchen Wert wir der Entwicklung und den Beteiligten, dem verwendeten Zugang und den zugrundeliegenden Theorien beimessen; die rationale Begründung suchen wir später. Das gilt umso mehr – nicht weniger –, je rationaler der Bereich angelegt ist. Wer Mathematik mit Angst oder Ehrfurcht betrachtet, bleibt mathematisch erfolglos, was die Ehrfurcht oder Angst nur steigert. »How can you do New Math problems with an Old Math mind?« fragt Charlie Brown verzweifelt.

Während Fühlen und Denken in der Psychologie meist getrennt gesehen werden, spielt ihre Integration in der psychotherapeutischen Theorie und Praxis oft eine zentrale Rolle. Nach Basch (1988) wird unser Handeln durch Affekte bestimmt, das Kognitive ist nur (biologisch wie evolutionär wie funktional) die Kappe über den Affekten; es dient, uns vor einem Übermaß an Affekten zu schützen: Wir können Aktionen verzögern, nicht aus dem Affekt handeln, sondern erst andere mögliche Handlungen in der Phantasie durchspielen. Das Kognitive ist evolutionär spät, die Fähigkeit zur Imagination und damit zum individuellen Lernen beginnt erst bei den Säugetieren. Die Fähigkeit zur Phantasie – andere und insbesondere sich selbst in ausgedachten Situ-

ationen agieren zu lassen – zeichnet uns Menschen aus. Dabei erleben wir uns als Lebewesen mit freiem Willen.

Mit den Affekten reagieren wir unmittelbar, physiologisch, durch das limbische System. Bei Gefühlen kommt (mit 18–24 Monaten) das Selbstgefühl hinzu. Aber erst wenn wir die anderen Menschen als eigenständige Partner einbeziehen, werden es Emotionen (Liebe, Haß). Ähnlich entwickeln sich unsere kognitiven Fähigkeiten in Stufen. Dabei wird aber meist nur der einzelne Mensch betrachtet, der soziale Zusammenhang bleibt unberücksichtigt. Intelligenz wird als individuelle Leistung gesehen und gemessen. Noch merkwürdiger ist, daß auch die Emotionen im allgemeinen individualisiert und noch tiefer innen angesiedelt werden.

Sicher liegen die Emotionen, da sie aus den Affekten entstehen, im innersten Kern unserer Persönlichkeit; gleichzeitig spiegeln sie aber unsere sozialen Beziehungen wider, wie Basch es beschreibt. Im begrifflichen Denken regulieren und differenzieren wir unsere Emotionen, die ihrerseits Sinnesreize erst zu sinnlichen Wahrnehmungen zusammenfassen, Denken also erst möglich machen. Kognitive Entscheidungen und emotionale Bewertungen tragen unser Handeln und Kommunizieren und so unsere sozialen Beziehungen. Umgekehrt ist individuelles Denken nur als ein Aspekt kooperativer Informationsverarbeitung zu verstehen (Gehm 1996). Auf diese Weise bilden Fühlen, Denken und Handeln über Wahrnehmung und Kommunikation eine Einheit. Stimmt die Verbindung irgendwo nicht, werden wir psychisch und physisch krank: Ist sie zu starr, wirken wir zwanghaft; zu locker, hysterisch; gehemmt, narzißtisch; blockiert, autistisch (Hell 1992).

Im ökologischen Modell sind wissenschaftliche und technische Gegebenheiten Repräsentationen unseres wissenschaftlich-technischen Handelns; sie entwickeln sich nur darüber. Und in den Prozessen, die in Arbeitsgruppen und Entscheidungsgremien ablaufen, verschmelzen die unterschiedlichen Aspekte, die wir in den Repräsentationen so schön getrennt halten. Maschinen und das Wissen darüber sind zwei getrennte Welten; aber im technischen Entwerfen und Bedienen sind sie eins. Wissen und Wertungen, Begriffe und Werte sehen wir als Gegensätze; aber Denken, auch begriffliches, und Fühlen sind nicht zu trennen – das habe ich oben diskutiert. Was nützt es mir, zu wissen, daß der Löwe beißt, wenn ich nicht Angst davor habe. Was nützt es mir zu wissen, daß ich rennen kann und wohin ich rennen muß; erst Angst macht Beine. So verschmelzen im Rennen körperliche, geistige und emotionale Fähigkeiten und Gewohnheiten zu einer Einheit.

Das geschieht aber nur in »kleinen Systemen«. Nur im Schmelztiegel der kleinen Gruppe werden die drei Bereiche zu einer sinnvollen Einheit (Siefkes 1998a, b). Denn nur in Gruppen handeln wir gemeinsam, kommen also Denken, Fühlen und Handeln verschiedener Menschen direkt zusammen. Nur in Gruppenprozessen verschmelzen die unterschiedlichen, wenn nicht gar gegensätzlichen Repräsentationen und bringen neue Formen hervor.

Ciampi (1997) bezeichnet sogar die Logik als affektabhängig: Ein Mensch, der sich freut, denkt und handelt anders als ein Mensch in Angst. In der Angstlogik gelten daher andere Gesetze als in der Logik der Freude. Das erklärt, warum man – wie ich oben behauptet habe – Mathematik nur lernen (und lehren) kann, wenn man Freude daran hat, nicht in Angst oder Ehrfurcht. Diese Be-

hauptung erregt oft Widerspruch. Mathematiker formalisieren, d. h. sie betrachten nur Formen, suchen alle Abhängigkeiten von Prozessen zu eliminieren. Insbesondere scheinen alle sozialen und emotionalen Beziehungen zu verschwinden.

Im ökologischen Modell löst sich der Widerspruch. Lernen heißt, sich mit vorgegebenen Formen zu beschäftigen und sie – insbesondere sich – dabei zu verändern. Formen lassen sich zerlegen und getrennt behandeln. Prozesse sind Vorgänge, die sich nicht zerlegen lassen; da kommt das Getrennte wieder zusammen, wir handeln emotional, verhalten uns sozial. Das gilt auch für die Mathematik, für alle Bereiche, in denen wir mit Symbolen arbeiten. Auf dem Papier stehen scheinbar bedeutungsleere Zeichen; sobald wir sie lesen, schreiben oder verändern, zeigen und ändern sie ihre Bedeutung. Zeichen sind mit dem, was sie bedeuten, nicht magisch und nicht durch Vorschriften verbunden, sondern durch die Prozesse, deren Repräsentationen beide sind. In der Mathematik härten wir diese Beziehung durch formale Regeln; so wird sie haarfein und besonders haltbar. So fein und fest sind unsere Emotionen in das mathematische Denken eingeflochten.

Sozialgeschichte der Informatik

Diese Verflechtung läßt sich wissenschaftlich nur indirekt rekonstruieren. Affekte, Gefühle und Emotionen empfinden wir, es sind Prozesse; analysieren können wir nur ihre Repräsentationen. Nach innen sind das Werte; Werte spielen fürs Fühlen die Rolle, die Begriffe fürs begriffliche Denken spielen. Nach außen sind es Orientierungen, die Wertungen, die unserem Handeln seine Richtung geben. Im IFP *Sozialgeschichte der Informatik* haben wir in Informatiktexten nach Orientierungen gesucht: In den Herangehens-, Denk- und Sprechweisen der Akteure werden die sozialen und kulturellen Hintergründe erkennbar, die in der wissenschaftlich-technischen Entwicklung eine Rolle gespielt haben; vgl. die Beiträge von Bohnsack, Eulenhöfer, Rammert, Siefkes und Stach in dem Band Siefkes et al. (1998).

Diese Vorgehensweise widerspricht der üblichen Vorstellung von Informatikgeschichte. Danach entwickeln sich Wissenschaft und Technik aus den technischen und wissenschaftlichen Gegebenheiten. Technik besteht aus Maschinen und dem Wissen darüber, Wissenschaft aus Theorien, die begrifflich formuliert sind. Werte oder gar Wertungen kommen in der Sicht nicht vor. Für eine Sozialgeschichte werden soziale Einflüsse aus z.B. der Art der Finanzierung oder allgemeiner der Institutionalisierung einbezogen. Die Verflechtung von »Technik, Macht und Markt« und Kultur bleibt aber unerklärbar, weil die Einflüsse der Akteure dazu nicht ausreichen (König 1993). Insbesondere die vielbemühte »Macht« hat wenig Erklärungswert; die Unterschiede in der Rechnerentwicklung in den USA und in Deutschland während des zweiten Weltkriegs sind ein gutes Beispiel dafür. Die Mächtigen müssen vom Wert oder Unwert einer neuen Technik überzeugt werden, bevor sie Einfluß ausüben können. Wer überzeugt sie, und wie?

Wissenschaftliche und technische Veränderungen geschehen weder in den Köpfen einzelner noch im Zupacken aller, sondern in kleinen Arbeitsgruppen. Natürlich haben nur die Innovationen Aussicht auf Erfolg, die die Gruppe durch Personen, Artefakte oder Darstellungen zur rechten Zeit und so überzeugend nach außen repräsentiert, daß sie sich verbreiten und allgemeine

Anerkennung finden. Nur dadurch verändert sich die wissenschaftliche oder technische Situation, in der dann neue Gruppenprozesse ablaufen können. Die Prozesse werden durch die »gesellschaftlichen Bedingungen« und die »individuellen Charaktere« ermöglicht und beschränkt, aber sie geschehen lokal. Wahrzunehmen sind die Veränderungen allerdings am deutlichsten an den Repräsentanten auf der Mikro- und Makroebene; daher beherrschen diese bisher weitgehend die soziologische Diskussion (Giddens 1984, Siefkes 1998b).

Von Neumann hat seinen *First Draft* geschrieben, während er in der ENIAC-Gruppe arbeitete. Es ist sein Werk; aber er setzt sich darin, ohne es zu sagen, kritisch mit den Vorstellungen und Zielen der Gruppe auseinander. Ohne die Gruppe wäre es nicht entstanden, erst recht nicht publiziert. Es ist fast symbolisch, daß wir nicht wissen, ob es zur Veröffentlichung bestimmt oder nur ein internes Diskussionspapier war.

Auf ganz andere Weise repräsentieren die Arbeiten der bundesdeutschen Wegbereiter der Informatik Gruppenprozesse. Nach dem Krieg arbeiteten in der Bundesrepublik Deutschland an verschiedenen Orten Gruppen an der Entwicklung elektronischer Rechenmaschinen zur Durchführung umfangreicher Rechnungen, die bis dahin in Rechenbüros oder vergleichbaren Einrichtungen abgewickelt wurden. Die uns zugänglichen Texte spiegeln die Arbeit der jeweiligen Gruppe wider, aber gleichzeitig die Beziehungen zu den anderen Gruppen, die bei aller lokaler Verschiedenheit engen Kontakt hatten. So lebte die bundesdeutsche Entwicklung aus der Vielfalt dieser lokalen Prozesse und ihrer Repräsentanten und Repräsentationen.

Turing ist nur scheinbar eine Ausnahme. Dissertationen werden üblicherweise allein geschrieben, und Turing war mehr als üblich ein Einzelgänger. Aber eine Schreibmaschine hat er als Zwölfjähriger entworfen, weil er den Klagen seiner Mutter über die Beschwerden der Schule wegen seiner schlechten Handschrift entgegen wollte: Technikentwicklung als Gruppenprozeß. Und seine Dissertation wurde bekannt, weil sein Doktorvater sie der Gruppe um Church, Gödel, Rosser und Kleene in Princeton schickte, wo sie erhebliche Wirkung hatte. Alle betrachteten Formalismen erwiesen sich als äquivalent, und Gödel akzeptierte daraufhin, daß sie universell sind (siehe oben). So sehe ich Turings Arbeitsgruppe als eine Zelle, in der andere Menschen durch Bücher, Briefe und Maschinen repräsentiert sind. Auch eine solche Gruppe wirkt noch als Tiegel, in dem diese Repräsentationen mit seinen eigenen Emotionen und Theorien, seinen Fähigkeiten und Unfähigkeiten – mit einem Wort: mit seinem Charakter – in kreativen Prozessen verschmelzen.

Wenn Gruppen Schmelztiegel für die soziale Entwicklung sind, dann sind Geschichten es für die geistige Entwicklung. Sie sind die Sinneinheiten, die wir fürs Handeln beziehungsweise fürs Verstehen brauchen; einheitstiftend sind die Emotionen. In Geschichten verarbeiten wir unser Erleben zu Erfahrungen und bereiten uns so auf neues Erleben vor. In Geschichten sehen wir uns selbst und andere; wir bringen anderen unsere Welt-sicht nahe und bringen uns selbst in die Welt der anderen ein (Carr 1986, Siefkes 1992b). So wie ich die Entwicklung größerer sozialer Einheiten aus den Prozessen der beteiligten Gruppen hervorgehen und neue solche Prozesse in Gang setzen sehe, gewinne ich eine Sozialgeschichte der Informatik aus den Ge-

schichten, die ich über daran beteiligte Gruppen erzähle, und liefere damit Stoff für neue Geschichten.

Faszination beim Formalisieren

Unsere Kultur ist geprägt von einer fruchtbaren Wechselwirkung zwischen Mathematik und Mechanik. Der Bau von mechanischen Geräten, insbesondere Maschinen, setzt mathematische Sichtweisen und Methoden voraus und befördert sie weiter (Coy 1984, Siefkes 1998a). Mechanische Maschinen arbeiten kontinuierlich, mit ihnen führen wir physische Abläufe aus; ursprünglich machen wir damit körperliche Bewegungen nach. Deswegen ist die klassische Ingenieurmathematik stetig. Dagegen zählen wir diskret: 1, 2, 3, ... Daher sind die klassischen Berechnungsmodelle diskret; wir modellieren Funktionen auf den natürlichen Zahlen. Ebenso argumentieren wir in der Logik diskret: wahr, falsch; ja, nein. Das ist viel älter. Die beiden diskreten Welten der Logik und der Berechenbarkeit sind in einem langwierigen historischen Prozeß über Leibniz, Dedekind, Frege, Peirce und andere zusammengekommen. Turing war der erste, der eine diskrete Maschine dachte. Zuse, Aiken, von Neumann und andere waren die ersten, die welche bauten. Für beide, Ingenieure und Mathematiker, muß das Umdenken genauso schwierig gewesen sein wie die technischen bzw. formalen Probleme.

Mathematiker, hatte ich oben gesagt, formalisieren, d. h. bringen Bewegliches in feste Formen. Die Formen sind Zeichen für formalisierte Sachverhalte, der Umgang mit ihnen kann daher auf formale Regeln reduziert werden. Mathematik verstehe ich als den Versuch, menschliches Handeln durch das Befolgen formaler Regeln zu ersetzen. Beim Übergang vom Denken zur Logik, vom Erzählen zum Beweisen, vom Messen zum Rechnen geht das Kontinuierliche verloren: Anschauung, Gefühle, Körperliches, Soziales (Kutschmann 1986, Trettin 1991, Siefkes 1998a). Aktivitäten sind aber kontinuierlich, nicht diskret. Daher sind die diskreten Repräsentationen der Logik und Berechenbarkeit so »wackelig« und so zwanghaft zugleich: der Geist wird »dressiert, in spanische Stiefel eingeschnürt«. Das paßt nie richtig, wackelt, die Beziehung muß erzwungen werden. Andererseits ist sie gerade dadurch nicht so zwingend wie die der kontinuierlichen Repräsentationen, läßt mehr Freiheit, mehr Raum für Abweichungen, für Kreativität.

Ich kann also mit den Hybridobjekten bei Trettin (1991) anschließen. Beginnend bei Aristoteles und endend bei Frege analysiert sie das Faszinierende an der Logik: Das gezwungene und zwanghafte Denken in Schritten und Kategorien. Die entsprechende Geschichte fürs Rechnen hat Krämer (1988) beschrieben, aber das Faszinierende nicht untersucht. Sie nennt Formalismen »syntaktische Maschinen«, sieht also das Zwanghafte am Rechnen, aber nicht das Faszinierende an der Maschine, die uns die Entscheidungen abnimmt.

Formalismen und Programmiersprachen

Die schaffenden Mathematiker sind kreativ: Sie setzen alle menschlichen Fähigkeiten ein, um neue Formalismen zu produzieren. Die ausführenden Mathematiker dürfen es nicht sein: Sie sollen den vorgegebenen Regeln folgen. Bei jedem Schritt muß aus den vielen Regeln eine ausgewählt werden; die Wahl kann

gut oder schlecht sein, sie kann zum Ergebnis führen oder in die Irre. Es sind immer noch Menschen in ihrer Dummheit oder Genialität, mit ihren Vorlieben und Unfähigkeiten, die mit dem Formalismus arbeiten. Dementsprechend sind auch die mathematischen Berechnungsformalismen bis Turing *nichtdeterministisch*: Der Ablauf einer Berechnung liegt nicht fest, sondern wird immer wieder durch die Rechnenden bestimmt. Noch Kleene macht 1936 in seinem Formalismus das Rechenergebnis mit Gewalt eindeutig: Er zählt alle Rechenwege auf und definiert das zuerst erreichte als *das* Ergebnis; bingo.

Turings Maschine ist der erste deterministische Berechnungsformalismus: Die Ausgangsdaten legen die Rechnung vollkommen fest. Interessanterweise beginnt Turing mit allgemeinen »Maschinen«, bei denen die Menschen gelegentlich eingreifen müssen; er bezieht sich dabei ausdrücklich auf den Umgang mit logischen Kalkülen. Dann aber schließt er die Wahlmöglichkeiten aus und beschränkt sich auf »automatische« Maschinen, die deterministisch sind. Er begründet das nicht, beweist auch nicht explizit, daß er dabei nichts einbüßt. Die Determiniertheit von Maschinen scheint ihn zu faszinieren (Siefkes 1998a); wenn sie einen universellen Formalismus liefern, sind sie besser als ihre menschlichen Vorbilder.

Programme sind Texte, die eine Klasse von Berechnungen definieren, sagen die Mathematiker. Berechnungen sind Schrittfolgen, die durch das Programm und seine Interpretation (durch einen »Rechner« – Mensch oder Maschine) und Eingabe festgelegt sind. Die Berechnungen sind gedacht, sie können von Menschen oder bei Programmiersprachen vom Computer ausgeführt werden. Die Bedeutung eines Programms sind die Vorstellungen, die ich von diesem Ausführen habe. Daher sind in der Bedeutung eines Programms der Text (die Rechenvorschrift) und der ausführende Rechner untrennbar verknüpft. Ich kann Programme nur in dieser Verknüpfung sinnvoll denken – Programme sind Hybridobjekte. Deswegen ist bei Programmen die feste Abfolge der Schritte – das Zwanghafte – immer in der Bedeutung drin. Wir erzeugen etwas Determiniertes, das auf doppelte Weise absolut sicher ist – als Ergebnis und als Schrittfolge: Immer wenn wir das Programm auf demselben Rechner mit derselben Eingabe starten, erhalten wir dieselbe Berechnung, in der jeder Schritt eindeutig bestimmt ist.

Faszination beim Programmieren

Tatsächlich hat der Nichtdeterminismus mathematischer Formalismen, den Turing so kommentarlos aufgibt, in der Informatikgeschichte eine wichtige Rolle gespielt. Bei der Entwicklung und Implementierung von Programmiersprachen wie Fortran oder Prolog war es ein zentrales Problem, aus der ausufernden Zahl von Berechnungen, die eine mathematische Formel beschreibt, eine günstige auszuwählen. Aus eleganten formalen Beschreibungen effiziente und trotzdem verständliche Programme zu gewinnen, ist theoretisch wie praktisch ein Kernproblem der Informatik. Dabei geht es oft darum, Nichtdeterminismus zu eliminieren.

Computer sind Maschinen, die Berechnungen automatisch ausführen. Als Maschinen sind sie deterministisch, aber anders als Turings Maschine brauchen sie keine Menschen, die die Schritte machen. Übrig bleibt das Einlesen der Daten und das Ablesen

der Ergebnisse. Und das Programmieren. Das Computerprogramm ist das vollkommene Hybridobjekt (Stach 1998a, Eulenhöfer 1998b): Es ist Text; denn es besteht aus Zeichen und beschreibt Berechnungen. Es ist Maschine; denn es bringt die Maschine zum Laufen. Es ist Lebewesen; nur Lebewesen machen Schritte. Es ist Geist; denn die Schritte sind mathematische, erfordern also höchste Intelligenz. Als Lebewesen mit Geist ist es Mensch, schließe ich. Und als Mensch bin ich es selber, denn ich habe es geschaffen. Ich schreibe ein Programm, bin also sein Schöpfer. Das Programm läßt mich durch die Berechnung springen, ist also mein Schöpfer. Ich bin im Programm, und das Programm ist in mir. Alles Gefühlsmäßige und Körperliche, damit alles Soziale, nehme ich mit ins Programm.

So verstehe ich die Faszination an der Informatik: Programme sind Objekte, die Dualismen in sich tragen. Nach der ökologischen Sicht entwickelt sich Lebendiges im Wechselspiel zwischen Form und Prozeß. Prozesse sind unteilbar, aber ihre Repräsentationen lassen sich in widersprüchliche Formen zerlegen: Geist und Materie, Maschine und Lebewesen, Beschreibung und Bewegung, Subjekt und Objekt. Dualismen: Nichts kann beides sein, und doch haben wir beides in uns. Das macht Leben so unberechenbar: Wann immer wir eine Seite im Griff zu haben meinen, überrascht uns die andere. Höchst ärgerlich für alle, die ein bißchen Ordnung um sich haben möchten. Mathematische Formalismen sind nur Beschreibungen; realisieren muß ich sie selber. In informatischen Programmen kann ich mich mit der Maschine identifizieren und bleibe trotzdem Herr der Lage. Ich schreibe ja die Programme selbst, kann sie jederzeit verändern. Textend bin ich mitten in der Welt. Nicht umsonst heißen die neuen Programmiersprachen »objektorientiert«.

Die Entwicklung geht aber weiter. Programme werden nicht nur geschrieben, sondern auch ausgeführt. Ich schaffe nicht nur mich selbst, sondern auch die Benutzer und die indirekt Betroffenen. Deren Körper-, Gefühls- und soziale Welt wird ebenso mit ins Objekt gedacht. Je ähnlicher sich Programme und Objekte werden, desto glatter und unbemerkter geht das. Die Geistmaschinenwelt nimmt einen immer breiteren Raum, genannt Hyperspace, in unserer Kultur ein. Informatikgeschichte wird immer direkter Sozial- und Kulturgeschichte. Wir sollten mehr darüber wissen, um besser mit dieser Entwicklung umgehen zu können.

Literatur

- Basch, Michael Franz 1988: Understanding Psychotherapy. Basic Books.
- Bohnsack, Ralf 1998: Rekonstruktive Sozialforschung und der Grundbegriff des Orientierungsmusters. In Siefkes et al. (1998).
- Carr, David 1986: Time, Narrative, and History. Indiana University Press.
- Coy, Wolfgang 1984: Industrieroboter. Rotbuch.
- Ciampi, Luc 1997: Die emotionalen Grundlagen des Denkens. Entwurf einer fraktalen Affektlogik. Vandenhoeck.
- Davis, Martin 1982: Why Gödel Didn't Have Church's Thesis. Information and Control, Vol. 54, pp. 3–24.
- Eulenhöfer, Peter 1998a: Der Informatiker als »deus ex mathematica«. In Siefkes et al. (1998).
- Eulenhöfer, Peter 1998b: Disziplingeschichte und die Disziplinierung der Geschichte. FfF-Kommunikation 2/98, S. 29–33.
- Gehm, Theo 1996: Informationsverarbeitung in sozialen Systemen. Psychologie Verlags-Union.
- Giddens, Anthony 1984: The Constitution of Society. Outline of the Theory of Structuration. Berkeley. – Deutsch: Die Konstitution der Gesellschaft. Campus 1988.
- Heintz, Bettina 1993: Die Herrschaft der Regel. Zur Grundlagengeschichte des Computers. Campus.
- Hell, Daniel 1992: Welchen Sinn macht Depression? Ein integrativer Ansatz. Rowohlt.
- König, Wolfgang 1993: Technik, Macht und Markt. Eine Kritik der sozialwissenschaftlichen Technikgeneseforschung. Technikgeschichte, Bd. 60, Heft 3.
- Krämer, Sybille 1988: Symbolische Maschinen. Wissenschaftliche Buchgesellschaft Darmstadt.
- Kutschmann, Werner 1986: Der Naturwissenschaftler und sein Körper. Suhrkamp.
- Rammert, Werner 1998: Die kulturelle Orientierung der technischen Entwicklung. Eine technikgenetische Perspektive. In Siefkes et al. (1998).
- Siefkes, Dirk 1991: Sinn im Formalen? Wie wir mit Maschinen und Formalismen umgehen. In Coy, Wolfgang et al. 1992: Sichtweisen der Informatik. Vieweg, S. 97–114.
- Siefkes, Dirk 1992a: Formale Methoden und kleine Systeme. Lernen, leben und arbeiten in formalen Umgebungen. Vieweg.
- Siefkes, Dirk 1992b: Fish in Schools or Fish in Cans. Evolutionary Thinking and Formalization. International Computer Science Institute Berkeley, TR-92-009.
- Siefkes, Dirk 1993a: Evolutionäre Denkmodelle in der Informatikausbildung. InfoTech, Jahrgang 5, Heft 4, S. 26–33.
- Siefkes, Dirk 1993b: Gegen Klassen, Hierarchien, Reduktionen. Zur Aufgabe einer evolutionären Erkenntnistheorie. InfoTech, Jahrgang 5, Heft 3, S. 30–35.
- Siefkes, Dirk 1994: Ökologische Modelle geistiger und sozialer Entwicklung. Beginn eines Diskurses zur Sozialgeschichte der Informatik. Wissenschaftszentrum Berlin für Sozialforschung, Bericht FS II 95–20.
- Siefkes, Dirk 1995: Über die fruchtbare Vervielfältigung der Gedanken beim Reden. Forschung und Lehre, Heft 10, S. 551–555.
- Siefkes, Dirk 1997: Computer Science as Cultural Development. Toward a Broader Theory. In Christian Freksa et al. (eds.): Foundations of Computer Science – Potential, Theory, Cognition. Springer, S. 37–47.
- Siefkes, Dirk 1998a: Von der Rationalität der Wissenschaft und der Einsamkeit des Studierens. FfF-Kommunikation 1/98, S. 32–36.
- Siefkes, Dirk 1998b: Die Rolle von Gruppenprozessen in der Informatikgeschichte. In Siefkes et al. (1998).
- Siefkes, Dirk, Peter Eulenhöfer, Heike Stach, Klaus Städtler 1998: Sozialgeschichte der Informatik. Kulturelle Praktiken und Orientierungen. Deutscher Universitätsverlag.
- Stach, Heike 1998a: Beschreiben, konstruieren, programmieren. Zur Verschmelzung von Theorie und Gegenstand. In Siefkes et al. (1998).
- Stach, Heike 1998b: Als Rechner zu abstrakten Maschinen wurden. FfF-Kommunikation 2/98, S. 33–40.
- Trettin, Käte 1991: Die Logik und das Schweigen. VCH, Acta humaniora, Weinheim.
- Turing, Alan 1936–37: On computable numbers, with an application to the Entscheidungsproblem. Proc. London Math. Society (2), vol. 42, pp. 230–265.
- Varela, Francisco, Evan Thompson, Eleanor Rosch 1991: The Embodied Mind. Cognitive Science and Human Experience. MIT Press. – Deutsch: Der mittlere Weg der Erkenntnis. Scherz 1994.
- Wagemann, Carl-Hellmut 1991: Briefe über Hochschulunterricht. Deutscher Studienverlag.

Der Beitrag erschien in der FfF-Kommunikation 2/1998.

Allein? Überhaupt nicht!

Vorratsdatenspeicherung, Abschaffung des Bargeldes, Fluggastdatenspeicherung, e-Health, NSA-Überwachung, Verschwörungstheorien ... Manchmal kann der Blick in die Tagespolitik einem ganz schön die Hoffnung verderben. Da ist es schön, eine gute Nachricht im Gepäck zu haben: Das Interesse am Thema wächst spürbar. Immer mehr Menschen bemerken, dass sie von Datensammelereien massiv betroffen sind und den zunehmenden Überwachungswahn nicht mehr länger hinnehmen möchten.

An 23 Orten im deutschsprachigen Raum wurden am Dienstag, den 9. Februar 2016 – zum *Safer Internet Day* – Lesungen gegen Überwachung veranstaltet. Das ist nicht nur eine herrlich-nerdige Zahl, das sind auch acht Lesungen mehr als beim letzten *Safer Internet Day*.

Überall das gleiche Bild

Alle Berichte, die uns bisher erreicht haben, kommen in ähnlichem Tenor daher: Es war eine (bisweilen kleine, aber feine) anregende Runde, es gab gute Stimmung, interessante Texte und intensive Unterhaltungen dazu. Viele Leute, die kamen, sind ganz neu in der Szene, entdecken das Thema durch die Lesung neu für sich.

Die Idee, sich zu treffen und gegenseitig vorzulesen, fand großen Anklang. Gerade in Zeiten, wo längere Texte von Kurznachrichtendiensten verdrängt werden und Kommunikation zunehmend nonverbal stattfindet, tut es richtig gut, sich in einer netten Runde gegenseitig Texte vorzulesen.

Wann gibt es so etwas wieder?

Mehrfach wurde die Frage gestellt, wann denn die nächste Lesung gegen Überwachung stattfinden würde. Die gute Nachricht ist: Das bestimmen Sie selbst. Denn das Konzept ist nicht darauf angewiesen, dass gleichzeitig an mehreren Orten gelesen wird. Wann immer es gut passt, kann jede.r eine Lesung (in beliebiger Größe) organisieren, darüber berichten und unter dem Hashtag *#LesenGegenUeberwachung* twittern. Selbstverständlich wird es auch weiterhin bundesweite Lese-Tage geben. Das sollte aber niemanden davon abhalten, auch in der Zwischenzeit eine Lesung zu organisieren.

Safer Internet Day: Play your part for a better Internet – Veranstaltungen in Bremen am 9. Februar 2016

Der Internationale *Safer Internet Day*¹ findet jährlich am zweiten Dienstag im Februar statt und stand in diesem Jahr unter dem Motto *Play your part for a better Internet*.

Zahlenmäßig klare Siegerin der deutschen Veranstaltungen zum *Safer Internet Day* war Bremen. Hier haben auf zwei Veranstaltungen insgesamt ca. 50 Menschen gegen Überwachung gelesen.

Koordiniert von Agnes Graf und der *Buchhandlung Geist* fand eine Lesung mit anschließender sehr lebendiger Diskussion statt. In den Räumen der Buchhandlung hörten 25 Menschen zu, wie

Christian Bergmann, Schauspieler der *Shakespeare Company* (eine bekannte Bremer Theatergruppe), aus dem Buch *Angriff auf die Freiheit* von Juli Zeh und Ilija Trojanow und einen kurzen Passus auch aus dem *Circle* vorlas. Auf dem kleinen Podium saßen zwei Leute vom CCC aus Bremen und ein IT-Sicherheitsexperte. Anschließend gab es eine über einstündige vielseitige Diskussion. Ein Teilnehmer berichtete von seiner Verweigerung, die elektronische Gesundheitskarte einzusetzen, und was das jetzt für einen Aufwand bei jedem einzelnen Arztbesuch für ihn bedeutet. Fazit war: Ein gelungener Abend und die Erkenntnisse, dass wir mehr informieren könnten und alle sich mehr dagegen wehren sollten, ihre Daten preiszugeben.

Eine gemeinsame Veranstaltung mit dem FIF im Herbst 2016 wird von Agnes Graf angeregt.

Am selben Tag veranstaltete das Bremer Cyberpeace-Team² in Zusammenarbeit mit der FIF-Regionalgruppe Bremen einen Vortrags- und Diskussionsabend in der Universität Bremen. Auf dem Programm standen drei Kurzvorträge mit jeweils anschließender Diskussion. Die Videoaufnahmen der drei Vorträge finden sich unter³. Gut 25 Menschen lauschten den drei Vorträgen und beteiligten sich rege an der Diskussion.



Vertrauliche Kommunikation – Jabber/XMPP und OTR Fritjof Bornebusch

Fritjof Bornebusch ging es um die vertrauliche Kommunikation mittels Jabber/XMPP, die Möglichkeit der Verschlüsselung der Metadaten durch TLS (Transport Layer Security), der Nutzdaten durch OTR (off-the-record messaging) sowie die Möglichkeiten, entsprechende Server aufzusetzen, um auf einer vertraulichen und sicheren Ebene Daten auszutauschen. Als Vorteile dieses Verfahrens wurden sowohl die Verschlüsselung und Beglaubigung als auch die Abstreitbarkeit und somit „Folgenlosigkeit“

keit in juristischer Hinsicht“ benannt. Dabei nutzt das System die Ende-zu-Ende-Verschlüsselung, es ist dezentral, bietet Schutz vor Überwachung und ist inhaltlich erweiterbar.

Anonym im Internet durch Tor und Tor Onion Services – Aaron Lye

Aaron Lye umriss die Notwendigkeit und die Möglichkeiten, die Kommunikation mittels *Tor* vollständig zu anonymisieren und die Kommunikationswege dabei zu verschleiern. Der Referent nannte als Gründe für die definitive Anonymisierung u. a. den Schutz der Privatsphäre und der Metadaten, den Schutz sensibler Themen, somit das Umgehen einer Zensur. Unter denen, für die Anonymisierung wichtig ist, wurden außer den privaten Nutzern beispielhaft Journalisten und deren Leserschaft, Aktivisten und Whistleblower sowie Strafverfolgungsbehörden, Geheimdienste und das Militär genannt.

Aaron ging sowohl auf die Funktionsweise von *Tor* als auch auf *Tor Onion Services* ein. *Tor Onion Services* bietet ebenfalls Ende-zu-Ende-Verschlüsselung, Location Protected Services, und ist selbst authentifizierend. *Tor Hidden Services* werden u. a. von Wikileaks und Global Leaks genutzt.

Zu beiden Vorträgen wurden die technischen Verfahren zum Verschlüsseln der Meta- und Nutz-Daten diskutiert. Dabei ist sicherzustellen, dass der Austausch auch tatsächlich mit dem gewünschten Gesprächspartner stattfindet.



Cyberpeace-Forderungen eines sicheren Internets – Hans-Jörg Kreowski

Hans-Jörg Kreowski erinnerte daran, dass das Thema Überwachung (der Daten) bereits seit mehr als 20 Jahren besteht und wies auf den erfolgreichen Hackerangriff auf die Rechnerarchitektur des Deutschen Bundestages im vergangenen Jahr hin. Oft vergessen wird die Bedrohung der zivilen Infrastruktur, wenn es um Hackerangriffe geht. Die Bundeswehr betreibt seit dem 30. Juli 2015 eine massive Cyberwar-Aufrüstung.

Unter dem Stichwort *Cyberpeace* behandelte Hans-Jörg Forderungen für ein sicheres Internet aus politischer Sicht. Hier wurden auch die 14 Forderungen⁴ des FlfF an ein demokratisches und ziviles Internet verdeutlicht.

Alle drei Beiträge zeigten, dass es bei dem Schutz vor Überwachung und Ausspähen vor allem darum geht, Verfahren und Möglichkeiten gegen die Ausnutzung von Schwachstellen bei der Datenübermittlung zu finden und anzuwenden.

Anmerkungen

- 1 <https://www.saferinternetday.org/web/sid/about>
- 2 <http://cyberpeace.flf.de/Kampagne/Home>
- 3 http://mlecture.uni-bremen.de/ml/index.php?option=com_content&view=article&id=285
- 4 <https://cyberpeace.flf.de/Kampagne/WirFordern>



Lesen & Sehen

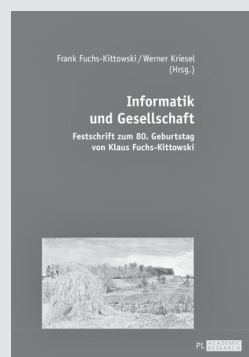
Neues für Bücherwürmer & Cineasten



Frank Fuchs-Kittowski, Werner Kriesel (Hg.) – Informatik und Gesellschaft. Festschrift zum 80. Geburtstag von Klaus Fuchs-Kittowski

Informatik und Gesellschaft erlebt eine Renaissance. Innovationen der Informatik treiben einen gravierenden gesellschaftlichen Wandel immer schneller voran, der für heftige Debatten sorgt. Aktuelle Themen behandelte die Tagung „Informatik und Gesellschaft“ zu Ehren von Klaus Fuchs-Kittowski als Pionier dieses Fachgebiets. Der Sammelband legt 44 Beiträge mit breitem Themenspektrum vor. Er behandelt den Einfluss von IKT auf die Arbeitswelt, Industriearbeit 4.0, Big Data, Datenschutz und Datenausspähung. Einzelne Beiträge sprechen Umweltinformatik, Informationssystemgestaltung, Softwareentwicklung, Künstliche Intelligenz, Cloud Computing sowie E-Learning (MOOC) an. Es werden auch künstliche Immunität, Avatare und die sozialen Aspekte behandelt. Ein weiteres Augenmerk liegt auf automatisierter Kriegsführung, hierzu werden insbesondere Ethik, Humanismus und Friedenserhaltung in einer global vernetzten Welt diskutiert.

(Umschlagtext des Verlags)

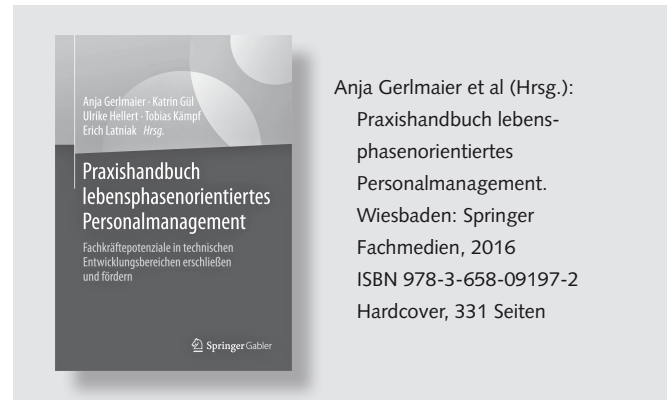


Frank Fuchs-Kittowski und Werner Kriesel (Hg.):
Informatik und Gesellschaft.
Festschrift zum 80. Geburtstag
von Klaus Fuchs-Kittowski.
Frankfurt am Main: Peter
Lang GmbH, 2016
ISBN 978-3-631-66719-4
Hardcover, 543 S.
Preis: € 89,95

Praxishandbuch lebensphasenorientiertes Personalmanagement

Das Institut Arbeit und Qualifikation und seine Partner haben das Projekt PINOWA abgeschlossen und die Ergebnisse in einem Praxishandbuch vorgelegt. Die Forschungsergebnisse sind für die praktische Anwendung gedacht und aufbereitet, ein Ziel, das auch die bisherigen Projekte dieser Sozialwissenschaftlerinnen und Sozialwissenschaftler auszeichnete. IfF hat sich am Projekt beteiligt, und wir haben in der IfF-Kommunikation 2/2015 vom letzten Transfer-Forum berichtet.

Anja Gerlmaiers Beitrag *Ausgeglichen oder ausgepowert?* auf Seite 18 dieser *IfF-Kommunikation* erläutert, warum es sinnvoll ist, angesichts von Fachkräftemangel und demographischem Wandel die unterschiedlich belastenden Episoden im Arbeitsleben zu berücksichtigen, und warum eine neue Perspektive für innovative Unternehmen mit ihren *Hochleistungskulturen* so wichtig ist. Das Praxishandbuch stellt in drei Teilen Konzepte und Begründungen, empirische Befunde, Empfehlungen und Instrumente für ein lebensphasenorientiertes Personalmanagement vor.



Innovation

„Trotz der vergleichsweise großen Unterschiede [...] besteht Einigkeit darin, dass eine gute Idee alleine noch keine Innovation ausmacht, sondern dass Innovation einen Prozess darstellt.“ (S. 173)

Unternehmen sind darauf angewiesen, gute Ideen erfolgreich und schnell in gute Produkte, auch Dienstleistungen, umzusetzen. Dafür sind die Bedingungen oft ungünstig: *„Innovationen sind in vielen durchrationalisierten und auf Kennzahlenerreichung ausgerichteten Organisationen strukturell nicht eingeplant.“* Gerlmaier untersucht deshalb in ihrem Beitrag *Was macht Entwicklungsteams wirklich innovativer – Erfolgsfaktoren eines nachhaltigen Innovations-Engineerings*, welche Bedingungen förderlich und welche hemmend wirken, und wie sie sich durch das Entwicklungsteam und seine Leitung beeinflussen lassen. Wichtige Wirkfaktoren sind dabei die kollektiven Wissensbestände der Teammitglieder, Gruppenprozesse und -beziehungen, Aufgabencharakteristika und Organisationsmerkmale. Diese Faktoren haben die Forscher:innen untersucht und nach förderlicher oder hemmender Wirkung eingestuft. Daraus ergeben sich konkrete Empfehlungen für die unterschiedlichen Phasen des Innovationsprozesses.

Da Menschen aber auch ein Leben neben dem Beruf haben, spielen nicht nur die betrieblichen Umstände eine Rolle. Fähigkeiten und Knowhow werden aufgrund der jeweiligen persönlichen Arbeits- und Lebenssituation nicht in dem Maße abgerufen, wie sie vorhanden sind, Innovationspotenziale in den Belegschaften oft nicht ausreichend erschlossen.

Lebensphasen

Es kommt Leben in die Unternehmen! So betiteln Katrin Gül, Andreas Boes und Tobias Kämpf einen Abschnitt ihrer Untersuchung von Möglichkeiten, mehr Nachhaltigkeit in die moderne Wissensarbeit zu bringen: Während das Durchschnittsalter der Belegschaften steigt, wird die Arbeitswelt weiblicher, gesellschaftliche Familienstrukturen verändern sich, all das begleitet von einem Wertewandel. Bei den Jungen trifft Technologie-Affinität auf den Wunsch nach einer Balance zwischen Arbeit und Freizeit.

„Bislang kamen Veränderungen in Unternehmen meist von oben, wir können nun erstmals von unten Druck machen. Denn meine Generation profitiert von ihrer geringen Zahl.“ (S. 61)

Gerlmaier und Latniak beschreiben Lebensphasen in den Erwerbsbiografien, die von Expert:innen (betrieblichen Akteuren, Personalverantwortlichen und Betriebsräten) als *anspruchsvoll* bewertet werden.

Diese Lebensphasen haben Gerlmaier und Latniak ausgemacht:

1. berufliche Orientierungsphase mit beispielsweise dem Übernehmen eigener Verantwortung für Aufgabenbereiche oder Projekte, häufigem Wechsel von Tätigkeit oder Unternehmen, einer sekundären Qualifizierung

Dagmar Boedicker

Dagmar Boedicker ist Journalistin und technische Redakteurin und hat Politikwissenschaft studiert. Sie ist seit langem Mitglied des IfF, war Vorstandsmitglied und stellvertretende Vorsitzende, und ist Redakteurin der *IfF-Kommunikation*.

2. mittlerer Erwerbsabschnitt mit beispielsweise dem Übernehmen von Führungsaufgaben, Familiengründung mit Karriere-Orientierung, in Voll- oder Teilzeit, mit speziellem, rarem Knowhow, das mehrfach gefordert ist
3. späterer Erwerbsabschnitt mit beispielsweise einer Spezialisierung ohne neuen Wissenserwerb über lange Zeit, familiären Krisen (*Sandwich-Generation*), gesundheitlichen Beeinträchtigungen, Abstieg oder Ausstieg.

Wenn ein Unternehmen diese persönlichen Arbeits- und Lebenssituationen kennt und richtig damit umgeht, wenn es seine Mitarbeiterinnen und Mitarbeiter angemessen unterstützt und fördert, lassen sich ihre Innovationspotenziale und ihr Knowhow sehr wohl abrufen. Das Werkzeug dafür stellen die Autor:innen in Teil II, Kapitel 10, vor: *Lebensphasenorientierte Potenzialanalyse (LPA)*.

Noch ein Instrument

Das Buch bietet auch andere Instrumente, unterlegt mit zahlreichen empirischen Befunden. Ich greife nur dieses eine

noch heraus: die *PINOWA-Toolbox*. In Kapitel 11 beschreiben Ute Peters, Christina Goesmann und Ulrike Hellert, wie Unternehmen, insbesondere kleine und mittlere (KMU), ihre Rekrutierung und Personalauswahl systematisch strukturieren und den Prozess erfolgreich gestalten können. Mit dieser Unterstützung rücken Anforderungskriterien in den Mittelpunkt und Verzerrungseffekte lassen sich vermeiden.

Kapitel 12 stellt den KMU-Check vor. Er soll dem Missstand abhelfen, dass viele Unternehmen zwar sehr wohl Maßnahmen nutzen, die sich an den Lebensphasen orientieren, und Mitarbeiterinnen und Mitarbeiter unterstützen, dass aber meist kein Konzept dahinter steht. Damit hängt es von einzelnen Führungskräften ab, ob und wie sich berufliche und andere Anforderungen vereinbaren lassen, welche Regelungen es zur Arbeitszeit, Weiterbildung, Gesundheit gibt. Mit dem KMU-Check können die Unternehmen ihre Personalstrategie mit Blick auf die Lebensphasen ihrer Beschäftigten analysieren, verbessern und weiter entwickeln. Er gehört zur PINOWA-Rekrutierungstoolbox, die als einfach zu nutzende Hilfe für die Praxis konzipiert ist.



Stefan Hügel

Log 1/2016

Ereignisse, Störungen und Probleme der digitalen Gesellschaft

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

August 2015

25. August 2015: In San Jose im Silicon Valley soll die Müllabfuhr fortlaufend die Kennzeichen von Fahrzeugen erfassen und, verbunden mit Zeit- und Ortsangaben, an die Polizei weiterleiten. Bereits zuvor wurden eine Drohne angeschafft und in einem Pilotprojekt Polizist:innen mit Körperkameras ausgerüstet (Quelle: Heise).

28. August 2015: Aus einer Übereinkunft zwischen der US-amerikanischen National Security Agency (NSA) und deutschen Geheimdiensten geht hervor, dass die Zusammenarbeit mit dem Bundesnachrichtendienst (BND) weit über das hinausging, was zuvor bekannt war. Offenbar erhielt der BND die Spähsoftware XKeyscore, installierte sie beim Bundesamt für Verfassungsschutz (BfV) und sorgte für den technischen Support. Erkenntnisse des BfV sollten an die NSA weitergeleitet, US-Bürger:innen dabei nicht ausspioniert werden (Quelle: Zeit, Heise).

28. August 2015: Redaktionsräume und Wohnungen von Journalisten dürfen nicht durchsucht werden, um damit vorrangig den Verdacht von Straftaten durch Informanten aufzuklären. Das Bundesverfassungsgericht hat entschieden, dass dies nicht verfassungsgemäß ist. Es sind „zureichende tatsächliche Anhaltspunkte für eine Straftat der konkret betroffenen Presse-

angehörigen“ erforderlich. Damit stärkt das Bundesverfassungsgericht erneut Pressefreiheit und Informantenschutz (Quelle: Bundesverfassungsgericht, Heise).

29. August 2015: Die Entscheidung eines US-Gerichts von 2013, die Vorratsdatenspeicherung der NSA in den USA würde „höchstwahrscheinlich“ gegen die US-Verfassung verstoßen, wird vom Berufungsgericht aufgehoben. Die Entscheidung gilt als Rückschlag für den Kampf gegen den Überwachungsstaat, obwohl das ursprüngliche Urteil ohnehin nicht durchgesetzt und von der NSA ignoriert worden war (Quelle: Heise).

30. August 2015: Ein 17-jähriger US-Amerikaner wird zu 11 Jahren Haft verurteilt, weil er den sogenannten *Islamischen Staat* (IS) unterstützt haben soll. Er habe online Propaganda gemacht und Tipps gegeben, wie IS-Mitglieder Bitcoin und Verschlüsselung nutzen könnten (Quelle: Heise).

September 2015

2. September 2015: Wegen verschlüsselter Daten auf dem Rechner eines Kontaktmanns wurden dieser und zwei britische Journalisten des Magazins *Vice* in der Türkei verhaftet. Der Rechner sei mit einer Software verschlüsselt, die auch von der terroristischen

tischen Vereinigung *Islamischer Staat* genutzt werde. Amnesty International bezeichnete das Vorgehen der türkischen Behörden als „bizar“ (Quelle: Heise).

5. September 2015: Nach Informationen des Spiegel hat der US-Geheimdienst CIA in einer Operation unter dem Decknamen *Glotaic* direkten Zugriff auf deutsche Telekommunikation. Der Geheimdienst hatte am deutschen Standort des Telekommunikationsanbieters MCI in Hilden dessen Telefon- und Faxverkehr mitgeschnitten. Angeblich kursierten beim BND interne Warnungen vor einem „politischen Skandal“, falls die Operation auffliegen sollte (Quelle: Spiegel, Heise).

7. September 2015: Nach Ansicht von Presseverbänden und TV-Sendern beeinträchtigt die neue Vorratsdatenspeicherung die Pressefreiheit. Weder verfassungsrechtlich noch europarechtlich sei sie zu rechtfertigen, so heißt es in einem Papier von DJV-Justiziar Bernd Pöppelmann. „Die anlasslose Speicherung, Erhebung und sonstige Verwendung solcher Daten auf Vorrat ist mit dem national und auf europäischer Ebene garantierten Recht auf informationelle Selbstbestimmung und den hieraus erwachsenden datenschutzrechtlichen Grundsätzen der Erforderlichkeit und der Datensparsamkeit nicht zu vereinbaren und deswegen unzulässig“, schreibt er. Das Vorhaben stelle „auch einen massiven Eingriff in die Bürgerrechte“ dar. Unterstützt wird die Stellungnahme von DJV, dju in ver.di, BDZV, VDZ, VPRT, dem Deutschen Presserat sowie den Sendern ARD und ZDF (Quelle: Heise).

9. September 2015: Demonstranten in der Türkei haben das Medienhaus der Zeitung *Hürriyet* angegriffen. Die Polizei sei erst nach einer halben Stunde erschienen, um die Menge zu zerstreuen. Die Angreifer, Anhänger der islamisch-konservativen AKP, hätten, Berichten zufolge, eine stärkere Verurteilung der kurdischen Arbeiterpartei PKK verlangt. Bereits am Sonntag zuvor war es zu ähnlichen Aktionen gekommen (Quelle: Heise).

10. September 2015: Der Bundestag ist wieder online, nachdem er Opfer eines massiven Cyberangriffs geworden war. Als Konsequenz aus dem Angriff sollen IT-Sicherheitsmaßnahmen deutlich ausgebaut werden. Mitarbeiter sollen speziell geschult, das IT-Personal aufgestockt und Angriffserkennungssysteme verbessert werden. Auch bauliche Veränderungen sind offenbar geplant. Der Zugriff auf zehntausende Internetseiten wurde „aus Sicherheitsgründen“ geblockt (Quelle: NDR, WDR, Süddeutsche Zeitung, Heise).

11. September 2015: Trotz der offenbar massiven Ausspähung der Bevölkerung sieht das Bundeskanzleramt keinen umfassenden Handlungsbedarf beim Bundesnachrichtendienst (BND). Es werde lediglich über „klarstellende Regeln“ gesprochen. Nach Ansicht im Bundeskanzleramt sei beispielsweise für die Ausspähung des Frankfurter Internetknotens DE-CIX, die als Operation *Eikonal* bekannt wurde, keine konkrete Eingriffsbefugnis erforderlich; die Generalklausel im BND-Gesetz habe dafür ausgereicht (Quelle: Heise).

11. September 2015: Die US-Streitkräfte wollen die heutige Anzahl von ca. 3.000 Militärkräften für Cyber-Operationen auf 8.000 Cybersoldaten erhöhen. Im Fünfjahresplan 2014–2018 stehen dafür 1,878 Milliarden US\$ zur Verfügung. Die Teams

sollen auf die neun vereinigten Kampfkommandos aufgeteilt werden, von denen zwei ihren Hauptsitz in Stuttgart haben (Quelle: Heise).

14. September 2015: Die Kapazitäten der Bundeswehr zur Cyber-Kriegführung sollen nach dem Willen von Bundesverteidigungsministerin Ursula von der Leyen gebündelt und der entsprechende Bereich den anderen Teilstreitkräften gleichgestellt werden. Damit will man dessen wachsender Bedeutung gerecht werden. Der Austausch mit anderen Behörden solle verbessert werden (Quelle: Süddeutsche Zeitung, Heise).

14. September 2015: Bundeskanzlerin Angela Merkel hat an den Gesetzgeber appelliert, beim Datenschutz „Vernunft“ walten zu lassen. Daten seien der Rohstoff der Zukunft; die geplante EU-Datenschutz-Grundverordnung dürfe nicht nur unter dem Gesichtspunkt des Datenschutzes betrachtet werden. Nicht nur Risiken sollten im Mittelpunkt der Digitalisierungsdebatte stehen (Quelle: Heise).

16. September 2015: Ein 14-jähriger Schüler wurde in den USA verhaftet, nachdem er eine selbstgebastelte Uhr in der Schule seinen Lehrern gezeigt hatte. Da die Uhr für eine Bombe gehalten wurde, wurde er verhaftet, verhört und erkennungsdienstlich behandelt. Den Polizeibeamten sei, einem Sprecher zufolge, klar gewesen, dass es sich nicht um eine Bombe gehandelt habe. Der muslimische Schüler habe aber keine plausible Erklärung geliefert, warum er die Uhr gebaut habe. Der 14-jährige war zuvor begeistertes Mitglied im schulischen Roboter-Club gewesen (Quelle: Dallas Morning News, Heise).

21. September 2015: Der *Strategischen Initiative Technik* des Bundesnachrichtendienstes (BND) zufolge will sich der Geheimdienst technisch auf die Erfassung und Analyse von Web 2.0, Big Data und dem Internet der Dinge (*Internet of Things*, IoT) und Biometrie vorbereiten. Damit verbunden ist ein Wechsel der Philosophie von der Erfassung der Kommunikationsinhalte hin zu Metadaten, also der Erfassung und Analyse von Verbindungs- und Standortinformationen (Quelle: Heise).

22. September 2015: Bürgerrechtler sind über den Ausbau der Speicherung von Biometriedaten alarmiert. Im Projekt *Next Generation Identification* werden Biometriedatenbanken massiv ausgebaut, indem beispielsweise auch Fingerabdrücke von Bewerbern für Arbeitsstellen, die die Arbeitgeber für eine Überprüfung zum Abgleich einsenden müssen, gespeichert werden. Das kalifornische Justizministerium gibt beispielsweise an, jährlich 1,2 Millionen Fingerabdrücke für solche Überprüfungen an das FBI zu übermitteln. Als nächster Schritt ist die Einführung einer Gesichtserkennung geplant (Quelle: Heise).

22. September 2015: Nach Ansicht von Bundeswirtschaftsminister Sigmar Gabriel sollen intelligente Stromzähler flächendeckend eingeführt werden, trotz Warnungen vor einer „Zwangsdigitalisierung durch die Kellertür“ durch den Bundesverband der Verbraucherzentralen (vzbv). Das sieht der Referentenentwurf für ein Gesetz zur „Digitalisierung der Energiewende“ vor. Damit verbunden sei die massenhafte Preisgabe sensibler Daten. Eine Kosten-Nutzen-Analyse hat dem Referentenentwurf zufolge ein Einsparpotenzial von drei Euro pro Jahr und Haushalt ergeben (Quelle: Heise).

24. September 2015: Bei einem massiven Angriff auf die US-Bundespersonalbehörde OPM wurden neben persönlichen Daten von 22 Millionen Bediensteten auch die Fingerabdrücke von 5,6 Millionen Beschäftigten kompromittiert (Quelle: Heise).

25. September 2015: Der Bundesrat hat das Gesetz für neue Geheimdienstbefugnisse, mit dem Kompetenzen und Ausstattung der Geheimdienste massiv gestärkt werden, nach kurzer Diskussion durchgewinkt. Dabei ist eine Erweiterung des *Nachrichtendienstlichen Informationssystems* (Nadis) geplant, durch das nun Volltextdateien beliebig gespeichert, ausgetauscht und ausgewertet werden sollen. Der Rechtsausschuss des Bundesrats hatte noch dafür plädiert, wegen der enthaltenen „automatisierten Ähnlichkeitsabfrage“ den Vermittlungsausschuss anzurufen (Quelle: Heise).

28. September 2015: Die Kampagne *Intelexit* wendet sich an Mitarbeiter von Geheimdiensten – Verfassungsschutz, Bundesnachrichtendienst, Militärischer Abschirmdienst und die befreundeten Dienste von NSA und GCHQ – und will ihnen eine Ausstiegshilfe unter dem Motto „Backdoor to democracy“ bieten (Quelle: Heise).

29. September 2015: Der Baufortschritt eines neuen Basketballstadions in Sacramento wird ständig durch Drohnen überwacht. Dabei überfliegen die Drohnen die Baustelle einmal am Tag; die Filmaufnahmen werden dann mit den digitalen Bauplänen des Stadions verglichen (Quelle: Heise).

29. September 2015: Untersuchungen von Sicherheitsforschern zufolge sind tausende medizinische Geräte aus dem Internet angreifbar. Viele dieser Systeme werden noch mit Windows XP betrieben, sind unzureichend abgesichert und können unter die Kontrolle der Angreifer geraten. Diese können dann Geräte steuern oder Patienten- und Personal-Daten abgreifen (Quelle: Heise).

Oktober 2015

1. Oktober 2015: Nils Muižnieks, der Menschenrechtskommissar des Europarats, kritisiert die mangelhafte Geheimdienstaufsicht in der Bundesrepublik Deutschland. Angesichts von nur 13 Mitgliedern und einem kleinen Sekretariat, denen allein rund 6.000 Mitarbeiter:innen des Bundesnachrichtendienstes (BND) gegenüberstehen, sei er „besorgt über das Fehlen von Ressourcen und Fachwissen seitens der Aufsichtsgremien“. Im G10-Sekretariat gebe es keinen IT-Experten, „der in der Lage wäre, mit den Entwicklungen der digitalen Welt Schritt zu halten“. Nach Ansicht des Menschenrechtskommissars ist die Geheimdienstkontrolle in keinem europäischen Land ausreichend (Quelle: Menschenrechtskommissar des Europarats, Heise).

2. Oktober 2015: Die Crowdfunding-Plattform *Patreon* wurde von Unbekannten angegriffen und deren Nutzerdaten im Web veröffentlicht. Darunter sind Daten zu Spendenkampagnen, Mail-Adressen, persönliche Nachrichten, verschlüsselte Passwörter und der Quellcode der Webseite; der Umfang beträgt ca. 15 GB. Die Daten konnten gestohlen werden, nachdem Entwickler versehentlich eine Kopie der Produktivdatenbank auf einem Entwicklungsserver zugänglich gemacht hatten (Quelle: Heise).

4. Oktober 2015: Nach einem Bericht des MDR unter Berufung auf das Landeskriminalamt ermittelt die thüringische Polizei immer häufiger wegen Hass-Kommentaren im Internet. Die Anzahl der Straftaten habe bereits im ersten Halbjahr 2015 um 53 % über der Zahl des gesamten Jahres 2014 gelegen. Die Aufklärungsquote sei sehr hoch. Straftaten seien Verleumdung, Beleidigung, Nötigung und Bedrohung, üble Nachrede, öffentliche Aufforderung zu einer Straftat, Volksverhetzung oder auch das Zeigen verfassungsfeindlicher Symbole (Quelle: MDR, Heise).

6. Oktober 2015: Das *Safe-Harbor*-Abkommen zwischen den USA und der EU, das den Datenschutz bei der Übermittlung personenbezogener Daten in die USA regelt, wird vom Europäischen Gerichtshof (EuGH) für ungültig erklärt. Damit folgt das Gericht dem Antrag des Generalanwalts Yves Bot. Die Europäische Kommission könne die Befugnisse nationaler Datenschutzbehörden weder beseitigen noch beschränken, so das Gericht. Der erlaubte Zugriff von Behörden auf Daten in den USA verletze dagegen „den Wesensgehalt des Grundrechts auf Achtung des Privatlebens“. US-Unternehmen seien verpflichtet, in Europa geltende Schutzregeln außeracht zu lassen, wenn US-Behörden aus Gründen der nationalen Sicherheit beziehungsweise des öffentlichen Interesses Zugriff auf persönliche Daten verlangten; es gebe auch keinen Rechtsbehelf für EU-Bürger:innen in solchen Fällen. Auslöser für das Verfahren war eine Beschwerde des österreichischen Juristen Max Schrems (Quelle: Heise).

6. Oktober 2015: Das Aktivitätstracker-Armband *Microsoft Band* wurde mit noch mehr Sensoren ausgestattet und kann so mehr und genauere Daten sammeln als die Vorgängerversion. Neben Beschleunigung erfasst es wie schon bisher Temperatur, Herzfrequenz, GPS-Koordinaten, UV-Strahlung, Hautwiderstand, Feuchtigkeit. Neu hinzugekommen ist nun ein barometrischer Höhenmesser, mit dem sich genauer als mit GPS feststellen lässt, welche Steigungen der Träger bewältigt. Das Gerät übermittelt über das gekoppelte Smartphone die ermittelten Körperdaten direkt in die Cloud-Plattform *Microsoft Health* (Quelle: Heise).

7. Oktober 2015: Die EU-Kommission und der luxemburgische Ratsvorsitz finden, dass trotz des EuGH-Urteils, das die bisherige rechtliche Basis *Safe-Harbor*-Abkommen für ungültig erklärt, Unternehmen weiterhin personenbezogene Informationen in die USA übermitteln dürften (Quelle: Heise).

8. Oktober 2015: Die Linke warnt vor anlassloser Rasterfahndung nach Finanzdaten in Echtzeit. Das mit EU-Fördermitteln entwickelte Verfahren *Ma³tch* – a³ steht für autonome anonyme Analyse – sei ein Beispiel für die Fahndung mit Vorratsdaten, so Andrej Hunko von der Linksfraktion im Deutschen Bundestag. Die Bundesregierung erklärt in ihrer Antwort auf eine kleine Anfrage, die Technik sei konform mit der 4. Anti-Geldwäsche-Richtlinie der EU und damit rechtmäßig (Quelle: Heise).

8. Oktober 2015: Nach Ansicht von Edward Snowden haben die USA kein Interesse an Aufarbeitung des NSA-Skandals. Er vermisst auch eine breite gesellschaftliche Auseinandersetzung: „Vielen in den USA ist es anscheinend egal, ob es gut oder schlecht war, was die NSA da gemacht hat“, erklärte er bei seiner Keynote zur Security-Fachmesse it-sa in Nürnberg (Quelle: Heise).

9. Oktober 2015: Der Jurist Ulf Buermeyer warnt vor unvorhersehbaren Auswirkungen des Gesetzes zur Vorratsdatenspeicherung. Durch den neuen Straftatbestand der „Datenhehlerei“ sei vor allem der investigative Journalismus gefährdet. Datenhehlerei begehe jeder, der Daten, die ein anderer rechtswidrig erlangt hat, sich verschafft oder einer weiteren Person überlässt, verbreitet oder sonst zugänglich macht. Dies gelte auch für Journalisten, die Informationen von Whistleblowern veröffentlichen (Quelle: Heise).

9. Oktober 2015: Nach der gemeinsamen Position des EU-Rats zur Datenschutzrichtlinie für die Strafverfolgung soll der Fluss personenbezogener Informationen zwischen Behörden möglichst offengehalten werden. Daten sollen auch für andere Zwecke als zunächst vorgesehen genutzt werden dürfen, solange die Nutzung „nötig“ sei und „verhältnismäßig“ erfolge. Bürger sollen das Recht erhalten, bei Strafverfolgungsbehörden eigene Daten einzusehen und gegebenenfalls zu verbessern. Es reiche dazu aber aus, Antragsteller:innen eine „Zusammenfassung“ aus den Akten in verständlicher Form zur Verfügung zu stellen. Das Auskunfts- und Korrekturrecht dürfe gesetzlich beschnitten oder ganz gestrichen werden, wenn diesem gängige Interessen der Strafverfolger oder Belange etwa zum Schutz der öffentlichen Sicherheit entgegenstünden (Quelle: Heise).

15. Oktober 2015: Der US-amerikanische frühere Drohnenpilot Brandon Bryant sagt vor dem NSA-Untersuchungsausschuss über die Rolle der Militärbasis Ramstein in Rheinland-Pfalz aus. Ramstein sei die zentrale Relaisstation gewesen, „wir hätten ohne Ramstein nicht gewusst, wo wir fliegen“. Dabei sei es auch immer wieder zu „Kollateralschäden“ unter Zivilisten gekommen. Jungen über 12 Jahren hätten schon als legitimierte Ziele gelten können, was wohl UN-Konventionen widerspreche. Gleichzeitig veröffentlicht die US-amerikanische Plattform *The Intercept* eine umfangreiche Artikelserie *The Drone Papers* mit Dokumenten, die den Drohnenkrieg der USA unter Präsident Barack Obama von 2011 bis 2013 dokumentieren. Einleitend heißt es dazu: „Drohnen sind Werkzeuge, keine Methode. Die Methode nennt man Ermordung“ (Quelle: The Intercept, Heise).

16. Oktober 2015: Die Inhaltsdaten von SMS können nach Erkenntnissen der Süddeutschen Zeitung aus technischen Gründen nicht von den Verbindungsdaten getrennt werden, so dass sie ebenfalls von der Vorratsdatenspeicherung erfasst werden. Die Inhalte würden zwar technisch maskiert, sie liegen aber dennoch für die Dauer der Vorratsdatenspeicherung bei den Providern vor (Quelle: Süddeutsche Zeitung, Heise).

16. Oktober 2015: Der Deutsche Bundestag führt nach ablehnenden Urteilen des Bundesverfassungsgerichts und des Europäischen Gerichtshofs die Vorratsdatenspeicherung zur anlasslosen Speicherung der Metadaten von Kommunikationsvorgängen wieder ein. In namentlicher Abstimmung votierten 404 Abgeordnete für den Entwurf des Bundeskabinetts, der trotz erheblicher Bedenken von Sachverständigen nicht mehr verändert worden war (Quelle: Heise).

19. Oktober 2015: Der E-Mail-Anbieter Posteo wirft dem Bundeskriminalamt einen Rechtsverstoß bei der Abfrage von Bestandsdaten vor. Die Daten seien ohne die nach dem Bundes-

datenschutzgesetz notwendigen Absicherungen erfolgt. Dies wurde durch Bundesinnenminister Thomas de Maizière bestätigt; es sei aber nur in absoluten Ausnahmefällen erfolgt (Quelle: Heise).

21. Oktober 2015: „Straßen? Wo wir hingehen, brauchen wir keine Straßen!“ Marty MacFly und Doc Brown landen auf ihrer Reise aus der Vergangenheit 1985. Entgegen der damaligen Erwartung haben sich fliegende Automobile und doppelte Kravatten heute noch nicht allgemein durchgesetzt (Quelle: Heise).

21. Oktober 2015: Eltern sind in der Lage, mit Hilfe von Tracking-Apps ihre Kinder jederzeit zu orten und zu kontrollieren. Neben der ständigen Ortung können soziale Netzwerke überwacht und unerwünschte soziale Kontakte gesperrt werden. „Ich halte das für einen vollkommen falschen Weg“, so der Vorstandsvorsitzende der Deutschen Kinderhilfe, Rainer Becker. „Alle in Deutschland haben mit Betroffenheit erlebt, wie uns die NSA überwacht. Niemand will das. Ich kann nicht nachvollziehen, warum wir das bei unseren eigenen Kindern machen, nur weil sie Kinder sind“ (Quelle: Heise).

25. Oktober 2015: Nach zwei Bombenanschlägen mit insgesamt 35 Todesopfern schaltet Pakistan Internet- und Mobilfunknetzdienste in allen größeren Städten ab (Quelle: Heise).

28. Oktober 2015: Bei der Untersuchung der Überwachungsbegriffe – sogenannter Selektoren – hat eine Task Force des Parlamentarischen Kontrollgremiums schnell eine erhebliche Zahl von Spionagezielen in den USA und in Europa gefunden. Zuvor war bereits bekannt geworden, dass der BND in seine eigenen Überwachungsprogramme Suchbegriffe der NSA eingespeist hatte, die gegen deutsche Interessen verstießen – also beispielsweise europäische Unternehmen betrafen. Zusätzlich habe der BND selbst entsprechende Selektoren angelegt. Der Ex-Bundesrichter Kurt Graulich, der als „Sonderermittler“ eingesetzt worden war, kam zu dem Ergebnis, dass bis zu 40.000 Selektoren – von ca. 1.000.000 – des BND gegen westeuropäische und deutsche Interessen gerichtet waren. Der Bundesnachrichtendienst hat nach Ansicht des SPD-Obmanns im Untersuchungsausschuss, Christian Flisek, mit seiner Praxis deutsches Recht verletzt (Quelle: Heise).

30. Oktober 2015: Nach Vorstellung der britischen Regierung sollen Provider dazu verpflichtet werden, neben den Verbindungs- und Standortdaten auch Inhalte ein Jahr anlasslos zu speichern. Die Verpflichtung erstreckt sich demnach auch auf Informationen über besuchte Webseiten sowie die E-Mail- oder die Chat-Kommunikation. Auch Verschlüsselung soll umgangen werden (Quelle: Telegraph, Heise).

November 2015

2. November 2015: Bundeskanzlerin Angela Merkel fordert Abwägungen zwischen wirtschaftlichen Belangen und den Grundrechten: Daten seien die „Rohstoffe des 21. Jahrhunderts“, erklärt sie anlässlich des Kongresses *Publishers' Summit*. Wir müssten „aufpassen, dass der Datenschutz nicht die Oberhand über die wirtschaftliche Verarbeitung gewinnt“ (Quelle: Heise).

5. November 2015: Die Verbraucherzentrale Nordrhein-Westfalen klagt wegen ungefragter Datenübermittlung gegen den südkoreanischen Elektronikhersteller Samsung. Über den HbbTV (Hybrid broadband broadcast TV)-Standard übermittelten die von Samsung hergestellten Fernsehgeräte die IP-Adresse des Anschlussinhabers an Server des Konzerns, sobald sie an das Internet angeschlossen würden. Deswegen sei eine Musterklage in Frankfurt am Main eingereicht worden. (Quelle: Heise).

9. November 2015: Die interaktive Barbie-Puppe *Hello Barbie* wird zum Weihnachtsgeschäft in den USA erhältlich sein. Die Barbie kann sprechen und ist mit Mikrofon und WLAN-Anschluss versehen. Stimmen werden aufgezeichnet und in der Cloud verarbeitet, um entsprechende Antworten zu generieren. Dabei werden die Daten gespeichert, um die Spracherkennung und -generierung der Puppe damit zu trainieren; der Hersteller beteuert, dass die Daten nicht zu Werbezwecken genutzt würden. Eltern und Datenschützer:innen warnen vor einem Missbrauch der kindlichen Privatsphäre. *Hello Barbie* wurde in Deutschland 2015 mit einem BigBrotherAward ausgezeichnet (Quelle: Heise).

9. November 2015: Trotz Bedenken des schweizerischen Bundesgerichts wegen möglichen Verstoßes gegen geltendes Recht hat die Züricher Kantonspolizei Überwachungssoftware des italienischen Unternehmens *Hacking Team* beschafft. Das Gericht hatte zuvor den Artikel 32 f des Züricher Polizeigesetzes für ungültig erklärt, in dem es heißt: „Eine Polizeioffizierin oder ein Polizeioffizier kann den Einsatz von technischen Mitteln zur Feststellung von verdächtigen Inhalten in einer einem beschränkten Benutzerkreis zugänglichen virtuellen Kommunikationsplattform anordnen, wenn die Abwehr einer drohenden Gefahr oder die Erkennung von Straftaten sonst aussichtslos wäre oder unverhältnismäßig erschwert würde.“ Es müsse stets eine richterliche Genehmigung vorliegen. Über diese Entscheidung hat sich die Kantonspolizei mit der Beschaffung hinweggesetzt (Quelle: zh.ch, Heise).

10. November 2015: Die europäische Polizeibehörde Europol fordert neue Befugnisse für das *Hinweiszentrum zur Internetüberwachung*. Betreiber sozialer Netzwerke wie Facebook oder Twitter sollten verpflichtet werden, der Behörde Informationen über Accounts und Profile, die mit einer bestimmten IP-Adresse verknüpft sind, zur Verfügung zu stellen. Das geht aus einem Papier der luxemburgischen Ratspräsidentschaft hervor, das durch *statewatch* veröffentlicht wurde. Die Daten sollten nicht nur für die Abwehr von Terrorismus genutzt werden; dem Bundesinnenministerium zufolge wolle man „flexibel auf veränderte

Anforderungen ... reagieren“. Denkbar wäre hier auch die Bekämpfung von Fluchthelfern (Quelle: statewatch, Tagesspiegel, Heise).

11. November 2015: Das *Unabhängige Landeszentrum für Datenschutz* (ULD) in Schleswig-Holstein kritisiert die dortige Praxis der Funkzellenabfrage. Es sei nicht klar, ob die Abfragen notwendig und verhältnismäßig seien, erklärte die stellvertretende Leiterin Barbara Körffer im schleswig-holsteinischen Landtag bei der Vorstellung eines entsprechenden Prüfberichts. Sie wies darauf hin, dass eine Funkzellenabfrage „in besonderem Maße eine Gefahr für Unbeteiligte“ erzeuge, „in die Ermittlungen einbezogen zu werden“. Bei der bisher umfangreichsten Abfrage wurden rund 7.000 Datensätze erfasst (Quelle: ULD, Heise).

12. November 2015: Im NSA-Untersuchungsausschuss hat die im Stab der Bundesdatenschutzbeauftragten für Geheimdienste zuständige Gabriele Löwnau die Verarbeitung von Daten durch den Bundesnachrichtendienst (BND) in Bad Aibling als „rechtswidrig“ bezeichnet. Voraussetzungen seien nicht erfüllt gewesen, die Dateien hätten die Anforderungen für eine Genehmigung durch Bundeskanzleramt und Datenschutzbehörde nicht erfüllt. Die Datenschutzbeauftragte des BND sei überhaupt nicht informiert worden (Quelle: Heise).

14. November 2015: Nach den Anschlägen am 13. November 2015 in Paris fordert ein Vertreter der Gewerkschaft der Polizei eine Ausweitung der Vorratsdatenspeicherung. Das „enge gefasste Gesetz zur Vorratsdatenspeicherung müsse überdacht werden, so der stellvertretende Vorsitzende der Gewerkschaft, Jörg Radek (Quelle: Rheinische Post, Heise).

19. November 2015: Frankreich verschärft nach den Anschlägen vom 13. November 2015 seine Sicherheitsgesetze. Der verhängte Ausnahmezustand soll um drei Monate verlängert werden; Gruppierungen, die aus Sicht der Behörden eine „schwere Gefährdung der öffentlichen Ordnung“ darstellen, sollen dabei aufgelöst werden können. In den Tagen nach den Morden gab es 414 Hausdurchsuchungen, 64 Menschen wurden vorläufig festgenommen, 60 kamen in Polizeigewahrsam, 118 Menschen wurden unter Hausarrest gestellt. Möglicherweise hat die Polizei einen weiteren Anschlag in Saint-Denis vereitelt (Quelle: Heise).

19. November 2015: Bundeswirtschaftsminister Sigmar Gabriel fordert „ein anderes Verständnis von Datenschutz“. Er plädiert für „Datensouveränität“ statt Datenschutz; ein „selbstbestimmter Umgang“ mit Daten sei wichtig. Datensparsamkeit passe nicht zum Geschäftsmodell *Big Data* (Quelle: Heise).



Stefan Hügel

Stefan Hügel, Vorsitzender des Fiff, studierte Informatik an den Universitäten Karlsruhe und Freiburg, wo er sein Studium mit der Diplomarbeit am Institut für Informatik und Gesellschaft abschloss. Er lebt in Frankfurt am Main und arbeitet als IT-Berater.

20. November 2015: Der EU-Datenschutzbeauftragte Giovanni Buttarelli weist darauf hin, dass auch bei *Big Data* Grundrechte gewahrt bleiben müssen. Die EU könne nicht einfach unkritisch „datengetriebene Technologien und Geschäftsmodelle“ aus „anderen Teilen der Welt“ importieren. Gegenwärtige Datenschutzprinzipien wie Transparenz, Verhältnismäßigkeit und Zweckbegrenzung blieben das Fundament, um die Grundrechte in einer *Big-Data*-Welt zu gewährleisten. Es gebe ein Problem der „Datenverschmutzung“ im Informationszeitalter, es drohe eine „Datendiktatur“ (Quelle: Heise).

25. November 2015: In Bayern soll der Einsatz von Uniformkameras bei Polizeieinsätzen getestet werden. Damit will man Angriffen auf Beamt:innen vorbeugen. Der bayerische Datenschutzbeauftragte Thomas Petri ist skeptisch: „Da glotzt ihn (den Bürger) ein drittes Auge an, und er wird das als Misstrauen des Staates empfinden.“ Er bezweifelt, dass dadurch eine Deeskalation eintreten wird. Die Ergebnisse eines Pilotversuchs in Hessen seien nicht übertragbar, da dort gleichzeitig die Polizeipräsenz erhöht worden sei (Quelle: Heise).

25. November 2015: Unter dem Eindruck der Anschläge vom 13. November wollen die Institutionen der EU die Zusammenarbeit bei der „inneren Sicherheit“ verstärken. Angestrebt wird unter anderem eine Einigung zur Fluggastdatenspeicherung noch im Jahr 2015. Die Gegner einer solchen Vorratsdatenspeicherung für innereuropäische Flüge im Europäischen Parlament werden gleichzeitig weniger; lediglich Grüne und Linke lehnen sie weiterhin ab (Quelle: Heise).

27. November 2015: Die zunehmende Videoüberwachung im öffentlichen Personennahverkehr kritisiert die niedersächsische Landesdatenschutzbeauftragte Barbara Thiel in ihrem Tätigkeitsbericht 2013/2014. „In den Fahrgastbereichen herrscht inzwischen eine totale Überwachung, flächendeckend und rund um die Uhr“, erklärte sie. Die dadurch vermittelte Sicherheit sei aber nur eine Suggestion (Quelle: Landesdatenschutzbeauftragte Niedersachsen, Heise).

28. November 2015: Eine bessere Überwachung von islamistischen Terroristen im Internet fordert EU-Digitalkommissar Günter Oettinger. Die Geheimdienste müssten technisch und personell ertüchtigt, der Austausch zwischen ihnen besser organisiert werden. „Gerade wir in Deutschland sollten endlich unser Grundmisstrauen gegenüber Geheimdiensten ablegen“, so Oettinger (Quelle: Heise).

Dezember 2015

1. Dezember 2015: Erstmals wurde in den USA nun ein *National Security Letter* veröffentlicht, mit dem die US-amerikanische Polizeibehörde FBI (Federal Bureau of Investigation) Unternehmen zur Herausgabe von Kundendaten bei gleichzeitigem völligem Stillschweigen verpflichtet. Aus dem Dokument geht hervor, in welchem Umfang die Behörde Daten ohne vorherigen richterlichen Beschluss anfordert. Die Daten umfassen unter anderem alle Adressen, die mit einem Account verbunden sind, Telefonnummern des Inhabers, An- und Abmeldungen des DSL-Accounts, Standortdaten eines zugehörigen Mobilfunkvertrags, verbundene Namen, Aufzeichnungen über Be-

stellungen, alle E-Mail- und IP-Adressen. Das Dokument durfte nur mit Schwärzungen veröffentlicht werden; die Geheimhaltung wird vom FBI damit begründet, dass potenziellen Zielpersonen nicht zu viel verraten werden dürfe (Quelle: ACLU, Washington Post, Heise).

2. Dezember 2015: Die Electronic Frontier Foundation (EFF) wirft Google vor, mit seinen Chromebooks Schulkinder auszuspiionieren. Chromebooks sind wartungsarm und wenig anfällig gegen Viren und deswegen an Schulen besonders beliebt. Aufgezeichnet würden Passwörter, besuchte Webseiten, Suchbegriffe, ausgewählte Suchergebnisse und Videos. Die Daten würden zwar nicht für Werbezwecke genutzt, könnten aber für andere Zwecke des Unternehmens und Zwecke Dritter verwendet werden (Quelle: EFF, Heise).

8. Dezember 2015: Aus Sicht der EU-Mitgliedsstaaten stellt die Rechtsprechung des Europäischen Gerichtshofs (EuGH), nach der dieser bezweifelt hatte, dass die Vorratsdatenspeicherung mit der Grundrechtecharta vereinbar sei, keine Hürde für die nationale Umsetzung einer Vorratsdatenspeicherung dar. Gleichzeitig fordern sie die EU-Kommission auf, eine neue EU-weite Grundlage dafür zu schaffen, um die heutige Fragmentierung der Datensammlung aufzuheben (Quelle: Heise).

10. Dezember 2015: Der Innenausschuss des Europäischen Parlaments hat der Vorratsspeicherung von Fluggastdaten zugestimmt. Die *Passenger Name Records* (PNR) sollen sechs Monate unmaskiert und weitere viereinhalb Jahre ohne direkten Personenbezug aufbewahrt werden; der Personenbezug dürfe aber unter bestimmten Umständen wiederhergestellt werden. Gespeichert werden sollen ca. 60 Datenkategorien, darunter E-Mail-Adresse, Telefon-, Konten-, Kreditkartennummern und Essenswünsche. Die Datensammlung erstreckt sich auf transkontinentale und innereuropäische Flüge (Quelle: Heise).

11. Dezember 2015: Volker Kauder, der Fraktionsvorsitzende der CDU im Deutschen Bundestag, spricht sich für eine enge Kooperation mit US-amerikanischen Geheimdiensten aus. „Ohne die enge Zusammenarbeit mit den Nachrichtendiensten in Europa und den USA wäre unser Land wesentlich unsicherer als jetzt“, behauptet der CDU-Politiker. „Wer diese Zusammenarbeit infrage stellt und meint, es gehe auch ohne diese Kooperation, gefährdet Menschen“ (Quelle: dpa, Heise).

19. Dezember 2015: Der britische Geheimdienst MI5 betreibt bereits seit 15 Jahren – offenbar am Parlament vorbei – unter dem Namen *Preston* eine Datenbank zu Vorratsspeicherung von Telekommunikations-, Finanz- und Reisedaten. Den Recherchen zufolge würden in der Datenbank pro Jahr rund vier Milliarden Verbindungs- und Standortinformationen aus der nationalen und internationalen Telekommunikation gesammelt (Quelle: The Register, Heise).

21. Dezember 2015: Für HTTP wird ein neuer Statuscode 451 eingeführt, der Zensur anzeigen soll, genauer: die Unterdrückung der Übertragung aus rechtlichen Gründen. Der Code geht auf den Roman *Fahrenheit 451* von Ray Bradbury zurück. In der Geschichte des Romans ist es verboten, Bücher zu besitzen; die Feuerwehr hat die Aufgabe, noch vorhandene Bücher zu verbrennen. *Fahrenheit 451* bezieht sich dabei auf die Tempera-

tur, bei der sich Papier entzündet. Die dazugehörige Meldung soll einen Text enthalten, der angibt, wer die Zensur auf welcher rechtlichen Grundlage verfügt hat und wer davon betroffen ist (Quelle: Heise).

23. Dezember 2015: Durch eine kritische Schwachstelle im Kabelnetz von *Kabel Deutschland/Vodafone* konnten fremde VoIP-Anschlüsse und Modems übernommen werden. Die Schwachstelle, von der 2,8 Millionen Kunden betroffen waren, wurde durch ein unzureichend abgesichertes Wartungsnetz verursacht (Quelle: Heise).

Januar 2016

11. Januar 2016: Der Bundesnachrichtendienst (BND) hat seine Kooperation mit der US-amerikanischen *National Security Agency* (NSA) in der Abhöranlage Bad Aibling wieder aufgenommen. Zuvor hatte die NSA begonnen, bei ihren Suchbegriffen Begründungen mitzuliefern. Die Kooperation war eingeschränkt worden, nachdem der BND ungeprüft Suchbegriffe in die Überwachungssysteme eingespeist hatte, die gegen europäische und deutsche Ziele gerichtet waren (Quelle: Süddeutsche Zeitung, WDR, NDR, Heise).

13. Januar 2016: Entgegen den Leitlinien im Kompromiss zur Einführung der Vorratsdatenspeicherung fordern Vertreter der CDU nun in der *Mainzer Erklärung*, dem Verfassungsschutz den Zugriff auf die gespeicherten Daten zu ermöglichen. Zugriffsmöglichkeiten für Sicherheitsbehörden sollen massiv ausgeweitet werden. Noch weiter geht die CSU in Bayern: Innenminister Joachim Herrmann brachte einen Gesetzentwurf auf den Weg, wonach das Landesamt für Verfassungsschutz als erste Geheimdienstbehörde bald auf Vorratsdaten zugreifen können soll (Quelle: CDU, Heise).

16. Januar 2016: Laut einem Bericht des Bundesverteidigungsministeriums bereitet die Bundeswehr angeblich eigene Cyber-Angriffe vor, um sich vor gegnerischen Attacken zu schützen. „Abwehrkonzepte, die über den rein passiven Schutz zur Minimierung der Auswirkungen“ eines Cyber-Angriffs hinausgehen, seien bereits von der NATO geprüft worden. Im April 2015 war in einem Strategiepapier die Rede von „offensiven Cyber-Fähigkeiten“ zur „Beeinträchtigung von fremden Informations- und Kommunikationssystemen“ (Quelle: netzpolitik.org, Spiegel, Heise).

19. Januar 2016: Nach den Erkenntnissen von *Amnesty International* werden im Kongo bei der Förderung von Kobalt, das in Laptops und Smartphones für Lithium-Ionen-Batterien benötigt wird, Kinder beschäftigt. Tausende, teilweise nur sieben Jahre alte Kinder seien ohne Sicherheitsausrüstung eingesetzt und erlitten unter anderem bleibende Lungenschäden. Der Lohn betrage ein bis zwei Dollar pro Tag. Das UN-Kinderhilfswerk hatte bereits 2014 geschätzt, dass in den Minen im Süden des Kongos rund 40.000 Minderjährige beschäftigt seien (Quelle: UN-Kinderhilfswerk, Amnesty International, Heise).

20. Januar 2016: Laut der Antwort der Bundesregierung auf eine Anfrage der Linksfraction wurde die Überwachung der Mobilkommunikation im zweiten Halbjahr 2015 deutlich aus-

geweitet. Die Zahl der *Stillen SMS* habe sich auf 116.948 vervielfacht. Auch das Bundesamt für Verfassungsschutz, der *Militärische Abschirmdienst* (MAD) und der Zoll setzten dieses Mittel ein. Aus Sicht von Andrej Hunko ist die *Stille SMS* als Ermittlungsinstrument rechtswidrig: „Polizei und Geheimdienste dürfen nur passiv die Kommunikation von Telefonen abhören. Als Ortungsimpulse werden die Stillen SMS aber von den Behörden selbst erzeugt“ (Quelle: Deutscher Bundestag, Andrej Hunko, Heise).

25. Januar 2016: Das umstrittene europäische Anti-Terror-Zentrum von Europol hat seine Arbeit aufgenommen. Europol-Direktor Rob Wainwright warnte dabei vor Anschlägen des *Islamischen Staats* in Europa. 39 Ermittler von Europol und fünf Experten aus Mitgliedsstaaten sollen zunächst am Anti-Terror-Zentrum arbeiten. Kritiker warnen davor, dass sich Europol zu einer kaum mehr kontrollierbaren Agentur entwickle (Quelle: Heise).

28. Januar 2016: Den durch die Snowden-Enthüllungen verursachten Imageschaden für ein „offenes Internet“ halten Diplomaten für schlimmer als die offengelegte Massenüberwachung, so der frühere Beauftragte für Cyber-Außenpolitik der Bundesregierung, Dirk Brengelmann, vor dem NSA-Untersuchungsausschuss. Man sei besorgt gewesen, dass das Narrativ des offenen Internets gegenüber Ländern wie Russland oder China nicht aufrechtzuerhalten sei (Quelle: Heise).

28. Januar 2016: Kanada stoppt den Austausch von Metadaten mit den *Five-Eyes*-Staaten, nachdem der Geheimdienst CSE (Communications Security Establishment) festgestellt hatte, dass bisher weitergegebene Metadaten nicht ausreichend anonymisiert gewesen seien. Vor der Weitergabe müsste das CSE dafür sorgen, dass Kanadier:innen in den Metadaten nicht mehr zu identifizieren seien (Quelle: CBC, Heise).

30. Januar 2016: Deutsche Sicherheitsbehörden sind überzeugt, dass die Cyberattacke auf den Deutschen Bundestag von der russischen Regierung ausging. Quelle des Angriffs sei klar ein russischer militärischer Nachrichtendienst. Bereits zuvor habe es Angriffe nach dem gleichen Muster gegeben; Ziel seien Rüstungsunternehmen und andere NATO-Staaten gewesen (Quelle: Spiegel, Heise).

Februar 2016

2. Februar 2016: Zwischen der EU und den USA wurde ein Nachfolgeabkommen für das vom EuGH abgelehnte Abkommen *Safe Harbor* ausgehandelt. Das neue Abkommen *EU-US Privacy Shield* sieht vor, dass das US-Handelsministerium die US-amerikanischen Firmen kontrolliert, die europäische Daten verarbeiten. Wer seine Datenschutz-Rechte im Namen der nationalen Sicherheit der USA verletzt sieht, könne sich an einen Ombudsmann wenden, der unabhängig von den US-Geheimdiensten sein soll. Jan Philipp Albrecht (Grüne), Abgeordneter des Europäischen Parlaments und Berichterstatter für die EU-Datenschutz-Grundverordnung bezeichnete die Erklärung als „Witz“, mit dem die EU-Kommission EU-Grundrechte verkaufe und eine erneute Niederlage vor dem EuGH riskiere (Quelle: Heise).



F..I..f..F..e..V.

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

Vierteljährlich erhalten Mitglieder die Fachzeitschrift FIfF-Kommunikation mit Artikeln zu aktuellen Themen, problematischen

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

FIfF-Mailinglisten

FIfF-Mailingliste

An- und Abmeldungen an:

<http://lists.fiff.de/mailman/listinfo/fiff-L>

Beiträge an: fiff-L@lists.fiff.de

FIfF-Mitgliederliste

An- und Abmeldungen an:

<http://lists.fiff.de/mailman/listinfo/mitglieder>

Mailingliste Videoüberwachung:

An- und Abmeldungen an:

<http://lists.fiff.de/mailman/listinfo/cctv-L>

Beiträge an: cctv-L@lists.fiff.de

FIfF online

Das ganze FIfF

www.fiff.de

Twitter FIfF e.V. – [@FIfF_de](https://twitter.com/FIfF_de)

Cyberpeace

cyberpeace.fiff.de

Twitter Cyberpeace – [@FIfF_AK_RUIN](https://twitter.com/FIfF_AK_RUIN)

Faire Computer

blog.faire-computer.de

Twitter Faire Computer – [@FaireComputer](https://twitter.com/FaireComputer)

Mitglieder-Wiki

<https://wiki.fiff.de>

FIfF-Beirat

Peter Bittner (Bad Homburg); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Wolfgang Coy** (Berlin); Prof. Dr. **Wolfgang Däubler** (Bremen); Prof. Dr. **Leonie Dreschler-Fischer** (Hamburg); Prof. Dr. **Christiane Floyd** (Hamburg); Prof. Dr. **Klaus Fuchs-Kittowski** (Berlin); Prof. Dr. **Michael Grütz** (Konstanz); Prof. Dr. **Thomas Herrmann** (Bochum); Prof. Dr. **Wolfgang Hesse** (Marburg); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (Konstanz); **Ulrich Klotz** (Frankfurt); Prof. Dr. **Klaus Köhler** (München); Prof. Dr. **Herbert Kubicek** (Bremen); Dr. **Constanze Kurz** (Berlin); Prof. Dr. **Klaus-Peter Löhr** (Berlin); **Werner Mühlmann** (Oppung); Prof. Dr. **Frieder Nake** (Bremen); Prof. Dr. **Rolf Oberliesen** (Bremen); Prof. Dr. **Arno Rolf** (Hamburg); Prof. Dr. **Alexander Rossnagel** (Kassel); Prof. Dr. **Gerhard Sagerer** (Bielefeld); Prof. Dr. **Gabriele Schade** (Erfurt); Prof. Dr. **Dirk Siefkes** †; **Ralf E. Streibl** (Bremen); Prof. Dr. **Marie-Theres Tinnefeld** (München); Dr. **Gerhard Wohland** (Waldorfhäslach)

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Prof. Dr. **Dietrich Meyer-Ebrecht** (stellv. Vorsitzender) – Aachen
Michael Ahlmann – Bremen
Sylvia Johnigk – München
Benjamin Kees – Berlin
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Rainer Rehak – Berlin
Jens Rinne – Mannheim
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Ingrid Schlagheck – Bremen
Anne Schnerrer – Berlin
Prof. Dr. **Werner Winzerling** – Fulda
Prof. Dr. **Eberhard Zehendner** – Jena

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FlFF)
Verlagsadresse	FlFF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 fiff@fiff.de
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 100 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FlFF-Kommunikation ist für FlFF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FlFF-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 Zehndner
Schwerpunktredaktion	Felix Freiling, Stefan Hügel
V.i.S.d.P.	Stefan Hügel
FlFF-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, SchlussFlFF	Beiträge für diese Rubriken bitte per E-Mail an redaktion@fiff.de
Layout	Berthold Schroeder
Titelbild	Valid street photography, Foto: Isengardt (li.) Kunstprojekt 11 TAGE, Florian Mehnert (re.)
Druck	Meiners Druck, Bremen

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

Die FlFF-Kommunikation ist das Organ des FlFF und den politischen Zielen und Werten des FlFF 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 FlFF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

(mehr Termine unter www.fiff.de)

32. FlFF-Konferenz FlFFKon 2016

25.-27. November 2016 in Berlin

FlFF-Kommunikation

2/2016 »Transhumanismus«

Karsten Wendland, Britta Schinzel

Redaktionsschluss: 6. Mai 2016

W&F – Wissenschaft & Frieden

1/15 – Afrika (mit Dossier 77: Rechter Terror in Deutschland)

2/15 – Technikkonflikte (mit Dossier 78: Zivilklauseln)

3/15 – Friedensverhandlungen (mit Dossier 79: Kriegführung im Cyberspace)

4/15 – Deutsche Verantwortung – Zäsur oder Kontinuität (mit Dossier 80: Feindbilder und Konflikteskalation)

1/16 Für den Frieden forschen? (mit Dossier 81: Deutsche Rüstungsexporte – Skandale und Reförmchen)

2/16 Stadt und Krieg (mit Dossier 82: Türkei)

3/16 Islamisierung

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

#210/211 Gesetzgebung zum Verbot der Suizidbeihilfe

#212 Reflexhaftes Strafrecht

#213 10 Jahre Versammlungsrecht der Länder

DANA – Datenschutz-Nachrichten

3/15 – Rote Linien zur EU-DSGVO

4/15 – Sichere Häfen

1/16 – Innere Sicherheit

Das FlFF-Büro

Geschäftsstelle FlFF 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 FlFF-Kommunikation:

redaktion@fiff.de

Schluss F...I...f...F...

Dietrich Meyer-Ebrecht

Der Kanarienvogel ist tot

Manche Dinge nimmt man erst wahr, wenn sie nicht mehr da sind. Wie zum Beispiel ein Haus, an dem man immer achtlos vorbeiging und das überraschend abgerissen worden ist. Und man fragt sich, da stand doch bisher ein Haus? Oder ein stetiges Hintergrundgeräusch. Dann verstummt es unerwartet, und wir merken erst jetzt, da war doch was? Die eigentliche Nachricht ist das Ausbleiben einer Nachricht. Leicht geht sie unter. Aber wieder haben Wachsame aufgepasst, die sich für die *Transparency Reports* interessieren, die seit kurzem von Unternehmen veröffentlicht werden, die Internetportale betreiben. Dieses Mal ging es um die Plattform *reddit.com*, auf der monatlich knapp eine viertel Milliarde registrierte Nutzer:innen ihre Mitteilungen, Ansichten, Kommentare teilen und ihre Informationen einstellen. Mit ihren *Transparency Reports* kommen diese Unternehmen dem Wunsch ihrer Nutzer:innen nach, über gerichtliche und behördliche Aufforderung zur Preisgabe persönlicher Daten und ihren Umgang mit ihnen zu informieren – und die Behörden auszutricksen ...

Denn seit 2001 verfügen US-Behörden wie das FBI mit dem *National Security Letter*, geschaffen mit dem *Patriot Act*, über ein Instrument, mit dem sie Unternehmen zur Herausgabe ihrer Kundendaten zwingen können. Damit verbunden schreibt darüber hinaus die so genannte *Gag Order* den betroffenen Unternehmen vor, dass sie ihren Kunden den Zugriff verschweigen müssen. Hier kommt nun der Kanarienvogel endlich ins Spiel: Wie der unter Tage mitgenommene Kanarienvogel die Bergleute vor drohendem Sauerstoffmangel warnen sollte – er reagiert früher als Menschen auf Sauerstoffmangel, hört auf zu singen und wird bewusstlos –, soll ein *Warrant Canary* ein Indikator für das Eintreffen eines *National Security Letter* sein. Unternehmen sollen, so die Empfehlung von Bürgerrechtlern, regelmäßig in *Transparency Reports* über alle Anweisungen zur Herausgabe von Kundendaten berichten und, solange dies der Fall ist, den *National Security Letter* explizit als nicht vorliegend erwähnen. Bleibt genau diese Meldung aus, ist der Kanarienvogel verstummt.

Dies nun fanden wieder einmal aufmerksame Leser in dem gerade von Reddit, Inc. veröffentlichtem *Transparency Report 2015*, wie das Portal *t3n* berichtet.¹ Während es im *Transparency Report 2014* noch hieß, „bis zum 29. Januar 2015 hat Reddit keinen *National Security Letter* erhalten“,² fehlt diese Meldung im gerade veröffentlichten neuen Bericht – *no comment* ... „Der Kanarienvogel singt nicht mehr“,³ titelt Simon Hurtz in der Süddeutschen Zeitung in seinem Bericht über den pfiffigen Trick, mit dem sich US-Unternehmen gegen den Maulkorb der Behörden wehren, wie seinerzeit *Gigaom* auch schon von Apple berichtete.⁴ „Der Kanarienvogel ist tot und jeder weiß, was das heißt.“ Natürlich beilegen sich die Behörden, *Warrant Canaries* für illegal zu erklären. Doch für Reddit hat der Kanarienvogel auch dieses Mal offensichtlich seinen Dienst getan. Lasst uns also in Zukunft weiter aufmerksam auf verborgene Vogelstimmen horchen ...

Anmerkungen

1 <http://t3n.de/news/gibt-reddit-fbi-zugriff-693771> (02.04.2016)

2 <https://www.reddit.com/wiki/transparency/2014> (29.01.2015)

3 *Süddeutsche Zeitung*, 02./03.04.2016, S. 26

4 <https://gigaom.com/2014/09/18/apples-warrant-canary-disappears-suggesting-new-patriot-act-demands/> (18.09.2014)

