H 7625

FIfF-Kommunikation

Zeitschrift für Informatik und Gesellschaft

36. Jahrgang 2019 Einzelpreis: 7 EUR 1/2019 – März 2019

Brave New World

Gestaltungsfreiheiten und Machtmuster soziotechnischer Systeme – 1

ISSN 0938-3476

• 70 Jahre Grundgesetz • 2. Cyberpeace-Forum • Überwachungsgesamtrechnung •

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

Titelbild: Motiv des Tagungsplakats der FIfFKon 2018

Inhalt

Ausgabe 1/2019

inhalt

Editorial

Im September fand in Berlin die *FIfF-Konferenz* 2018 statt. *Brave new World – Gestaltungsfreiheiten und Machtmuster soziotechnischer Systeme* war das Leitmotiv der Konferenz, für die wir eine Reihe hochkarätiger Referentinnen und Referenten für Vorträge und Workshops gewinnen konnten – so viele, dass ein Heft dafür nicht ausreicht und wir einen zweiten Teil in der folgenden Ausgabe 2/2019 planen.

Ein ausführliches Schwerpunkteditorial führt in die Beiträge dieser Ausgabe ein:

> *Viele Produkte, Entwicklungen und Einsatzfelder der Informatik scheinen sich unausweichlich und technisch notwendig so entwickelt zu haben, wie wir sie heute kennen. … [Doch] es gibt immer verschiedene Wege, ein Problem anzugehen und entsprechend Ressourcen für dessen Lösung aufzuwenden. Oftmals liegen den tatsächlichen Entwicklungen gerade keine primär technischen Überlegungen zu Grunde, sondern ökonomische oder politische Motive. … Wir wollen auch aktiv an aktuellen und zukünftigen tiefgreifenden Veränderungen mitwirken, denn die Informatik ist immer auch Gestaltungsdisziplin – weit über die reine Technik hinaus. Wir wollen Sichtweisen und konkrete Wege erarbeiten, auf welche Weise nicht-technische Werte wie demokratische Teilhabe, Freiheit und Selbstbestimmung, Pluralismus von Lebensentwürfen und Nachvollziehbarkeit von Entscheidungen genauso in technischen Systemen und den politischen Entscheidungen darüber Eingang finden, wie die Verhinderung verdeckter Machtzentren, die Bekämpfung von Diskriminierung und struktureller Benachteiligung, Privatisierung staatlicher Kernaufgaben. … Wir müssen die Freiheitsgrade der Technik ausnutzen, aber vor allem müssen wir den politischen Willen dafür aufbringen. Wir wollen tatsächlich mutig sein und mit den Vorträgen dieser Konferenz dazu beitragen, eine neue, bessere Welt für alle Menschen zu erdenken um sie dann zu bauen.*

In diesem Jahr begehen wir ein Jubiläum: *70 Jahre Grundgesetz*. Doch *Dagmar Boedicker* zieht dazu eine ernüchternde Bilanz: Nach dem *Großartigen Versprechen 1949, so* stellt sie fest,

> *„… haben [wir] Anlass, an der Verwirklichung nahezu aller Konzepte der vier Verfassungsmütter und 61 Verfassungsväter zu zweifeln: Der Gesetzgeber versäumt es seit Gründungszeiten des Internet, uns vor Datenkraken zu schützen, seien es Geheimdienste, IT-Monopolisten oder andere. Ganz im Gegenteil bedient er sich der allgegenwärtigen Technik, um die in zahllosen Gesetzen erlaubte heimliche Überwachung durchzuführen und zerstört unsere Erwartungen an eine weder dem Staat noch anderen zugängliche Privatsphäre."*

Mit dem Bundesverfassungsgericht fordert sie eine Überwachungsgesamtrechnung, die die Erforderlichkeit von neuen Befugnissen nachweist. In einem zweiten Beitrag, *Leerstelle in der legislativen Praxis*, bekräftigt und konkretisiert sie diese Forderung.

Fridays for Future ist die Bewegung von Schülerinnen und Schülern, Studentinnen und Studenten, die uns und die Politik auffordert, Klimaschutz endlich ernst zu nehmen und ihre Zukunft nicht länger zu gefährden. Doch selbst eine Forderung, die selbstverständlich scheint – Einhaltung des Pariser Übereinkommens für den Klimaschutz – ruft erheblichen Widerstand bei den Profiteuren klimaschädlichen Wirtschaftens hervor – von den Klimaleugnern gar nicht erst zu reden. Doch *Fridays for Future kann* sich auf wissenschaftliche Erkenntnisse – beispielsweise des IPCC – berufen, die von seriösen WissenschaftlerInnen nicht mehr bestritten werden. Rund 27.000 Unterschriften sammelten die *Scientists for Future*, die die Forderungen nachdrücklich unterstützen.

Die Verbindung zwischen Umwelt und Digitalisierung thematisierte die Konferenz *Bits & Bäume*, bei der im November *Ökos* und *Techies* in Berlin zusammenkamen, um gemeinsame Positionen zu erarbeiten und Möglichkeiten der Zusammenarbeit auszuloten. Die Forderungen, die auf der Konferenz erhoben wurden, drucken wir ebenfalls in dieser Ausgabe.

Das zweite große Thema, das in den letzten Wochen vor allem junge Menschen auf die Straße trieb, ist das neue Urheberrecht. Ein zeitgemäßes Urheberrecht wird von Vielen seit langem gefordert – was wir aber nun bekommen haben, ist eine Richtlinie, die mit Upload-Filtern Überwachung und Zensur Vorschub leistet und deren Nutzen für die eigentlichen Urheber – zugunsten der großen Verlage – weithin in Zweifel gezogen wird. *Anna Biselli* stellt in einem Beitrag, den wir aus *netzpolitik.org* übernehmen, die Vorgeschichte dieser Urheberrechtsreform dar.

Was bei der Debatte zum Urheberrecht ebenso wie bei *Fridays for Future* auffiel, ist ein sich etablierender Stil des öffentlichen Diskurses, der ohne jede Beißhemmung anstrebt, Kritik zu delegitimieren und lächerlich zu machen. Demonstranten mit Hass und Häme zu überschütten, eine politische Bewegung als „fremdgesteuert" und als „Bots" abzuqualifizieren, ist erbärmlich und beschämend und darf in einer demokratischen Gesellschaft nicht akzeptiert werden.

Inzwischen wurde das neue Urheberrecht trotz der Proteste beschlossen. Welche Auswirkung Verlauf und Ergebnis der Debatte auf die politische Kultur haben, wird sich zeigen.

Machine Learning und *Künstliche Intelligenz* sind Themen, die für das FIfF eine wachsende Bedeutung haben und voraussichtlich weiterhin haben werden. Unsere *FIfF-Konferenz* 2019 in Bremen wird sich im November damit auseinandersetzen. In dieser Ausgabe der *FIfF-Kommunikation* rezensiert *Britta Schinzel* ausführlich den Sammelband *Machine Learning. Medien, Infrastrukturen und Technologien der Künstlichen Intelligenz*.

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

Stefan Hügel
für die Redaktion

Der offene Brief

Fridays for Future[1] – FIfF for Future!

Liebe Schülerinnen und Schüler,

Ihr seid großartig! Wohl keine Bewegung hat es bisher geschafft, in so kurzer Zeit so viele Menschen weltweit auf die Straße zu bringen. 300.000 Demonstrierende alleine in Deutschland, Zigtausende an vielen Orten weltweit, insgesamt offenbar mehr als eine Million – wow! Und die echten „Profis" habt Ihr auf Eurer Seite: Eure Forderungen werden von den eigens gegründeten ScientistsForFuture nachdrücklich unterstützt, mit einer Stellungnahme, die von rund 27.000 WissenschaftlerInnen unterzeichnet wurde.[2]

Manche behaupten, man würde Euch nicht ernst nehmen, weil Ihr Jugendliche und Kinder seid. Das ist ein Irrtum: Die Delegitimierungskampagnen, die bereits auf Hochtouren laufen, beweisen das Gegenteil.[3] Dass einige von Euch bei McDonalds einen Hamburger gegessen und anschließend das Papierl auf den Boden geworfen haben sollen, gegen den Klimaschutz ausspielen zu wollen, ist erbärmlich.

Doch was fordert Ihr eigentlich? Die Basis der Forderungen von Greta Thunberg bei ihren Klimastreiks seit August in Stockholm war die Einhaltung des Übereinkommens von Paris, eines völkerrechtlichen Vertrags zum Klimaschutz. Es ist beklemmend, welchem Widerstand man sich heute gegenüber sieht, wenn man nur die Einhaltung völkerrechtlicher Abkommen fordert.

Doch lassen wir hier Greta Thunberg selbst zu Wort kommen:

> *„Our civilisation ist being sacrificed for the opportunity of a very small number of people to continue making enormous amounts of money. [...] It is the sufferings of the many which pay for the luxuries of the few. […] You say, you love your children above all else. And yet, you're stealing their future in front of their very eyes. […] We cannot solve a crisis without treating it as a crisis. […] And if solutions within this system are so impossible to find, then maybe we should change the system itself. […] We have run out of excuses and we are running out of time. We have come here to let you know that change ist coming, whether you like it or not. The real power belongs to the people."*[4]

Immer wieder wird beklagt, dass Ihr zu wenig politisch aktiv seid – und wenn Ihr es seid, ist es auch wieder nicht recht. Früh in eine Partei eintreten – egal in welche –, dann vielleicht in Partei- und öffentlichen Ämtern Karriere machen und danach einer lukrativen Tätigkeit als Lobbyist nachgehen. Das ist wohl gemeint, wenn Ihr von PolitikerInnen zu mehr Engagement aufgefordert werdet. Wirklich Eure Zukunft in die eigenen Hände zu nehmen, ist damit eher nicht so gemeint.

Erinnerungen an die Zeit, als ich selbst noch Schüler war, in den 1980er-Jahren: Schon damals wies uns unser Englisch-Lehrer auf den CO_2-Ausstoß und die Folgen für das Klima hin. Zweifellos ist seither auch einiges passiert – aber nicht genug. Und es haben auch nicht alle begriffen: Das *Sports Utility Vehicle* (SUV) – das wohl als eins der eindrücklichsten Sinnbilder für den verantwortungslosen Umgang mit der Umwelt gilt – wurde erst danach erfunden und fand weite Verbreitung.

Übrigens darf meine Generation nicht behaupten, sie habe von nichts gewusst: Wir wurden die „Null-Bock-Generation" genannt; den damals verbreiteten Slogan „No Future!" habt Ihr im Grunde mit „Fridays for Future!" ins Positive gewendet. Damals ging es um Atomrüstung und Atomenergie – ersteres durch die Kündigung des INF-Vertrags wieder aktueller denn je. 1980 wurde die Partei „Die Grünen" gegründet. Viel von den radikalen Umwelt- und friedenspolitischen Forderungen der damaligen Zeit hat sich im Lauf der Jahre abgeschliffen – heute sind die Grünen mitverantwortlich für Kriegseinsätze der Bundeswehr, und auch umweltpolitisch ist man „pragmatisch" geworden, wie zum Beispiel beim Bahnhof Stuttgart 21 sichtbar ist, der unter der Verantwortung der Grünen – sowohl im Land Baden-Württemberg als auch in Stuttgart – immer weiter vorangetrieben wird. Gleichzeitig ist aber – trotz alledem – das Bewusstsein für die Umwelt seit damals gestiegen. Ich glaube, wir wären heute entsetzt, wenn wir in die 1970er- oder 1980er-Jahre zurückversetzt würden – mit der damaligen Verschmutzung der Luft, der Gewässer und von Umweltkatastrophen wie Seveso, Bhopal, Harrisburg, Tschernobyl, … Befremdlich, dass sich einige „Konservative" gerade diese Vergangenheit zurück wünschen.

À propos – was sagen eigentlich die Konservativen? „Konservativ" kommt von lat. „conservare", das bedeutet „erhalten" oder „bewahren". Das ist doch genau das, was wir gerade brauchen, müsste man meinen. Doch das Einzige, was so mancher „Konservative" offensichtlich bewahren möchte, sind überkommene Machtstrukturen und seine eigenen Privilegien.

Eins wird Euch möglicherweise nicht erspart bleiben: Wenn Ihr Erfolg habt und die Klimakatastrophe noch abgewendet werden kann, werden sich „Profis" – vielleicht ja auch Christian Lindner – breitbeinig hinstellen und erklären, dass ihre vorausschauende Politik für die Rettung der Welt verantwortlich sei. Für diesen Fall solltet Ihr Euch vorsorglich ein Beißholz bereithalten.

Widerwillig komme ich – weil es offenbar nicht zu vermeiden ist – auf den Begriff des „Schuleschwänzens". Das ist Unsinn! Ziel der Schule darf nicht das Absitzen von Schulstunden, sondern Bildung sein: Die Welt zu begreifen und das Begriffene auch anzuwenden. Genau das tut Ihr. Und sollte es Einzelne unter Euch geben, die gerne eine „Freistunde" bei den Streiks ausnutzen: Bestimmt gibt es genügend Abgeordnete des Deutschen Bundestags, die nicht wegen Ihrer politischen Haltung, sondern allein aus Eigennutz, nämlich für Karriere und Geldverdienen, ihr Mandat wahrnehmen.

Ihr sollt in der schulfreien Zeit streiken, wird gefordert – so ein Quatsch. Wann, glaubt Ihr, führen PolitikerInnen ihre Gespräche

mit Energielobbyisten? Womöglich während ihrer von uns allen bezahlten Arbeitszeit? Eben!

Letztlich dient auch diese Diskussion nichts anderem, als Euer berechtigtes Anliegen zu delegitimieren und davon abzulenken. Ihr habt es längst selber gemerkt: Wer über „Schuleschwänzen" spricht, braucht sich scheinbar mit den Folgen des Klimawandels nicht mehr auseinanderzusetzen.

Umweltpolitik und Klimawandel sind nicht die Kernkompetenzen des FIfF. Doch auch wir beschäftigen uns damit: Bei der Konferenz „Bits & Bäume"[5] setzten wir uns gemeinsam mit vielen Umweltorganisationen mit dem Zusammenhang von Ökologie und Digitalisierung auseinander. Eins ist völlig klar: Der Klimawandel betrifft uns alle – und so seid Euch unserer umfassenden Unterstützung gewiss.

Mit FIfFigen Grüßen

Stefan Hügel

Anmerkungen

1 *https://fridaysforfuture.de*

2 *Webseite und Stellungnahme unter https://www.scientists4future.org; die Aufzeichnung von der Bundespressekonferenz am 12. März 2019 ist unter https://www.youtube.com/watch?v=OAoPkVfeTo012 zu finden.*

3 *Lesenswert dazu: von Lucke A (2019) „Fridays for Future": Der Kampf um die Empörungshoheit. Wie die junge Generation um ihre Stimme gebracht werden soll. Blätter für deutsche und internationale Politik 3'19, https://www.blaetter.de/archiv/jahrgaenge/2019/maerz/fridays-for-future-der-kampf-um-die-empoerungshoheit*

4 *Rede von Greta Thunberg vor der UN-Klimaschutzkonferenz in Katowice, https://www.youtube.com/watch?v=qvmwt8iJIB4*

5 *Die Webseiten zur Konferenz sind unter https://bits-und-baeume.org zu finden. Ein Dokumentationsband ist in Vorbereitung.*

Dagmar Boedicker

70 Jahre Grundgesetz

Alle staatliche Gewalt ist laut Artikel 1 des Grundgesetzes verpflichtet, die Würde des Menschen nicht nur zu achten, sondern sie auch zu schützen. Leider fällt eine Bilanz darüber beschämend aus, wie die staatliche Gewalt dieser Pflicht in den letzten Jahrzehnten nachgekommen ist. Sie muss etwas falsch verstanden haben, wenn sie nicht etwa die unantastbare Würde des Menschen als Supergrundrecht *betrachtet, sondern ein Innenminister*[1] *ein fiktives Supergrundrecht* Sicherheit *propagiert. Selbst an diesem Anspruch dürfen wir sie aber nicht messen, denn sicher sind wir in Zeiten der* Insecurity of Things (IoT) *und der massenhaften Ausspähung durch staatliche und private Stellen wahrhaftig nicht. Es wird Zeit, unsere enteignete Würde zurück zu erobern, auch von unseren Repräsentanten in den Parlamenten. Leider genügt es nicht, wenn das Bundesverfassungsgericht (BVerfG) uns den Anspruch darauf bescheinigt, sich der Gesetzgeber aber einfach einen Dreck darum schert.*

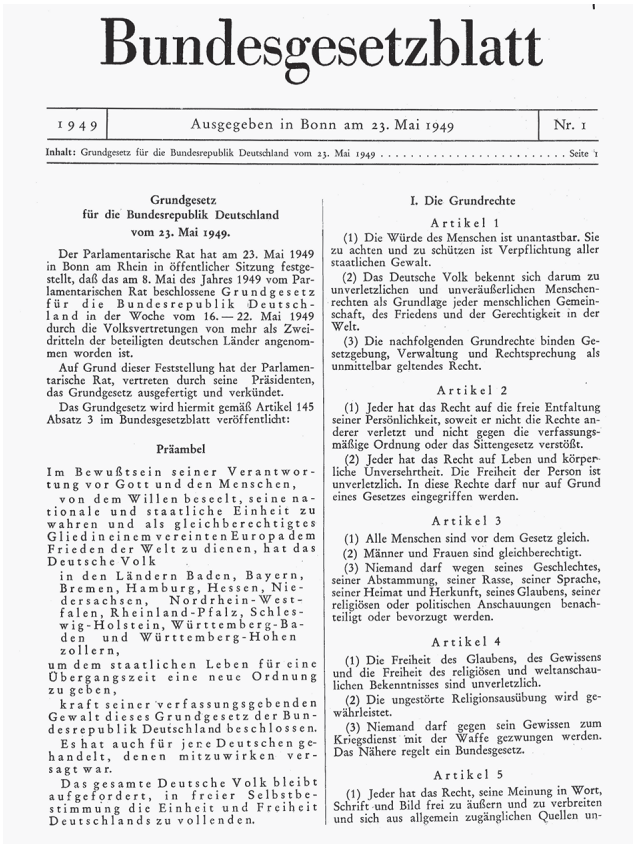
Wie fragil die Demokratie ist, wenn zu wenige sie verteidigen, wird uns wohl die Wahl zum Europäischen Parlament am 26. Mai demonstrieren. Bisher standen dort freiheitlich denkende Abgeordnete den nationalen Bedürfnissen nach Überwachung immer wieder mal im Weg.[2] *Das wird sich ändern, wenn wir nicht erkennen, dass Freiheit nicht allen Abgeordneten ein Anliegen ist, und dass die Zahl derjenigen ein beängstigendes Ausmaß erreicht hat, die Kontrolle über unsere Meinung und unser Verhalten höher bewerten. Sie bevorzugen die Einschüchterung durch ausufernde Überwachung.*

Es ist an sich gut, dass viele nationale Kompetenzen auf die Ebene der Europäischen Union verlagert worden sind, denn Nationalstaaten können sie angesichts der technischen und ökonomischen Globalisierung nicht mehr ausreichend wahrnehmen. Die Grundrechte-Charta der EU und die Menschenrechts-Konvention des Europarats sollten unsere Freiheitsrechte auch ausreichend schützen. Wieso fällt dann aber trotz mehrerer Urteile des Europäischen Gerichtshofs (EuGH), des Europäischen Gerichtshofs für Menschenrechte (EGMR) und des Bundesverfassungsgerichts (BVerfG) die Überwachungsgesamtrechnung desaströs aus und nur *die üblichen Verdächtigen* regen sich darüber auf?

Vorderseite der 10-DM-Gedenkmünze „50 Jahre Grundgesetz der Bundesrepublik Deutschland"

1949. Großartiges Versprechen

Im Grundgesetz finden sich Lehren aus den Erfahrungen mit der Nazi-Diktatur. Freiheitsrechte sind festgeschrieben, wie das Abwehrrecht gegenüber dem Staat und das Asylrecht. Artikel 1 unterliegt der Ewigkeitsgarantie, der Bundestag kann ihn nicht ändern, auch nicht mit verfassungsändernder Mehrheit.[3] Artikel 1 verpflichtet den Staat dazu, die Menschenwürde nicht nur zu achten sondern auch aktiv zu schützen. „In keinem Fall darf ein Grundrecht in seinem Wesensgehalt angetastet werden."[4] Eine unabhängige Justiz soll dem Gesetzgeber auf die Finger sehen. Medien haben die Aufgabe, die Legislative, Exekutive und Judikative zu beobachten und frei und unabhängig zu informieren.



Bundesgesetzblatt

1949 | Ausgegeben in Bonn am 23. Mai 1949 | Nr. 1

Inhalt: Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 ..... Seite 1

Grundgesetz
für die Bundesrepublik Deutschland
vom 23. Mai 1949.

Der Parlamentarische Rat hat am 23. Mai 1949 in Bonn am Rhein in öffentlicher Sitzung festgestellt, daß das am 8. Mai des Jahres 1949 vom Parlamentarischen Rat beschlossene Grundgesetz für die Bundesrepublik Deutschland in der Woche vom 16. — 22. Mai 1949 durch die Volksvertretungen von mehr als Zweidritteln der beteiligten deutschen Länder angenommen worden ist.

Auf Grund dieser Feststellung hat der Parlamentarische Rat, vertreten durch seine Präsidenten, das Grundgesetz ausgefertigt und verkündet.

Das Grundgesetz wird hiermit gemäß Artikel 145 Absatz 3 im Bundesgesetzblatt veröffentlicht:

Präambel

Im Bewußtsein seiner Verantwortung vor Gott und den Menschen,

von dem Willen beseelt, seine nationale und staatliche Einheit zu wahren und als gleichberechtigtes Glied in einem vereinten Europa dem Frieden der Welt zu dienen, hat das Deutsche Volk

in den Ländern Baden, Bayern, Bremen, Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Schleswig-Holstein, Württemberg-Baden und Württemberg-Hohenzollern,

um dem staatlichen Leben für eine Übergangszeit eine neue Ordnung zu geben,

kraft seiner verfassungsgebenden Gewalt dieses Grundgesetz der Bundesrepublik Deutschland beschlossen.

Es hat auch für jene Deutschen gehandelt, denen mitzuwirken versagt war.

Das gesamte Deutsche Volk bleibt aufgefordert, in freier Selbstbestimmung die Einheit und Freiheit Deutschlands zu vollenden.

I. Die Grundrechte

Artikel 1

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.

(3) Die nachfolgenden Grundrechte binden Gesetzgebung, Verwaltung und Rechtsprechung als unmittelbar geltendes Recht.

Artikel 2

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

Artikel 3

(1) Alle Menschen sind vor dem Gesetz gleich.

(2) Männer und Frauen sind gleichberechtigt.

(3) Niemand darf wegen seines Geschlechtes, seiner Abstammung, seiner Rasse, seiner Sprache, seiner Heimat und Herkunft, seines Glaubens, seiner religiösen oder politischen Anschauungen benachteiligt oder bevorzugt werden.

Artikel 4

(1) Die Freiheit des Glaubens, des Gewissens und die Freiheit des religiösen und weltanschaulichen Bekenntnisses sind unverletzlich.

(2) Die ungestörte Religionsausübung wird gewährleistet.

(3) Niemand darf gegen sein Gewissen zum Kriegsdienst mit der Waffe gezwungen werden. Das Nähere regelt ein Bundesgesetz.

Artikel 5

(1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen un-

Erste Ausgabe des Bundesgesetzblatts I vom 23.05.1949 mit dem Text des Grundgesetzes

Jeder Mensch im Geltungsbereich des Grundgesetzes hat das Recht auf ihre/seine Meinung, auch darauf, sie zu äußern. Das sind Grundbedingungen der freiheitlich demokratischen Grundordnung.

2019. Große Enttäuschung

Inzwischen bestimmen zwei Generationen ohne Diktatur- und Kriegserfahrung das politische Geschehen. Wäre es unfair, wenn man ihnen – oder vielmehr uns – vorwerfen würde, geschichtsvergessen zu sein? Möglicherweise braucht das unvernünftige Menschengeschlecht direkte Erfahrung, zumindest von Zeitzeugen im Nahbereich. Es hätte geholfen, wenn die Mitgliedstaaten der EU nach dem Fall des Eisernen Vorhangs ihre Diktaturerfahrungen gemeinsam aufgearbeitet hätten. Griechenland und Slowenien, Portugal, Polen und die Slowakei hätten sich und uns viel zu sagen gehabt. Ein solcher Diskurs vieler Stimmen hat nicht stattgefunden. Vielleicht will sich niemand daran erinnern, wohin es führt, wenn ein Autokrat auf Untertanen trifft. Anders kann ich mir das Desinteresse vieler an Demokratie und Rechtsstaat nicht erklären und den Eifer von Abgeordneten, im Rechtsstaat wie in einem Steinbruch zu Werke zu gehen.

Wir haben Anlass, an der Verwirklichung nahezu aller Konzepte der vier Verfassungsmütter und 61 Verfassungsväter zu zweifeln: Der Gesetzgeber versäumt es seit Gründungszeiten *des Internet,* uns vor Datenkraken zu schützen, seien es Geheimdienste, IT-Monopolisten oder andere. Ganz im Gegenteil bedient er sich der allgegenwärtigen Technik, um die in zahllosen Gesetzen erlaubte heimliche Überwachung durchzuführen und zerstört unsere Erwartungen an eine weder dem Staat noch anderen zugängliche Privatsphäre.

Sind die Medien ein kontrollierendes Gegengewicht? Der Blick auf die Kommunikationskultur in manchen Echokammern der sogenannten sozialen Netze überzeugt nicht recht. Klassische Medien wie die gedruckten, das Fernsehen oder Radio sehen sich unter Wettbewerbsdruck und oft überfordert von ihrer Aufgabe. Sie sollen über wenig klare und viel zu viele Gesetzesnormen informieren, bei zu geringen Kontrollrechten und Auskunftspflichten. Da ist es eine undankbare Arbeit, Transparenz herzustellen, zumal Zuschauer, Hörer und Leser wenig Interesse dafür aufbringen.

Was können wir von der Justiz erwarten? Sie soll die rechtmäßige Gestaltung und Umsetzung der Gesetze prüfen, von Gesetzen, deren Gehalt immer wieder vom Bundesverfassungsgericht als verfassungswidrig beurteilt wurde. Viel hilft das nicht, wenn das Bundesverfassungsgericht beispielsweise Regelungen im BKA-Gesetz schon 2008[5] und erneut 2016[6] als nicht mit der Verfassung vereinbar erklärt. Wie viele Verfassungsbeschwerden gegen wie viele Sicherheitsgesetze sind eigentlich anhängig vor dem Bundes- und vor Landesverfassungsgerichten? Wie lange dauert es, bis die Gerichte entscheiden? Richtet sich der Gesetzgeber nach ihren Urteilen, nachdem sie entschieden haben? Bis dahin wenden die Sicherheitsbehörden diese Gesetze regelmäßig weiterhin an und sammeln Information über uns, was das Zeug hält.

Exekutive und Parlamente tasten Grundrechte in ihrem Wesensgehalt an und weigern sich, darüber Rechenschaft abzulegen. Eine solche Rechenschaft würde voraussetzen, dass sie jede neue Befugnis im Licht dessen betrachten, was bereits möglich ist, und den Nachweis liefern, dass vorhandene Maßnahmen erfolgreich waren und ihre Ausweitung unabdingbar ist.

Was können wir tun?

Wir fordern eine Überwachungsgesamtrechnung vor jedem Gesetz auf Landes- oder Bundesebene, das Überwachungsbefugnisse enthält. Der Gesetzgeber muss nachweisen, dass weitere Überwachungsbefugnisse erforderlich sind, und prüfen, ob sie dem Verfassungsgerichts-Urteil noch entsprechen oder es bereits missachten. In einem Beitrag auf Seite 8 konkretisiere ich, warum wir eine solche Überwachungsgesamtrechnung brauchen, und welche weiteren Forderungen sinnvoll sind.

Anmerkungen

1 *Friedrich, 2013, anlässlich der NSA-Affäre, deren Aufdeckung wir dem Whistleblower Edward Snowden zu verdanken haben.*

2 *Siehe Datenschutz-Grundverordnung, Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, Vereinbarung der EU-Staaten zum Austausch von Fluggastdaten, …*

3 *Artikel 79 (3) GG*

4 *Artikel 19 (2) GG*

5 *BVerfG, U. v. 07.02.2008, BVerfGE 120, 274*

6 *BVerfG, U. v. 20.04.2016, BVerfGE 141, 220 (sog. BKAG-Urteil)*

Forderungen

Wir, zehn Organisationen aus der Netz-, Umwelt- und Entwicklungspolitik, haben mit der Konferenz *Bits & Bäume* eine gemeinsame Grundlage dafür geschaffen, wie die Digitalisierung so gestaltet werden kann, dass sie dem Gemeinwohl und Frieden dient, Datenschutz ernst nimmt und soziale und ökologische Ziele gleichermaßen fördert. Die fast 2.000 TeilnehmerInnen der Konferenz in Berlin, die Ergebnisse der Workshops und die zahlreichen Diskussionen auf und vor der Bühne zeigen: Die Zivilgesellschaft und eine kritische Wissenschaft haben gemeinsam die Wissensgrundlage, die Kompetenzen, die Weitsicht, den Willen und auch die Kraft, eine nachhaltige Digitalisierung mitzugestalten, wenn sie sich zusammenschließen.

Wir können die Digitalisierung nicht alleine der Wirtschaft und der Politik überlassen. Deshalb werden wir uns zukünftig noch stärker und gemeinsam in die gesellschaftliche Diskussion und die praktische Umsetzung einbringen.

Als Bündnis von Organisationen mit zehn verschiedenen Perspektiven auf die notwendigen Veränderungen stellen wir gemeinsam diese Forderungen:

Sozial-ökologische Zielsetzung bei Gestaltung der Digitalisierung

1. Die Gestaltung der Digitalisierung soll dem Gemeinwohl dienen. Sie darf nicht einseitig auf die Förderung einer wirtschafts- und wachstumspolitischen Agenda abzielen, sondern muss auf sozial-, umwelt-, entwicklungs- und friedenspolitische Ziele ausgerichtet sein. Die Digitalisierung soll zu einer nachhaltigen Energie-, Verkehrs-, Agrar- oder Ressourcenwende beitragen und konkrete Beiträge zur umfassenden Gewährleistung der Menschenrechte, der Klimaschutzziele und zur Beendigung von Hunger und Armut leisten. Eine nachhaltige Digitalisierung in unserem Sinne setzt auf sinnvolle, menschenwürdige Arbeit, soziale Gerechtigkeit und suffiziente Lebensstile.

Demokratie

2. Basis einer gerechten Gesellschaft sind demokratische Entscheidungen: Die Digitalisierung muss in sich demokratischer gestaltet werden und gleichzeitig demokratische Prozesse unterstützen, statt diesen entgegenzuwirken. Dafür muss sie konsequent darauf ausgerichtet werden, emanzipatorische Potenziale, dezentrale Teilhabe, offene Innovationen und zivilgesellschaftliches Engagement zu fördern.

Datenschutz und Kontrolle von Monopolen

3. Datenschutz, Manipulationsfreiheit und informationelle Selbstbestimmung sollen als Grundlage von freien, demokratischen, friedlichen und langfristig souveränen Gesellschaften national und global vorangetrieben werden.

4. Es müssen Rahmenbedingungen zur Kontrolle digitaler Monopole geschaffen werden, damit sich im Norden und globalen Süden eine eigene, selbstbestimmte digitale Wirtschaft entwickeln kann. Bestehende Monopole von BetreiberInnen kommerzieller Plattformen müssen gebrochen werden, indem beispielsweise eine definierte Schnittstelle zum Austausch zwischen Social-Media-Diensten verpflichtend eingeführt wird.

Bildung

5. Politische Regulierung muss darauf zielen, auch Informationen und Bildungsangebote zu Technik und Wirkungsweisen als einen Teil des öffentlichen Gemeinguts zu begreifen, sie müssen elementarer Bestandteil des öffentlichen Wissens sein. Ein kritischer und emanzipatorischer Umgang mit digitaler Technik soll Teil von digitaler Bildung sein, dazu gehört auch der kompetente Umgang mit Falschinformationen und Hassrede in digitalen Medien.

Entwicklungs- und Handelspolitische Aspekte

6. Länder des globalen Südens müssen die Möglichkeit haben, eine eigene auf die lokalen und nationalen Bedürfnisse ausgerichtete Digitalisierung zu entwickeln. Alle Gesellschaften sollen gleichen Anteil an Nutzen und Kosten der Digitalisierung haben können. Die negativen Seiten wie menschenunwürdige Arbeitsbedingungen, Umweltverschmutzung, Gesundheitsschäden und Elektroschrott dürfen nicht einseitig auf den globalen Süden abgewälzt werden.

7. Bilaterale und multilaterale Handelsabkommen dürfen keine Verbote und Einschränkungen in den Bereichen Besteuerung (Taxation), Offenlegung des Quellcodes (Open Source) und Ort der Datenverarbeitung (Localisation) enthalten.

8. Die Technologie-Branche muss verpflichtet werden, in Fragen der Ressourcenschonung und Nachhaltigkeit die Prinzipien menschenrechtlicher und ökologischer Sorgfaltspflichten in den Abbau- und Produktionsländern konsequent anzuwenden.

IT-Sicherheit

9. Mangelhafte Software hat negative Folgen für deren NutzerInnen, die Sicherheit ihrer Daten und die digitale Infrastruktur insgesamt. Es bedarf einer Softwarehaftung, damit Software-Hersteller die Verantwortung für die entstehenden Risiken (z. B. Sicherheitslücken) tragen, statt die Qualität ihrer Software dem Profit zu unterwerfen. IT-Sicherheit ist die Grundlage einer nachhaltigen digitalen Gesellschaft.

Langlebigkeit von Software und Hardware

10. Software muss selbstbestimmt nutzbar sein, reparierbar sein und langfristig instand gehalten werden können, so wie es Open-Source-Software bereits verwirklicht. Hersteller müssen daher beispielsweise Sicherheitsupdates für die Hardware-Lebensdauer von Geräten bereitstellen und nach Ende des Supports den Quellcode als Open-Source-Variante freigeben, statt *Software Locks* einzubauen.

11. Elektronische Geräte müssen reparierbar und recyclebar sein – geplante Obsoleszenz darf es nicht geben. Dafür müssen Garantiefristen massiv ausgeweitet werden; Hersteller müssen Ersatzteile, Reparaturwerkzeug und Know-How für alle anbieten und langfristig vorhalten. Dies soll unterstützt werden durch eine stärkere finanzielle Förderung offener Werkstätten bzw. Repair-Cafés und gemeinwohlorientierter Forschung und Produktentwicklung. Öffentliches Forschungsgeld darf es nur für Open-Source-Produkte geben.

Trägerkreis Bits & Bäume

Brot für die Welt, BUND – Friends of the Earth Germany, CCC – Chaos Computer Club, DNR – Deutscher Naturschutzring, FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, Germanwatch, IÖW – Institut für ökologische Wirtschaftsforschung, Konzeptwerk Neue Ökonomie, OKF – Open Knowledge Foundation Deutschland, Technische Universität Berlin

Dagmar Boedicker

Leerstelle in der legislativen Praxis

Plädoyer für eine Überwachungsgesamtrechnung

Über den Daumen gepeilt sind es 50 bis 80 Gesetze, die es den unterschiedlichsten Sicherheitsbehörden auf mehreren Ebenen gestatten, mich zu überwachen. Nicht nur mich, Sie natürlich auch. Schätzen Sie mal, was alles über Sie gespeichert wird, wenn Sie mit der Bahn von Bremen nach Frankfurt fahren, um dort in ein Flugzeug zu steigen, das Sie nach Rom bringt. Falls Sie aus der EU ausreisen und wieder heimkommen möchten, werden es noch ein paar Dateien und Sicherheitsbehörden mehr. Wie lange wird das eigentlich alles gespeichert? Wer bekommt da was von wem? Kontrolliert jemand, wann es gelöscht wird?

Vielleicht erwarten Leserinnen und Leser der *FIfF-Kommunikation* gar keine Antwort auf diese Fragen mehr. Ich glaube, das ist ein Fehler! Es ist das eine, realistisch zu sein, und es ist das andere hinzunehmen, dass unsere Grundrechte verfassungswidrig laufend verletzt werden. Menschenwürde setzt nämlich voraus, dass die staatliche Ordnung sich aus unserem Leben weitgehend heraushält, dass es Bereiche gibt, wo Sicherheitsinteressen weniger wichtig sind als unsere Würde.

Spuren einer Reise

Ich will versuchen, eine Geschäftsreise nach Rom zu beschreiben, die Sie jederzeit unternehmen könnten. Bei dieser Reise verhalten Sie sich ausnahmslos legal. Sie geben keinerlei Anlass für staatliche Eingriffe zur Gefahrenabwehr oder Strafverfolgung:

Die Bremer Straßenbahnen errechnen den für Sie günstigsten Tarif anhand der Route und stellen ihn auf Ihrer Monatskarte in Rechnung. Am Bahnhof übt die Bahn ihr Hausrecht aus und filmt Sie auf Ihrem Weg. Die Bahnfahrkarte haben Sie online gekauft, sie wird von Ihrem Konto abgebucht. Im Zug sitzen Sie an einem Vierertisch und in einer Funkzelle[1] mit einem dunkelhäutigen Herrn. Einem mutmaßlichen Gefährder, wovon Sie natürlich keine Ahnung haben. Während der Fahrt nutzen Sie WIFIonICE für Ihr Pad und einen anderen Telekommunikations-Anbieter für Ihr Smartphone, beide Anbieter speichern mindestens MAC- und IP-Adresse, wahrscheinlicher sind es 29 Verbindungsinformationen pro Verbindung. In Deutschland speichern Telekommunikations-Dienstleister u. a. sämtliche Verkehrsdaten für zehn Wochen. „Aus diesen Daten lassen sich genaue Schlüsse auf das Privatleben der Betroffenen, insbesondere deren Kontakt- und Interessenprofil ziehen."[2]

Lek, Lawrence (2017): Geomancer. Ausstellung Open Codes. The World as a Field of Data. 2018 im ZKM Karlsruhe

In Frankfurt werden Sie wieder am Bahnhof gefilmt. Mit dem Ticket haben Sie der Fluglinie allerhand Information geliefert, die diese teilweise gemäß Fluggastdatengesetz[3] für die PNR-Datei übermittelt[4]. Sie speichert aber noch weitere Daten, wozu sie gesetzlich gar nicht verpflichtet ist. Auch am Flughafen Frankfurt werden Sie gefilmt. In der Confiserie kreuzt sich Ihr Weg mit dem einer gerade angekommenen polnischen Staatsbürgerin, Sie stehen beide an derselben Kasse und wechseln einige Worte. Vor dem Geschäft verabschieden Sie sich höflich. Was Sie natürlich nicht wissen können: Die junge Frau hat sich polnischem Recht entzogen, denn sie hat abgetrieben und darauf stehen in Polen drei Jahre Haft.[5] Am Flughafen in Rom werden Sie gefilmt, in der Autovermietung ebenfalls, die Bilder werden aufgezeichnet. Ihr Hotel in Rom hat Ihre Reservierungsdaten an die zentrale Datenbank der Kette geliefert, zu der es gehört. Leider sind die bei einem Hack in falsche Hände geraten.[6] Der WLAN-Anbieter im Hotel speichert natürlich Ihre MAC-Adresse, was sonst noch gespeichert wird, entnehmen Sie bitte den AGBs. Als Sie am nächsten Tag mit Ihrem Mietwagen nach Bologna fahren, passieren Sie auf der Autobahn mehrere Mautstellen, Video-überwacht. Sie treffen sich mit einer Geschäftspartnerin aus Island in einem Restaurant und geraten bei der Rückfahrt auf einer Landstraße in eine Verkehrskontrolle. Die Polizei registriert die Daten von Ihnen und Ihrer Begleiterin. Mit nationalem italienischen Recht kenne ich mich nicht aus, aber EU-Recht gilt auch dort. Und im Schengen-Informations-System SIS sind jedenfalls jetzt alle Ihre Grenzübertritte und die Daten der Verkehrskontrolle vermerkt. Dabei haben Sie noch Glück. Wären Sie keine EU-Bürgerin, stünden Ihnen die Segnungen des Etias bevor:

> *„Das Reiseinformations- und -genehmigungssystem Etias dient der Vorkontrolle visafreier Besucher. Betroffene müssen laut Beschluss des EU-Rats über einen Online-Antrag den Behörden Auskünfte zu Identität, Reisedokument, Aufenthaltsort, Kontaktmöglichkeiten, infektiösen Krankheiten und Ausbildung übermitteln. Die Daten werden dann automatisch mit verschiedenen IT-Systemen im Sicherheitsbereich abgeglichen und fünf Jahre auf Vorrat gespeichert.“*[7]

Die Rückreise muss ich wohl nicht mehr beschreiben. Aber ich möchte einige Sicherheitsbehörden aufzählen, die gesetzlich befugt sind, im Verdachtsfall auf die gespeicherten Daten zuzugreifen: Polizei, Landeskriminalamt und Verfassungsschutz in Bremen, Niedersachsen und Hessen, Bundespolizei, Bundeskriminalamt, Zoll, Bundesamt für Verfassungsschutz, Bundes-Netzagentur, Bundesnachrichtendienst (obwohl der eigentlich nur außerhalb Deutschlands ermitteln dürfte), MAD. Zu den italienischen Sicherheitsbehörden kann ich nichts sagen, aber für Deutschland allein sind es 16 während dieser kurzen Reise. Bei jedem Bundesland, das Sie betreten, kommen drei hinzu. Europol ist dabei und von den ausländischen Nachrichtendiensten wie CIA, FSB, MIT, NSA schreibe ich hier nichts, weil es mir um etwas anderes geht.

Die Befugnisse der Sicherheitsbehörden beschränken sich nicht darauf, anderswo gespeicherte Daten abzufragen. Sie dürfen selbst Daten erheben, auch mit *besonderen Mitteln.* Besondere Mittel der Datenerhebung sind beispielsweise längerfristige Observation, der verdeckte Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen oder -aufzeichnungen, zur Feststellung des Standortes oder der Bewegungen einer Person oder zum Abhören oder zur Aufzeichnung des nichtöffentlich gesprochenen Wortes, verdeckte Ermittler, automatisierte Kennzeichenerkennungssysteme. Diverse Datenerhebungen dürfen durchgeführt werden, selbst wenn Dritte unvermeidbar betroffen werden, beispielsweise Bild- und Tonaufzeichnungen von Drohnen aus.[8]

Telekommunikations-Dienstleister müssen in Deutschland Verkehrsdaten 10 Wochen speichern. Auch darauf dürfen die Behörden zugreifen. Dritte sind betroffen. Wenn die neue Beweismittel-Übergabe-Verordnung (E-Evidence-Verordnung[9]) Wirklichkeit wird, müssen die TK-Anbieter alles herausrücken, was sie über bestimmte Kunden wissen, wenn die Strafverfolgungs-Institutionen eines EU-Mitglieds das fordern. Im Regelfall haben die Anbieter dafür zehn Tage Zeit, in Eilfällen nur sechs Stunden.

> *„Werden Daten herausgegeben, erlangen die zuständigen Justizbehörden hiervon jedoch keine Kenntnis. Der Vorschlag sieht keine Informationspflicht gegenüber den Behörden am Sitz des Unternehmens vor.“*[10]

Die deutsche Konferenz der Datenschutzaufsichtsbehörden fordert, den Vorschlag für eine E-Evidence-Verordnung zu stoppen, und ist sich dabei mit dem Europäischen Datenschutzausschuss (früher Artikel-29-Gruppe) einig, der nicht einmal eine Rechtsgrundlage für die Verordnung sieht.[11]

Unsichtbare Mauern

Europäische Reisefreiheit fühlt sich frei an, keineswegs wie ein Bentham‘sches Panoptikum, in dem Wächter uns beobachten, die wir nicht sehen können. Anders als die Insassen des Panoptikums stoßen wir nie an Mauern, jedenfalls dann nicht, wenn wir westeuropäisch aussehen, uns unauffällig verhalten und keinen Anlass zu Kontrollen geben. Trotzdem werden wir auf Schritt und Tritt überwacht und haben keine Ahnung, wann die virtuellen zu konkreten Mauern versteinern könnten.

> *„Es steht zu befürchten, dass die weltweite Zunahme der Mauern einen neuen Mauermenschen erzeugt: Dieser Mensch begrüßt die neuen Mauern als Wellenbrecher, mit denen die Stürme der Globalisierung, die Migrationswellen, islamistische Terroristen und kriminelle Banden gestoppt werden. […] Mauern verwandeln Furcht in Zutrauen, Unsicherheit in Sicherheit, Orientierungslosigkeit in Orientierung, Identitätsnot in Identitätsgewissheit. […] Schließlich produzieren die neuen Mauern nicht nur ein Außen, sondern eben auch ein Innen, sie formen das Bild der Ausgesperrten ebenso wie das Selbstbild der Eingesperrten. Sind wir schon eingesperrt?“* [12]

Verdeckte Maßnahmen, bei denen harmlose Menschen wie Sie und ich gern zum *Beifang* werden, haben einen besonderen Pferdefuß. Wir wissen nicht, dass unsere Daten erhoben und gespeichert wurden, dass wir zu den *Dritten* gehören, bei denen das *aus technischen Gründen unvermeidbar ist.* Damit kommen wir gar nicht auf die Idee, Auskunftsrechte in Anspruch zu nehmen,

Löschfristen einzufordern, ganz allgemein den Datenschutzkonformen Umgang mit unseren personenbezogenen Daten zu kontrollieren. Fast alle Gesetze, die zu verdeckter Überwachung ermächtigen, verpflichten die Sicherheitsbehörden deshalb dazu, die Betroffenen zu benachrichtigen. Bisher habe ich allerdings noch niemanden getroffen, die oder der jemals eine solche Benachrichtigung erhalten hätte. Sie vielleicht? Angesichts des Rundum-sorglos-Pakets an polizeilichen und nachrichtendienstlichen Befugnissen stimmt da etwas nicht.

Rechtsstaat?

Die Befugnisse der Polizeien wurden seit dem 11. September 2001 kontinuierlich ausgebaut, beginnend mit dem Sicherheits-Paket des damaligen Innenministers Otto Schily, spöttisch als *Otto-Katalog* bezeichnet. Dasselbe gilt für die Nachrichtendienste. Regierungen und Parlamente haben Polizeigesetze, Gesetze für die Verfassungsschutz-Ämter, den Zoll usw. gewaltig erweitert und in ganz Deutschland eine Überwachungs-Infrastruktur auf- und ausgebaut, die uns Menschen das Vornehmste verweigert: unsere Würde. Das Gefühl des Überwachtwerdens wächst stetig.

Häufig hat das BVerfG an Polizei- und anderen Gesetzen fehlende Normenklarheit bemängelt. In einem Rechtsstaat sollte es selbstverständlich sein, dass die Staatsdiener ihre Grenzen sehr genau kennen und einhalten. Für die Betroffenen ist es wichtig zu wissen, was sie dürfen und was ihre Obrigkeit darf. Ich bezweifele stark, dass wir oder die Sicherheitsbehörden darüber tatsächlich Bescheid wissen. Niemand, weder Sicherheitsbehörden noch Betroffene, kann sich mehr auskennen, wenn Gesetze zur Definition von Gefahren von einem Gesetz auf ein zweites und von dort auf ein drittes verweisen[13]. Wenn dazu mangelhafte Zweckbindung der personenbezogenen Daten bei ausgedehnten Eingriffsvoraussetzungen kommt, tappen wir im Dunkeln: Darf uns die Polizei bei einer Demonstration fotografieren oder filmen? Was darf sie mit den Bildern und Videos tun? Bleiben wir bei Protesten gegen die *Münchner Sicherheitskonferenz* besser weg? Filmt mich die Drohne? Mit oder ohne Ton? Wann haben Sicherheitsbehörden meinen Standort bei welcher Gelegenheit mit einer Funkzellenabfrage ermittelt? Sind die Verkehrsdaten gespeichert? Wo und wie lange? Haben sie mich bei einer präventiven Rasterfahndung mit im Netz gehabt? Wohin wurde die Information übermittelt? Sollten wir Auskunft verlangen? Bekommen wir die, oder machen wir uns nur erst recht verdächtig? Wurde unser Kennzeichen an einer innereuropäischen Grenze oder auf einer deutschen Autobahn automatisch erkannt? Gespeichert? Genutzt für was? Datenbanken gibt es in jedem Bundesland, jedem europäischen Mitgliedstaat, in Drittstaaten, in denen wir die Speicherung unserer personenbezogenen Daten befürchten müssen.[14]

Bei der Quellen-TKÜ oder Online-Durchsuchung werden massenhaft höchst persönliche Daten ausgeleitet. Gehören wir zu den unbeteiligten Dritten und wurden wir jemals darüber informiert? Haben die verdeckten Maßnahmen jemals zu einem Ergebnis geführt? Hat eine Sicherheitsbehörde eine Gefahr damit abgewehrt oder eine Person einer schweren Straftat überführt? Diesen Nachweis bleiben uns Exekutive und Legislative bisher schuldig. Außerdem zeigt sich, dass Beschäftigte des BKA eine eigenwillige Definition davon haben können, was zum Kernbereich privater Lebensgestaltung gehört, oder nach ihrer Auffassung eben nicht.[15]

Spätestens 2010 hätte etwas geschehen müssen. Es hatte mehrere Verfassungsbeschwerden gegen die Vorratsdatenspeicherung gegeben und in ihrer Entscheidung aus dem Jahr 2010 haben die Richterinnen und Richter dem Gesetzgeber eine Überwachungsgesamtrechnung[16] auferlegt. Sie haben klargestellt, dass neue Überwachungsmaßnahmen und Eingriffe in das Grundrecht auf informationelle Selbstbestimmung immer im Kontext bereits bestehender Instrumente geprüft werden müssen. Im Dezember 2016 hat es auch der Europäische Gerichtshof (EuGH) auf Grundlage der europäischen Grundrechte-Charta untersagt, Telekommunikationsanbieter ganz allgemein zur Speicherung persönlicher Nutzerdaten zu verpflichten.[17] Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) schützt geschäftliche wie private Kommunikation und der Europäische Gerichtshof für Menschenrechte (EGMR) verlangt Mindestsicherungen bei der Informationssammlung und -speicherung durch einen Geheimdienst.[18] Wenn nämlich „Daten aus Kommunikationsverläufen behördlich aufgezeichnet und verwertet werden", entsteht

> *„ein Klima, in dem die Menschen sich bei der Äußerung der eigenen Meinung ebenso wie beim Konsum von Informationen zur Bildung einer eigenen Meinung selbst bei völlig legalen Inhalten immer häufiger selbst beschränken, um mögliche nachteilige Folgen zu vermeiden. Diese Selbstbeschränkung bei der Ausübung der durch Artikel 10 EMRK garantierten Meinungs- und Informationsfreiheit wird auch als „chilling effect" bezeichnet."*[19]

Unsere Forderungen

Mit dem BVerfG sind wir überzeugt, dass „die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf“[20]. 2006 hat es in seinem Urteil zur Rasterfahndung[21] eine Abwägung verlangt zwischen der Eingriffsschwere, den verfolgten Schutzzielen und der gesellschaftlichen Relevanz dieser Maßnahme wegen ihrer Streubreite und der möglichen Einschüchterung ganzer Bevölkerungsgruppen. Wenn die Instrumente zur Kontrolle vorhanden sind, können sie gegen uns verwendet werden, das haben Gestapo, SD und Stasi gezeigt.

- Deshalb fordern wir eine Überwachungsgesamtrechnung: Wir fordern den Nachweis des Gesetzgebers, dass weitere Überwachungsbefugnisse erforderlich sind, und dass sie dem Verfassungsgerichts-Urteil entsprechen! Der Nachweis kann durch unabhängige Forschungseinrichtungen oder die zuständigen Datenschutzbeauftragten erbracht werden, die mit den dafür erforderlichen Ressourcen auszustatten sind.

- Wir fordern, dass Überwachungsmaßnahmen gestrichen werden, wenn sich ihre Notwendigkeit und Verhältnismäßigkeit nicht belegen lässt!

- Wir fordern eine Evaluierung der großen staatlichen Datensammlungen, ob sie durch anlassbezogenere Datenverarbeitung ersetzt werden müssen!

- Wir fordern eine unabhängige Instanz, die prüft, ob die Sicherheitsbehörden bei ihren Überwachungsmaßnahmen verhältnismäßig und damit verfassungsgemäß vorgehen!

- Wir fordern den Nachweis der Sicherheitsbehörden, dass sie alle Betroffenen tatsächlich über alle Überwachungsmaßnahmen aufgeklärt haben! Der Nachweis kann durch die zuständigen Datenschutzbeauftragten erbracht werden, die mit den dafür erforderlichen Ressourcen auszustatten sind.

Diese Forderungen richten wir an die Gesetzgeber auf Landes-, Bundes- und europäischer Ebene. Es ist ihre verfassungsrechtliche Pflicht sie zu erfüllen!

Anmerkungen

1 *https://media.ccc.de/v/35c3-9972-funkzellenabfrage_die_alltagliche_rasterfahndung_unserer_handydaten (Stand Januar 2019)*

2 *Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – Münster, 7. November 2018 zur E-Evidence-Verordnung, S. 2*

3 *Gesetz zur Umsetzung der Richtlinie (EU) 2016/681*

4 *Die Daten (Anschlussflüge, Flugscheindaten, Zahlungsinformationen, Vielfliegereinträge, Gepäckangaben, Informationen über Mitreisende etc.) aus den nationalen PNR-Dateien werden im Advance Passenger Information System (APIS) zusammengeführt. „Der Europäische Datenschutzbeauftragte geht von mehr als 300 Millionen betroffenen nicht-verdächtigen Fluggästen aus, die von der PNR-RL betroffen sind, European Data Protection Supervisor, Opinion 15/2015, 7.“ Tschohl, Christoph et al: HEAT – Handbuch zur Evaluation der Anti-Terror-Gesetze, Version 1.2. S. 94. https://epicenter.works/document/706 (Stand Oktober 2018)*

5 *Nach der Europäischen Herausgabeverordnung (E-Evidence, siehe Endnote 9) kann Polen die über diese Dame gespeicherten Daten von italienischen Dienstleistungs-Anbietern fordern, unabhängig davon, ob eine Abtreibung in Italien strafbar ist. Kriterium ist die Freiheitsstrafe von drei Jahren.*

6 *Die Marriot-Kette musste zugeben, dass ihr im November 2018 ca. 500 Millionen Kundendaten inkl. Geburtsdatum, Kreditkartennummer usw. gestohlen wurden. Die Täter hatten sich Zugang zur Reservierungsdatenbank der Marriot-Tochterfirma Starwood verschafft und offenbar schon seit 2014 Zugriff auf das System. http://www.lirobit.de/sicherheitsvorfaelle-hackerangriffe-chronologischer-ueberblick/ (Stand 28. Januar 2019)*

7 *Krempl S (2018) Big Brother Europa. EU plant biometrische Superdatenbank. https://www.heise.de/select/ct/2018/18/1535696151919730; Krempl S (2018) ESTA für Europa: EU-Vorkontrolle visafreier Reisender soll 2021 starten. https://www.heise.de/newsticker/meldung/ESTA-fuer-Europa-EU-Vorkontrolle-visafreier-Reisender-soll-2021-starten-4156695.html (Stand 28. Januarv2019)*

8 *Die hier genannten Befugnisse stammen aus dem Bayerischen Polizeiaufgaben-Gesetz, Art. 33 und 47, sie finden sich auch in anderen Polizeigesetzen.*

9 *Die Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM (2018) 225 final) sieht vor, dass die Strafverfolgungsbehörden der EU-Mitgliedstaaten die Befugnis erhalten, Anbieter von Telekommunikations- und Internetdienstleistungen in anderen Mitgliedstaaten der EU und auch in Staaten außerhalb der EU (Drittstaaten) unmittelbar zur Herausgabe von Bestands-, Zugangs-, Transaktions- und Inhaltsdaten zu verpflichten. Das Recht des Staates, in dem die Daten gespeichert sind, soll von den Anbietern der Dienstleistungen grob geprüft werden, nicht etwa von staatlichen Rechtsinstanzen. Die Verordnung kann nur noch im Trilog gestoppt werden.*

10 *Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – Münster, 7. November 2018*

11 *Europäischer Datenschutzausschuss: Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters. https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-commission-proposals-european-production-and_de (Stand 30.1.19)*

12 *Körner T (2019) Von Mauern und Menschen. Deutschlandfunk, 13. Januar 2019, 9.30 Uhr*

13 *Unterrichtung durch die Bundesregierung. Evaluationsbericht zu den §§ 4a, 20j, 20k des Bundeskriminalamtgesetzes. https://dip21.bundestag.de/dip21/btd/18/130/1813031.pdf, S. 33 (Stand 28. Januar 2019)*

14 *Seit 2006 gibt es beispielsweise das Gemeinsame-Dateien-Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder.*

15 *Unterrichtung durch die Bundesregierung. Evaluationsbericht zu den §§ 4a, 20j, 20k des Bundeskriminalamtgesetzes. dip21.bundestag.de/dip21/btd/18/130/1813031.pdf, S. 45 (Stand 28. Januar 2019)*

16 *Rossnagel A (2010) in: Neue Juristische Wochenschrift 18/2010, Seite 1238*

17 *Rechtssachen C-203/15 und C-698/15*

18 *Tschohl C et al (2018) HEAT – Handbuch zur Evaluation der Anti-Terror-Gesetze, Version 1.2. S. 134f. https://epicenter.works/document/706. (Stand Oktober 2018)*

19 *Tschohl C et al (2018) a.a.O. S. 136*

20 *BVerfG, Urteil vom 2.3.2010, NJW 81 (2010), 833, 839*

21 *BVerfG, B. v. 04.04.2006, 1 BvR 518/02*

Editorial zum Schwerpunkt

Viele Produkte, Entwicklungen und Einsatzfelder der Informatik scheinen sich unausweichlich und technisch notwendig so entwickelt zu haben, wie wir sie heute kennen. Seien es die Mechanismen sozialer Netzwerke, der aktuelle Ansatz Künstlicher Intelligenz, das Vorhandensein globaler IT-Monopole, zentralisierte Smart-City-Konzepte oder der wenig regulierte Adress- und Datenhandel. Technische Entwicklungen bauen aufeinander auf, aber finden natürlich nicht im luftleeren Raum statt. Es gibt immer verschiedene Wege, ein Problem anzugehen und entsprechend Ressourcen für dessen Lösung aufzuwenden.

Oftmals liegen den tatsächlichen Entwicklungen gerade keine primär technischen Überlegungen zu Grunde, sondern ökonomische oder politische Motive. Folglich ist es erhellend, Informatik- und Technikgeschichte auch unter diesen Aspekten zu betreiben. So können Entscheidungsalternativen oder Weggabelungen herausgestellt werden, um die dahinterliegenden Machtinteressen, aber auch die sachlichen wie sozialen Dynamiken und Zwänge freizulegen. Dieses Wissen ermöglicht es dann, heutige technische Entwicklungen und Weichenstellungen besser zu verstehen.

Doch wir wollen auch aktiv an aktuellen und zukünftigen tiefgreifenden Veränderungen mitwirken, denn die Informatik ist immer auch Gestaltungsdisziplin – weit über die reine Technik hinaus. Wir wollen also mithelfen, die stetige Digitalisierung und Vernetzung der Gesellschaft so mitzuprägen, dass die Freiheit des Individuums und das Wohl der Gesellschaft im Vordergrund jeglicher Technikentwicklung und ihres Einsatzes stehen – sowohl in unseren Endgeräten und Anwendungen als auch in unserer digitalen Infrastruktur.

Wir wollen Sichtweisen und konkrete Wege erarbeiten, auf welche Weise nicht-technische Werte wie demokratische Teilhabe, Freiheit und Selbstbestimmung, Pluralismus von Lebensentwürfen und Nachvollziehbarkeit von Entscheidungen genauso in technischen Systemen und den politischen Entscheidungen darüber Eingang finden, wie die Verhinderung verdeckter Machtzentren, die Bekämpfung von Diskriminierung und struktureller Benachteiligung, Privatisierung staatlicher Kernaufgaben. Wir wollen keine smarten Privatstädte mit herrlichem Kundenerlebnis, sondern lebendig-diverse Städte mit emanzipierten BürgerInnen. Wir wollen keine zentralisierten Infrastrukturen, die von globalen, intransparenten Konzernen betrieben werden, sondern dezentralisierte und selbstverwaltete Systeme. Wir wollen unsere Kommunikationsmittel nicht von Geheimdiensten und Militär durchdrungen wissen, sondern integre und vertrauliche Systeme mit Respekt sowie Vertrauen in Menschen und ihre Grundrechte. Wir wollen diese Werte konkret realisiert sehen.

Die Informatik erlaubt all dies in ihren Systemen. Wir müssen die Freiheitsgrade der Technik ausnutzen, aber vor allem müssen wir den politischen Willen dafür aufbringen. Wir wollen tatsächlich mutig sein und mit den Vorträgen dieser Konferenz dazu beitragen, eine neue, bessere Welt für alle Menschen zu erdenken um sie dann zu bauen.

Dieser Schwerpunkt der *FIfF-Kommunikation* enthält Beiträge zu der Konferenz. Neben zwei auf den Vorträgen fußenden Autorenbeiträgen – ein Beitrag von Daniel Guagnin und Jörg Pohle und ein Beitrag von Werner Rammert – haben wir die Beiträge transkribiert bzw. zusammengefasst; der erste Teil davon ist auf den folgenden Seiten zu finden. Ganz herzlichen Dank an alle Helferinnen und Helfer, die die Beiträge zusammengestellt haben und ohne die diese Ausgabe in der vorliegenden Form nicht möglich gewesen wäre. Die Transkripte und Zusammenfassungen wurden mit größter Sorgfalt erstellt und aus Zeitgründen i. d. R. nicht autorisiert – alle verbliebenen Fehler gehen damit zu Lasten der Redaktion.

Wegen des Umfangs des Materials teilen wir diesen Schwerpunkt auf zwei Hefte auf – Beiträge, die in dieser Ausgabe keinen Platz mehr gefunden haben, werden in der Folgeausgabe 2/2019 erscheinen, genauso wie die Beiträge der Preisträger des Weizenbaum-Studienpreises.

Die Welt ist nicht vom Himmel gefallen – sie wird gemacht, von sozialen Akteuren mit Interessen und gerade auch mit Hilfe von Informatiksystemen. Der Originalbeitrag *Welt → Modell → Technik → Welt'* von *Daniel Guagnin* und *Jörg Pohle* gibt einen knappen Überblick über ein in einer soziologisch-informatischen Kooperation entwickeltes Framework für die Analyse und Gestaltung von Informatiksystemen, das die zugrunde gelegten und eingeschriebenen Annahmen, Reduktionen und Setzungen aufdecken und hinterfragen hilft. Technik ist gestaltbar und muss gestaltet werden – gestalten wir sie!

Doch wer oder was gestaltet eigentlich auf welche Weise die Produkte der Informatik? Wie verteilen sich die Machtkonstellationen von der Entwicklung über die Einrichtung bis hin zur massenhaften Nutzung jeweils neu? Sind es die Visionäre und Pioniere der Informatik? Oder die Entrepreneure disruptiver Innovation? Oder die politischen Regulierer demokratisch legitimierter Repräsentanten oder autokratischer Regime? Oder die

Masse der User und ihre alltäglichen Praktiken? Diese *großen Fragen* stellt *Werner Rammert* in seinem Beitrag *Konstellationen neu verteilter Gestaltungsmacht – Lehren für die Informatik?* Diese werden anhand kleiner Fallstudien zur Konstruktion von Expertensystemen, zur Sozionik verteilter Agenten und zum Profiling in Überwachungssituationen exemplarisch geklärt.

Besser steuern durch mehr Daten? Das fragen *Anne K. Krüger*, *Judith Hartstein* und *Felicitas Hesselmann*. Während die Einen von der Lösung gravierender Menschheitsprobleme träumen, warnen Andere vor einer allumfassenden Überwachung durch die neuen Möglichkeiten soziotechnischer Systeme. Doch steht sowohl hinter der Utopie des Solutionismus als auch hinter der Dystopie totaler Überwachung die Frage, warum, wofür und wie die dazu notwendigen Daten überhaupt produziert und genutzt werden. Lassen sich durch viele neue Daten jetzt ganz viele alte Probleme lösen? Oder werden wir alle von den Daten gegen unseren Willen fremdbestimmt? Der Beitrag geht aus einer soziologischen Perspektive heraus den Problemen der neuen Möglichkeiten von Datenproduktion und -nutzung nach und fragt, was passiert, wenn wir soziale Wirklichkeit nur noch durch die Daten sehen, die durch soziotechnische Systeme produziert werden.

Über *Empire and Power: The Forgotten History of the Internet as a Weapon* sprach *Yasha Levine*. Die Umgestaltung des Internet in eine Waffe ist heute ein wichtiges Thema. Berichte darüber dominieren die Nachrichten. Viele denken, das sei neu: Das Internet, früher eine demokratische und egalitäre Kraft, wurde durch dunkle Kräfte „gehackt". Doch das Internet war immer schon eine Waffe, seit seiner Entstehung im Pentagon als ARPANET. Der Beitrag betrachtet diese vergessene Geschichte des Internet, besonders die Episoden, die verloren, vergessen oder kulturell unterdrückt wurden – von den Einflüssen auf Datennetze aus der Zeit der Aufstandsbekämpfung im Vietnamkrieg bis hin zur frühen Opposition gegen das ARPANET als Mittel militärischer Kontrolle, zu Google und dem Silicon Valley, zu Werkzeugen für Privatheit und die Freiheit des Internet wie Tor.

Der Vortrag von *Christian Grothoff* behandelte *Netzwerkdienste für sozial-liberale Gesellschaften*. Welche politischen Anforderungen könnten wir an neue Netzwerktechnik stellen? Die politischen Anforderungskataloge für das *GNU Name System* und *GNU Taler* werden kurz vorgestellt. Danach wird gezeigt, wie diese Anforderungen technisch umgesetzt wurden.

Der folgende Beitrag kommt von *Volker Grassmuck*: *Völkerverständigung ist Volksmacht plus Vernetzung der ganzen Welt.* Das Versprechen jeder Kommunikationsverbindung ist, dass die Angeschlossenen durch ihren Austausch zu einem gemeinsamen Verständnis kommen. Heute ist die Welt global vernetzt wie nie. Doch statt Horizonterweiterung und Neugier auf Vielfalt erleben wir Xenophobie, Grenzschließungen und eine Internationale der Nationalisten. Die Koevolution von technischen, psychischen und sozialen Systemen läuft selten wie geplant. Wie kann da die Informatik ihrer Selbstverpflichtung nachkommen, Handlungsalternativen im Hinblick auf die absehbaren Wirkungen und möglichen Folgen ihrer Systeme aufzuzeigen?

Über *Gemeinwohl, Demokratie und gute Arbeit in der digitalen Gesellschaft – Von Macht und Mitgestaltung* sprach anschließend *Annette Mühlberg*. Manche Menschen kaufen sich ganze Städte oder Teile davon, doch der damit verbundenen Gestaltungsmacht ist bislang wenig entgegengesetzt worden. Es geht dabei um Macht und Kontrolle von Verkehr, Kommunikation, Energie und Arbeit kompletter urbaner Räume. Technische Zentralisierung unterminiert etwa die rechtlich und politisch gebotene Gewaltenteilung und die Mitbestimmung von lokalen Behörden. Wir müssen neue Regularien finden, insbesondere auch für die Arbeitswelt mit ihren sehr bestimmenden Machtasymmetrien. Dies drückt sich u. a. auch ganz konkret in demokratisch auszuhandelnden Anforderungen an die dort verwendeten IT-Systeme aus. Fachleute aus Informatik, Recht oder Politik müssen dafür ebenfalls einbezogen werden.

The revolution will not be optimized? Seda Gürses behandelte in ihrem Vortrag *Protective Optimization Technologies* (POT). In den 1990er Jahren entwickelte sich die Softwaretechnik von Softwarepaketen und PCs hin zu Services und Clouds, die verteilte Architekturen mit Echtzeit-Feedback von den AnwenderInnen möglich machen. Digitale Systeme wurden dabei zu Technologieschichten hinter objektiven Funktionen. Diese Funktionen steuern unter anderem die Auswahl von Softwarefunktionen, Service-Integration, Cloud-Nutzung, Benutzerinteraktion und -wachstum, Kundenservice und Erfassung von Umgebungsbedingungen. Während sich Informationssysteme auf die Speicherung, Verarbeitung und den Transport von Informationen sowie das Organisieren von Wissen – mit damit verbundenen Überwachungsrisiken – konzentrierten, nutzen heutige Systeme das gesammelte Wissen, um die Welt nicht nur zu verstehen, sondern auch zu optimieren und den maximalen wirtschaftlichen Nutzen durch die Erfassung und Manipulation von Aktivitäten und Umgebungen der Menschen zu erzielen. Die Fähigkeit dieser Optimierungssysteme, die Welt nicht als statischen Ort zu behandeln, sondern als Ort der Wahrnehmung und gemeinsamen Gestaltung, birgt soziale Risiken wie Social Sorting, Massenmanipulation, ungleiche Verteilung von Ressourcen, Dominanz von Mehrheiten, und Auslöschung von Minderheiten. Im Rahmen der Optimierung entstehen diese Schäden durch die Wahl unzulänglicher Zielfunktionen. Seda Gürses legte dar, was sie unter Optimierungssystemen versteht, beschrieb deren externe Effekte und unterbreitete Vorschläge für Protective Optimization Technologies.

Ein *Update des Staatstrojaners* gibt *Constanze Kurz*. Seit dem ersten höchstrichterlichen Urteil zum Staatstrojaner im Jahr 2008 konnte keine Bundesregierung und kein Innenminister von dem Versuch lassen, das staatliche Hacking in das Arsenal der Ermittlungswerkzeuge aufzunehmen. Inzwischen wurde der Staatstrojaner als normales Ermittlungsinstrument für Dutzende Straftaten erlaubt. Die technisch ziemlich komplexe Aufgabe, einen Staatstrojaner zur Anwendung zu bringen, bereitet den Behörden bis heute Probleme. Und viele ungelöste Fragen bestehen vor und beim Einsatz der Schadsoftware noch immer. Der Vortrag gibt einen Überblick über den Stand der Dinge bei deutschen Staatstrojanern und spart natürlich auch nicht mit Forderungen, was zu tun wäre.

Der *FIfF-Jahresrückblick – eine freudige Panoramafahrt durch das FIfF-Jahr von Benjamin Kees, Rainer Rehak und Stefan Hügel* bildet den (vorläufigen) Abschluss des Schwerpunkts in dieser Ausgabe.

Daniel Guagnin, Jörg Pohle

Welt → Modell → Technik → Welt'

Grundrisse eines Frameworks zur Analyse und Kritik der Modellifizierung und Einschreibung von Machtmustern in soziotechnische Systeme

Die Welt ist nicht vom Himmel gefallen – sie wird gemacht, von sozialen Akteuren mit Interessen und gerade auch mit Hilfe von Informatiksystemen. Der vorliegende Beitrag gibt einen knappen Überblick über ein in einer soziologisch-informatischen Kooperation entwickeltes Framework für die Analyse und Gestaltung von Informatiksystemen, die die zugrunde gelegten und eingeschriebenen Annahmen, Reduktionen und Setzungen aufdecken und hinterfragen hilft. Technik ist gestaltbar und muss gestaltet werden – gestalten wir sie!

Einleitung

Ansätze zur Beschreibung, Analyse und Gestaltung soziotechnischer Systeme – und dabei vor allem Informatiksysteme oder solche, die von Informatiksystemen mit gesteuert werden – sind seit Jahrzehnten Gegenstand der Forschung, gerade auch im FIfF und seinem Umfeld. Ein solches Framework soll mithin nicht nur dazu dienen, in sozio-technische Systeme eingeschriebene Machtmuster zu erkennen, sondern sie auch analysieren und an ihnen Kritik üben, intervenieren und damit die Richtung, in die sie entwickelt werden, ändern zu können. Das Ziel der Systemgestaltung muss, wie Heinz von Foerster (2002: 303) es ausdrückte, sein, neue Freiheiten zu schaffen – und nicht bestehende zu beschneiden oder gar aufzuheben.

Die derzeitige Debatte in und außerhalb der Wissenschaft ist jedoch häufig oberflächlich, wenig differenziert und zugleich alarmistisch. Sie setzt sehr stark auf Fremdbeschreibungen – Beschreibungen über Informatik und über Informatiksysteme, die wenig beeinflusst sind vom Kenntnisstand in der Informatik, insbesondere von den seit Jahrzehnten geführten Debatten im Bereich Informatik und Gesellschaft. Im Gegensatz dazu soll das Framework, das hier vorgestellt wird, explizit auf den Erkenntnissen dieser Vorarbeiten aufbauen, sie weiterentwickeln und dabei die Unterscheidungskraft schärfen, um genauer in den Blick nehmen zu können, an welchen Stellen und in welcher Form wie Technik gestaltet wird, wie dort Machtmuster eingeschrieben werden und – zumindest langfristig auch – wie GestalterInnen intervenieren können.

Das Meta-Modell

Am Anfang steht ein Meta-Modell, das sowohl Aufschluss über die zugrunde gelegte erkenntnistheoretische Grundposition gibt, als auch als analytisches Raster für die Analyse soziotechnischer Systeme dient. Zugleich lässt sich anhand des Meta-Modells das Vorgehen in der Analyse verfolgen (siehe Abbildung 1).

Ausgangspunkt ist die Annahme, dass es eine Welt gibt, in der Entwicklung und Einsatz solcher Systeme stattfindet. Diese Welt wird abgebildet, ob deskriptiv oder konstruktionistisch, in Modelle, auf deren Basis dann Probleme identifiziert und analysiert werden – nicht einfach als wahre, gar objektive, sondern immer als von den modellierenden AkteurInnen gemachte Probleme (vgl. Floyd 1989: 11ff). Anschließend werden Lösungen vorgeschlagen – Lösungen, die selbst immer abhängig sind von den Weltmodellen und Problemsetzungen sowie den diesen zugrunde liegenden Annahmen und Zuschreibungen. Diese Lösungen werden dann – mehr oder weniger direkt – in Technik umgesetzt. Und zuletzt wirkt die derart gestaltete Technik wieder zurück auf die Welt – die dann und damit aber nicht mehr Welt ist, sondern Welt'.

Das Meta-Modell erlaubt es, genauer auszuführen, wie und an welchen Stellen das geschieht, und dabei zusätzliche und für die interdisziplinäre Debatte produktivere Unterscheidungskriterien einzuführen, die es zugleich ermöglichen, neben einer Analyse auch Anknüpfungspunkte für Interventionen zu liefern, insbesondere für eine reflektierte Gestaltung von Informatiksyste-

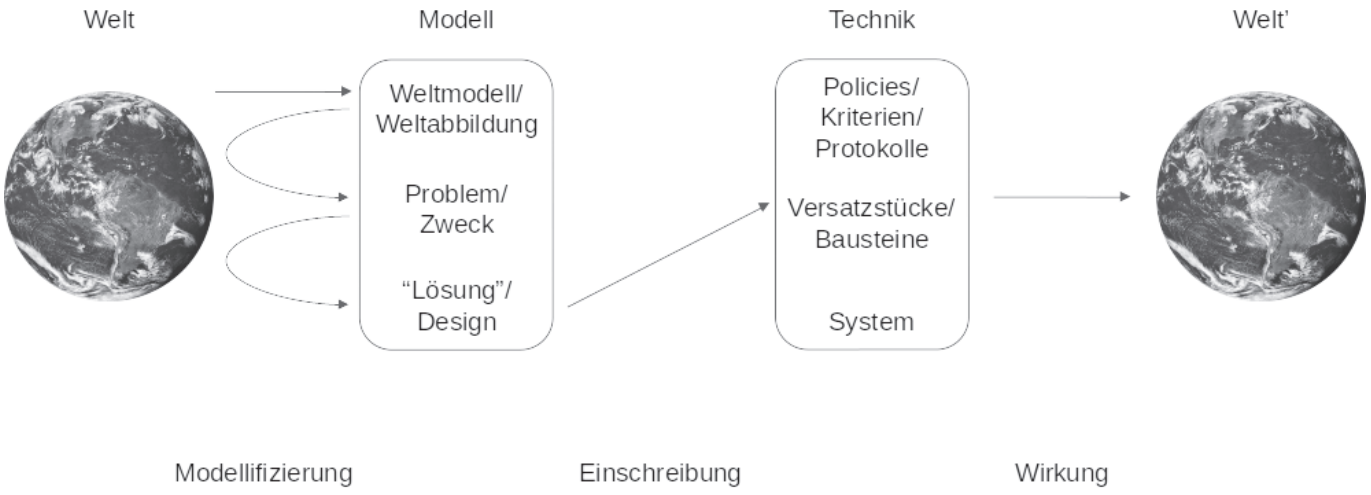


Abbildung 1: Meta-Modell

men. Vieles von dem ist nicht grundsätzlich neu und wird bereits in den beteiligten Disziplinen betrachtet, aber noch zu abstrakt oder zu sehr entlang von Einzelfällen (vgl. zur Kritik des soziologischen Einschreibungsbegriffs: The Berlin Script Collective 2018). Es werden Einzelfallstudien über konkrete technische Entwicklungen und deren Umsetzung in der Praxis durchgeführt, ohne verallgemeinerungsfähige Aussagen über die technischen Einschreibungen von Modellannahmen zu machen (z. B. de Laet/Mol 2000), oder es werden Theorien über die Durchsetzung bestimmter Technologien (vgl. z. B. Pinch/Bijker 1984) oder den technologischen Wandel entwickelt (z. B. Geels 2002), ohne konkrete Anknüpfungspunkte zu liefern, um in die praktische Entwicklung solcher Informatiksysteme einzugreifen und die Gestaltung zu beeinflussen. Ein wichtiger Schritt dafür ist, konsequent zwischen Modell und Einschreibung zu trennen – etwas, das in den beteiligten Disziplinen selten gemacht wird: In der Informatik wird der Prozess der Einschreibung nicht gesondert von der Modellierung betrachtet (vgl. z. B. Floyd/Klischewski 1998)[1], während in der Soziologie die Modellierung als Teil technologischen Designs, des Einschreibungsprozesses, subsumiert wird (vgl. z. B. Orlikowski 1992: 410).

Modellifizierung und Modelle

Der erste Abschnitt dieses Modellifizierungs- und Einschreibungsprozesses soll nun genauer beleuchtet werden. Modellifizierung soll mit Wilhelm Steinmüller der Prozess und das Produkt der Modellierung heißen (Steinmüller 1980), also die Abbildung der Welt in informationsverarbeitende Systeme. Dieser Schritt soll als Modellifizierung, und nicht als Modellierung bezeichnet werden, weil – wie etwa auch bei Kommodifizierung oder Objektifizierung – der Substitutionsaspekt der produzierten Modelle zentral ist. Die Produkte können Abbildmodelle sein – basierend auf der Annahme, wie immer sie begründet sei, dass es eine Realität gebe, die abgebildet werde in einem Modell – oder konstruktionistische Modelle – etwa über zukünftige Welt (siehe umfassend Stachowiak 1973, 1983, Fischer et al. 1995, Floyd/Klischewski 1998, Wyssusek 2004, Mahr 2009). Es können Prozess-, Struktur- und Interaktionsmodelle sein, es können Menschen-, Ding- oder Konzeptmodelle sein, und bei den Menschenmodellen können es Personen-, Gruppen- oder Bevölkerungsmodelle sein. So sind dann etwa „Skripte", wie sie die Techniksoziologie versteht (vgl. Akrich 1992), konstruktionistische Handlungsmodelle, die in technische Systeme vergegenständlicht, eingeschrieben sind, und so den Technikhandelnden zukünftige Handlungen strukturieren, nicht unbedingt erzwingend sondern auch ermöglichend (vgl. z. B. Akrich/Latour 1992: 261).

Die im Zusammenhang mit der Modellifizierung auftretenden Probleme lassen sich in drei Kategorien zusammenfassen: Modellannahmen, Modellierungshoheit und Entscheidungsprämissen (vgl. Pohle 2018: 241ff).

Zu den Modellannahmen: Im Gegensatz zu den meisten Modellen in den verschiedenen Technikwissenschaften, die erst wieder „in die Welt" umgesetzt werden müssen, und deren Beschränktheiten deshalb breit reflektiert und in der Praxis kompensiert werden – so muss ein Schiffsmodell nicht unbedingt schwimmen können, das am Ende zu bauende Schiff jedoch schon – werden informatische Modelle im allgemeinen so gestaltet, dass man direkt auf ihnen prozessieren kann. Diese Prozessierbarkeit informatischer Modelle ist dann sowohl notwendige wie hinreichende Bedingung: Alles, was relevant ist, ist dann eben die Frage der Berechenbarkeit – nicht mehr die Frage der Validität der Modelle. Und diese Modelle reflektieren die ihnen zugrunde liegenden und gelegten Modellannahmen und Daten-, Variablen- und Parameterauswahlentscheidungen (Harbordt 1975: 76): Welche Variablen und Beziehungen werden als wesentlich in das Modell aufgenommen? Welche werden vernachlässigt oder gar ausgeblendet? Welche Größen werden als veränderbar angesehen und welche als vermeintliche Konstanten? Abbildungen sind dabei verkürzt, verzerrt, aber nicht einfach falsch oder richtig, sondern funktional oder zweckmäßig (Luhmann 1964: 222). Und daher geht es zentral um die Frage, wessen Perspektive, welche Zwecke und wessen Zwecke die Modelle geprägt haben.

Das zweite Problemfeld, die Modellierungshoheit, wirft genau diese Fragen auf: Welche Zwecke, wessen Zwecke? Modellierungshoheit bezeichnet dabei die Entscheidungsmacht über die Zwecksetzung und die Modellannahmen, auf deren Basis dann diese Modelle gebildet werden, und die Kontrolle über die Prozesse der Modellbildung (Pohle 2016: 8): Wer bildet ab? Wer misst? Wer entscheidet, was abgebildet und gemessen wird – und was nicht? Wie wird abgebildet oder gemessen – qualitativ oder quantitativ, mit welchen Werkzeugen? Wie stark oder schwach sind Zuschreibungen und Festschreibungen, auch über Zeit? Und wie leicht oder schwer – bei informatischen Modellen oft eher leicht – verselbständigen sich die Modelle – aus dem Kontext, in dem sie ursprünglich entstanden sind, von den Zwecken, zu denen sie ursprünglich geschaffen wurden (vgl. „data-shadow", Anér 1972: 179)?

Entscheidungsprämissen sind, drittens, Vorentscheidungen, die Entscheidungen zugrunde gelegt werden und die damit den Entscheidungsrahmen einengen. Sie stellen insoweit organisierte Pfadabhängigkeiten dar: Sie werden für alle nachfolgenden Prozessschritte als wahr angesehen, als Grundlage für weitere Entscheidungen angenommen, kurz: einfach weiter prozessiert. Auch das ist nicht neu: In Bezug auf die bürokratische Verwaltung hieß es immer schon „Quod non est in actis, non est in mundo" – Was nicht in den Akten steht, ist nicht in der Welt (vgl. Vismann 2000). Und schon lange ist auch als Erweiterung bekannt: Was nicht im Computersystem steht, ist nicht in der Welt (Warner und Stone 1970: 67).

Nach diesem Überblick über einige Grundlagen zum Verständnis der Rolle von Modellen in der Technikentwicklung und der Modellifizierung im Besonderen betrachten wir nun den zweiten Schritt, die Einschreibung dieser Modelle in sozio-technische Systeme.

Einschreibung und Technik

Unter Einschreibung verstehen wir die schrittweise Umsetzung der Modelle in die Technik; hier konkretisieren sich die Annahmen der Modelle in Artefakte. In Abgrenzung zu einem holistischen Einschreibungsbegriff, der auf die im fertigen Produkt eingeschriebenen Handlungsmodelle abhebt und dabei gänz-

lich vom eigentlichen Einschreibungsprozess abstrahiert (Akrich 1992: 208f, Berlin Script Collective 2018: 129), geht es uns hier genau um diesen Umsetzungsprozess der Modelle in das technische System. Der in der Informatik gebräuchliche Begriff der Implementierung vernachlässigt die Aspekte der Realität, die gerade nicht abgebildet, aber dennoch in der Technik – als blinde Flecken – integriert werden.

Wie bei der Modellbildung sind auch im Einschreibungsprozess wiederum InformatikerInnen und EntwicklerInnen sowie ProjektleiterInnen beteiligt. Bei Open-Source-Projekten kann theoretisch sogar jede/r, die/der möchte, zum Code beitragen. Jede/r, die/der an der Umsetzung der Modelle beteiligt ist, bringt schließlich ihre/seine Ideen und Vorstellungen von „Welt" durch ihre/seine Interpretation der Modelle mit ein (vgl. Schäufele 2017: 67f). Stück für Stück werden durch die Umsetzung der Modelle die Freiheitsgrade der Technik immer weniger (vgl. z. B. Dierkes 1989), die Modelle werden materialisiert. Dadurch entsteht ein wirksames, fixiertes Stück Technik, in das die Annahmen der Modellbildung eingeschrieben sind.

Im Prozess der Einschreibung werden in die entstehende Technik durch die Verwendung verschiedener Artefakte auch Annahmen und Normen integriert:

1. Policies und Kriterien, die festgelegt werden,

2. Bausteine und Versatzstücke, die von Dritten für andere Zwecke gemacht wurden und entsprechende Festlegungen enthalten,

3. ganze Systeme können integriert werden.

Durch diese Festlegungen wird das System sukzessive definiert, und teils implizite Annahmen und Normen der Modelle werden mit eingeschrieben.

Neben den genannten Artefakten wirken sich auch die Strukturen der Arbeitsorganisation auf die Beschaffenheit des Produkts aus (ebd.). Verschiedene Anforderungen und damit verbunden unterschiedliche Rechte, Pflichten und Entscheidungsbefugnisse haben Einfluss darauf, welche Modelle, welche Bibliotheken, welche Code-Beiträge schließlich in welcher Form in das technische Konstrukt einfließen. Die Normen, praktischen Gepflogenheiten und Arbeitsstrukturen einer Entwicklungsgemeinschaft oder -organisation spielen auf eine spezifische Weise zusammen und formen innerhalb ihrer organisatorischen Einheit einen gemeinsamen Konsens, wie Dinge „notwendigerweise" gemacht werden müssen.[2] Dies lässt sich als epistemisches Regime beschreiben, etwa wie verschiedene Linux-Communities die Installationsroutine auf ihre jeweils spezifische Weise gestalten, und wie sich in der Gestaltung der Software die unterschiedlichen Annahmen über Kompetenz-Anforderungen an ihre NutzerInnen und die Strukturen der Arbeitsorganisation widerspiegeln (Guagnin i. E.). Im einen Extremfall wird durch das Verbergen von Konfigurationsmöglichkeiten vermieden, dass die User etwas Falsches machen (Ubuntu Linux), im anderen Extremfall wird durch das Weglassen eines vereinfachenden Assistenten vermieden, dass User, die das System nicht verstehen, es erfolgreich installieren (Arch Linux). Die als Modellannahme fungierende Setzung, für wen die an sich funktional äquivalenten Systeme geeignet sein sollen, zeigen sich hier sehr deutlich im Endprodukt.

An Ganzkörperscannern, wie sie etwa in Flughäfen eingesetzt werden, werden die je mehr oder weniger offensichtlichen Annahmen, die eingeschrieben wurden, deutlich. Wie sich an der Breite des Durchgangs sehen lässt, liegt der Gestaltung offensichtlich die Annahme zugrunde, dass das Gerät von Menschen benutzt wird, die auf zwei Beinen hindurchzugehen in der Lage sind, nicht aber Menschen, die mit einem Rollstuhl unterwegs sind.[3] Die weniger offensichtlichen Annahmen betreffen die Verteilungen von Körpermasse, die in das Gerät eingeschrieben sind (vgl. ausführlich Schäufele 2017: 131ff). Anstatt den BenutzerInnen der Geräte die halbnackten Bilder der Passagiere zu zeigen, wurde eine Softwareschicht eingebaut, die nur angibt, wo etwas von der Norm abweicht und damit als „verdächtig" und zu überprüfen definiert wird. Diese Methode schlägt notwendigerweise fehl, wo Menschen von der angenommenen und eingeschriebenen Norm abweichen, etwa aufgrund von atypischen Geschlechtsorganen. Diese Menschen sind nicht verdächtig – sie werden verdächtigt und diskriminiert.

Die materialisierte Einschreibung von Modellannahmen werden in den Beispielen sehr deutlich. Aber wie wirkt sich das auf unser Handeln mit Technik aus? Ähnlich wie Sozialstruktur eine beeinflussende Wirkung auf Handeln hat, strukturiert auch Technik unser Handeln und wirkt sich auf unsere Welt aus.

Wirkung

Zur theoretischen Erfassung der Wirkungsweise von Technik auf unser Handeln folgen wir der Argumentation des Berlin Script Collective (2018). Dabei geht es hier nicht um Macht im Sinne einer Androhung physischer Gewalt, sondern um verschiedene Stufen der Beeinflussung im Sinne einer Umsetzung einer Verhaltenserwartung.[4]

Dies kann erreicht werden durch Veränderung der Handlungsmöglichkeiten oder die Veränderung der Zielbildung des Handelnden, indem man Menschen dazu bringt, dass sie gar nicht mehr auf eine bestimmte Art handeln können oder auf die eine oder andere Art handeln wollen (vgl. The Berlin Script Collective 2018: 126f).

Dazu können entweder

1. Gegebenheiten der Situation verändert werden, die Handlungsoptionen betreffen, etwa durch technisch erzwungene Notwendigkeiten („Taste drücken, um fortzufahren") oder

2. Möglichkeiten geschaffen oder begrenzt werden (z. B. Konfigurationsmöglichkeiten im oben genannten Beispiel der Linux-Installationsroutine) oder

3. die Zielbildung beeinflusst werden, etwa durch positive oder negative Sanktionierung (z. B. Gamification) oder

4. Informationen zur Bewertung der Situation gegeben werden („Die Formatierung der Platte kann zu Datenverlust führen").

Die Form der technikvermittelten Beeinflussung ist nicht übermächtig, aber sie ergänzt sehr wohl andere soziale Formen der Beeinflussung wie die Vermittlung durch soziale Strukturen (z. B. Hierarchien) oder durch soziale Interaktion von Akteuren (vgl. Berlin Script Collective 2018: 127). Das zeigt, dass Technik wirksam soziales Handeln beeinflusst. Hierbei werden Annahmen modellhaften Handelns materialisiert in Beeinflussungsmodi der konkreten Gestaltung von Technik.

Eingeschrieben in die Technik, die uns umgibt, werden diese Annahmen in den verschiedenen Kontexten wirksam, in denen die Technik zum Einsatz kommt. Dabei ergeben sich verschiedene Wirkungsebenen in der Beziehung zu verschiedenen NutzerInnen. Dies veranschaulicht das obige Beispiel des Ganzkörperscanners. Neben dem Sicherheitspersonal, das die Maschine bedient, wirkt die Technik auch auf Passagiere, die der Scanner durchleuchtet.

Zu diesen zwei Ebenen der Benutzung kommen noch Dritte, die nicht Teil der Situation des Technikhandelns selbst sind, aber deren Auswirkungen zu spüren bekommen. Das können etwa MitarbeiterInnen in Geschäften hinter den Ganzkörperscannern sein, die die schlechte Laune von PassagierInnen zu spüren bekommen, die falsch kategorisiert und deshalb lange und intensiv befragt wurden. Das kann aber auch die Gesellschaft als Ganzes sein, weil es immer weniger Orte gibt, an denen solche Kontrollsysteme nicht eingesetzt werden, und sich damit die Freiheitsräume der Gesellschaft zunehmend schließen.

Es gibt also verschiedene ganz klare Wirkungsweisen der in Technik eingeschriebenen Annahmen, und es gibt vielfältige Wirkungsebenen der Technologien.

Schluss

Zum Ende kommen wir noch einmal auf das Ausgangsbild mit unserem Meta-Modell zurück. Damit können wir jetzt für ein Informatiksystem, was immer das im Konkreten ist, an dessen Entwicklung wir beteiligt sind, den Weg der Entwicklung verfolgen und dabei jeweils die Punkte identifizieren, an denen wir im Laufe der Entwicklung intervenieren können, etwa wenn es darum geht, bestimmte Code-Fragmente oder Software-Bausteine einzusetzen, die jeweils schon eine Einschreibung mitbringen.

Was also sind für uns vor diesem Hintergrund die zentralen Erkenntnisse? Wir glauben, dass im Gegensatz zu der herrschenden Diskussion, die sich vor allem an Konzepten wie Bias abarbeitet – Bias unterstellt einen wahren Wert, von dem es eine objektive Abweichung gibt, nämlich gerade den Bias –, wir einige Probleme sehr viel genauer fassen können. Erstens: Man kann nicht nicht modellieren. In der Folge ist aber damit aber auch klar, dass es keinen wahren Wert geben kann, oder anders: Es kann keine Systeme ohne Bias geben, sondern es lässt sich immer nur entscheiden, wie und in welche Richtung ein System oder ein Modell verzerrt ist oder sein soll. Es gibt keine objektiven Modelle von Welt, sondern die sind immer gemacht – von Akteuren mit Interessen und Zielen in vermachteten sozialen Beziehungen. Zweitens: Man kann auch nicht nicht einschreiben. Es wird immer etwas eingeschrieben. Drittens: Es gibt keine Neutralität von Technik. Es gibt also auch keine per se „freie" Technik. Viertens: Alles, was wirkt, hat auch Nebenwirkungen. Das heißt, das, was wir in Technik und mit Technik umsetzen, wirkt, wenn es wirkt, auf unterschiedliche Akteure, die davon betroffen sind, unterschiedlich. Selbst, wenn es also gut gemeint ist, ist es nicht unbedingt gut gemacht – für die Betroffenen und für alle Betroffenen gleichermaßen –, unabhängig davon, ob es auf der (ingenieur-)technischen Ebene gut gemacht ist.

Was ist dann zu tun? Wir denken, es muss in einem ersten Schritt darum gehen, insbesondere auch implizite Modellannahmen aufzudecken und zu explizieren, um sie damit erstens sichtbar und zweitens hinterfragbar zu machen. Immanent wichtig ist dabei, auch sichtbar zu machen, was nicht im Modell enthalten ist, das heißt die Leerstellen oder Fehlstellen, kurz: Was wurde ausgeblendet? Und nicht zuletzt ist zu fragen: Was ist dann konkret eingeschrieben in die Dinge, die wir „einfach so" benutzen, weil sie schon da sind, seien es Bausteine, Module

Daniel Guagnin und Jörg Pohle

Daniel Guagnin ist Soziologe und Informatiker. Er forscht und berät bei praemandatum zu ethischen Fragen in der Technikgestaltung, ein Teilaspekt davon betrifft Privatsphäre, Überwachung und Datenschutz. In seiner Doktorarbeit befasst er sich mit der Rolle von Laien in GNU/Linux-Communities.

Dr. **Jörg Pohle** ist PostDoc am Alexander von Humboldt Institut für Internet und Gesellschaft in Berlin, wo er das Forschungsprogramm *Daten, Akteure, Infrastrukturen* co-leitet und sich unter anderem mit gesellschaftlichen Aushandlungen im Bereich Privacy, Surveillance, IT-Sicherheit und Datenschutz befasst. Sein Forschungsinteresse gilt dem Schnittbereich von Informatik und Recht, dem Feld Informatik und Gesellschaft, der Modellifizierung und ihren gesellschaftlichen Auswirkungen sowie dem Datenschutz durch Technikgestaltung. Jörg Pohle studierte Rechtswissenschaft, Politikwissenschaft und Informatik in Berlin. Seine Diplomarbeit beschäftigte sich mit der Sicherheit von und dem Sicherheitsdiskurs zu Wahlcomputern. Er promovierte bei Wolfgang Coy an der Humboldt-Universität zu Berlin über Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung.

oder Frameworks. So ist etwa für ein Identitätsmanagementsystem zu fragen: Was wird dort als Identität verstanden? Welche Eigenschaften werden dort jenen, die Identität haben, zugeschrieben? Wie langlebig sind diese Identitäten, aber auch deren Einzeleigenschaften? Wie leicht oder schwer lassen sich die Identitäten von wem kontrollieren, ändern, löschen oder neu erzeugen? EntwicklerInnen müssen sich also immer genau damit auseinandersetzen, was sie sich einkaufen, wenn sie bestehende Systeme oder Teile davon nutzen. Kurz: Wir müssen immer fragen, was in diese Systemen schon jeweils eingeschrieben ist, bevor wir im Zuge der weiteren Entwicklung noch weitere Modelle einschreiben.

Und damit kommen wir zurück zu unserer Eingangsforderung: Technik ist gestaltbar und muss gestaltet werden – gestalten wir sie!

Literatur

Madeleine Akrich (1992), The De-Scription of Technical Objects. In: W. E. Bijker, J. Law. (Hrsg.), In Shaping Technology/Building Society: Studies in Sociotechnical Change. Cambridge, MA: MIT Press, S. 205–224.

Madeleine Akrich und Bruno Latour (1992), A convenient vocabulary for the semiotics of human and non-human assemblies. In Wiebe E. Bijker und John Law. Shaping Technology/Building Society: Studies in Sociotechnical Change. MIT Press.

Kerstin Áner (1972), Attack is the best defence. In: Management Informatics, S. 179–180.

Meinolf Dierkes (1989), Technikgenese als Gegenstand sozialwissenschaftlicher Forschung: erste Überlegungen. In: Ludwig von Friedeburg, Otto Jacobi (Hrsg.), Konzepte sozialwissenschaftlicher Technikforschung: Verhandlungen des Workshops 1987. München: Verbund Sozialwissenschaftliche Technikforschung, Koordinationsstelle, S. 154-170.

Martin Fischer, Gernot Grube und Fanny-Michaela Reisin (Hrsg.) (1995), Abbild oder Konstruktion – Modellierungsperspektiven in der Informatik. Berlin: KIT Report 125.

Ludwik Fleck (1979), Genesis and development of a scientific fact. Chicago: University of Chicago Press.

Christiane Floyd (1989), Softwareentwicklung als Realitätskonstruktion. In: W.-M. Lippe (Hrsg.), Software-Entwicklung: Konzepte, Erfahrungen, Perspektiven. Fachtagung, veranstaltet vom Fachausschuß 2.1 der GI, Marburg, 21.-23. Juni 1989. Proceeding. Berlin: Springer, S. 1–20.

Christiane Floyd und Ralf Klischewski (1998), Modellierung – ein Handgriff zur Wirklichkeit. Zur sozialen Konstruktion und Wirksamkeit von Informatik-Modellen. In: K. Pohl, A. Schürr, G. Vossen (Hrsg.), Modellierung ‚98 – Proceedings. Universität Münster, Bericht # 6/98-I, S. 21–26.

Heinz von Foerster (2002), Understanding Understanding. Essays on Cybernetics and Cognition. Berlin: Springer.

Frank W. Geels (2002), Understanding the dynamics of technological transitions. A co-evolutionary and socio-technical analysis. Enschede: Twente University Press (TUP)..

Steffen Harbordt (1975), Die Gefahr computerunterstützter administrativer Entscheidungsprozesse: Technokratisierung statt Demokratisierung. In: G. E. Hoffmann, B. Tietze, A. Podlech (Hrsg.), Numerierte Bürger. Wuppertal: Peter Hammer Verlag, S. 71–77.

Daniel Guagnin (im Erscheinen), Linux für alle? Zur Rolle von Laien in Communities der quelloffenen Softwareproduktion. Dissertation Technische Universität Berlin.

Marianne de Laet und Annemarie Mol. „The Zimbabwe Bush Pump: Mechanics of a Fluid Technology". Social Studies of Science 30, Nr. 2 (1. April 2000): 225–63. https://doi.org/10.1177/030631200030002002.

Niklas Luhmann (1964), Funktionen und Folgen formaler Organisation. Berlin: Duncker & Humblot.

Bernd Mahr (2009), Die Informatik und die Logik der Modelle. In: Informatik-Spektrum 32(3), S. 228–249.

Wanda J. Orlikowski (1992), The Duality Of Technology: Rethinking The Concept Of Technology In Organizations. In: Organization Science 3(3), S. 398–427.

Jörg Pohle (2016), Transparenz und Berechenbarkeit vs. Autonomie- und Kontrollverlust: Die Industrialisierung der gesellschaftlichen Informationsverarbeitung und ihre Folgen. In: Mediale Kontrolle unter Beobachtung 5(1), URL: http://www.medialekontrolle.de/wp-content/uploads/2016/03/Pohle-Joerg-2016-05-01.pdf.

Jörg Pohle (2018), Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung. Dissertation Humboldt-Universität zu Berlin. URL: https://dx.doi.org/10.18452/19136.

Fabia Schäufele (2017), Profiling Zwischen Sozialer Praxis Und Technischer Prägung. Ein Vergleich von Flughafensicherheit Und Credit-Scoring. Wiesbaden: Springer VS.

Herbert Stachowiak (1973), Allgemeine Modelltheorie. Wien: Springer.

Herbert Stachowiak (Hrsg.) (1983), Modelle – Konstruktion der Wirklichkeit. München: Wilhelm Fink Verlag.

Wilhelm Steinmüller (1980), Rationalisation and Modellification: Two Complementary Implications of Information Technologies. In: S. H. Lavington (Hrsg.), Information Processing 80. Amsterdam: North-Holland, S. 853–861.

M. G. Stone und Malcolm Warner (1970), Politics, Privacy, and Computers. In: The Political Quarterly, S. 256–267.

The Berlin Script Collective (2018), Technik vergleichen: Ein Analyserahmen für die Beeinflussung von Arbeit durch Technik. In: Arbeits- und Industriesoziologische Studien 11(2), S. 124–142.

Cornelia Vismann (2000), Akten: Medientechnik und Recht. Frankfurt am Main: Fischer Taschenbuch.

Trevor J. Pinch und Wiebe E. Bijker (1984), The social construction of facts and artifacts: Or how the sociology of science and the sociology of technology might benefit each other. In: Social Studies of Science 14, S.399-441

Boris Wyssusek (2004), Methodologische Aspekte der Organisationsmodellierung in der Wirtschaftsinformatik – Ein soziopragmatisch-konstruktivistischer Ansatz. Dissertation TU Berlin. URL: https://dx.doi.org/10.14279/depositonce-898.

Anmerkungen

1 *Die Unterscheidung, die wir vornehmen, ist nicht deckungsgleich mit der Unterscheidung zwischen Entwurf und Gestaltung (vgl. Floyd 1989: 10), aber das genaue Verhältnis zwischen beiden Unterscheidungen muss vorerst ungeklärt bleiben.*

2 *In Anlehnung an Ludwik Fleck (1979), der über Denkstile und Denkformen geschrieben hat, lässt sich übertragen sagen: „Do, what can be done in no other ways".*

3 *Die Offensichtlichkeit bedeutet aber keineswegs, dass die Entscheidung für die eine und gegen die andere Nutzer*innengruppe bewusst getroffen wurde.*

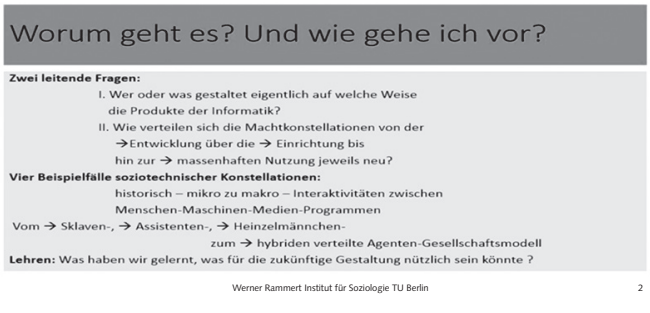
4 *Die physische Gewalt steht uns natürlich implizit auch gegenüber, wenn wir beispielsweise an die Ganzkörperscanner denken, aber weniger im Sinne einer technischen Androhung von Gewalt als einer sozialstrukturellen (Sicherheitsdienst).*

Werner Rammert

Konstellationen neu verteilter Gestaltungsmacht – Lehren für die Informatik?[1]

Wer oder was gestaltet eigentlich auf welche Weise die Produkte der Informatik? Wie verteilen sich die Machtkonstellationen von der Entwicklung über die Einrichtung bis hin zur massenhaften Nutzung jeweils neu? Sind es die Visionäre und Pioniere der Informatik? Die kapitalistischen Unternehmen disruptiver Innovation? Die politischen Regulierer demokratisch legitimierter Repräsentanten oder autokratischer Regime? Die kreativen Gruppen und kritischen sozialen Bewegungen? Oder die Masse der User und ihre alltäglichen Praktiken? Diese großen Fragen *werden anhand kleiner Fallstudien zur anfänglichen Gestaltung des Computers durch Nutzergruppen, zur späteren Konstruktion und Verwendung von Expertensystemen und zur Sozionik verteilter Agenten exemplarisch geklärt.*

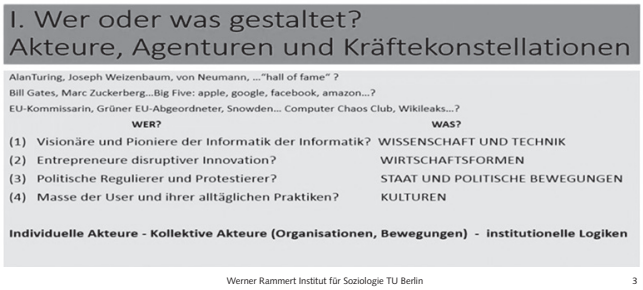
Gegenstand sind die wechselnden Formen, die Machtkonstellationen bei der Gestaltung von Computern und Künstliche-Intelligenz-Technologien annehmen können. Gefragt wird danach, wie in der Geschichte der Informatik die Gestaltungsmacht immer wieder neu und anders verteilt wird. Dabei wird zwischen verschiedenen sozialen Akteuren, wie Entwickler, Nutzergruppen, Professionen oder verwendende Organisationen, und institutionellen Kräften der Gestaltung, wie etwa Wirtschaft, Wissenschaft, Technologie, Politik oder Kultur, unterschieden. Diese Form der sozialen Verteiltheit des Handelns und der Handlungsmacht ist für die soziologische Perspektive vertraut und kennzeichnend. Die Form der technischen Verteiltheit von Operationen und Teilsystemen ist im Rahmen der technologischen Perspektive entwickelt worden. Sie ging von parallel arbeitenden Prozessen an Großrechnern aus, wie sie dann später für Systeme der ‚Verteilten Künstliche Intelligenz' typisch geworden sind. Beide Formen werden in diesem Beitrag zu einer sozionischen Perspektive zusammengeführt, um die Interaktivitäten und die Interferenzen zwischen den enger verkoppelten technischen und den sozialen Strukturen besser beobachten zu können. Sie bilden eine hybride Konstellation aus systemischen und nicht-systemischen Ordnungen, aus technischen Agenten und menschlichen Akteuren. Was zunächst kompliziert klingt, soll im Folgenden schrittweise und analytisch differenziert entfaltet werden. Welche Lehren die heutige Informatik aus der techniksoziologisch rekonstruierten Gestaltungsgeschichte ihrer Produkte ziehen kann, möge diese am Ende selbst herausfinden.



Zwei Fragestellungen leiten den Gang meiner Analyse. Die erste zielt auf die Identifizierung der Gestaltungskräfte: Wer oder was gestaltet eigentlich auf welche Weise die Produkte der Informatik? Die zweite konzentriert sich auf ihre Verteilung und Veränderung: Wie verteilen sich die Machtkonstellationen von der Entwicklung über die Einrichtung bis hin zur massenhaften Nutzung jeweils anders? Mit jeder neuen technischen Konfiguration, in jeder neuen sozialen Situation und in jeder neuen Phase der Entwicklung im Verlauf der Innovation verändern sich die Machtbeziehungen. Dieser Prozess wird hier anhand einiger Fallstudien kursorisch nachgezeichnet. Die Beispielfälle sind historisch angeordnet, reichen von der Mikroebene der Mensch-Computer-Interaktion bis zur Makroebene gesellschaftlicher Konfliktarenen und betrachten die Interaktivitäten zwischen Menschen und medialen Maschinen, zwischen sozialen Praktiken und Software-Programmen.

Im Vorgriff könnte man pauschalisierend sagen: Der Bogen, in welcher Beziehung die Techniken zum Menschen stehen, reicht vom Sklavenstatus bis zum Assistentenstatus der jeweiligen Technik, dann zum hintergründig wirkenden „Heinzelmännchen" bei den Multiagenten-Systemen [3] bis hin zum hybriden Modell einer auf menschliche und technische Agenten verteilten Konstellation. Mit dem Rückblick auf die Konstellationen verteilter Gestaltungsmacht, wie er hier für die frühen Techniken der Informatik aus den 1970er, 1980er und 1990er Jahren unternommen wird, lässt sich auch etwas über die heutigen Herausforderungen durch die Künstliche Intelligenz lernen, wie sie sich etwa bei der Gestaltung der Industrie 4.0, des Internets der Dinge, der Smart Cities oder der intelligenten Mobilität stellen.

Wer sind die Akteure der Gestaltung?



Wenn man schnell Namen nennen soll, die an der Gestaltung der Informatik und der Technologien der Künstlichen Intelligenz beteiligt sind, fallen einem zunächst etwa Alan Turing, Norbert Wiener, Joseph Weizenbaum, John von Neumann und manche anderen ein. In der „Hall of Fame" für die Pioniere der Informatik sind schon über 40 Personen versammelt. Weiterhin ganz oben in der Merkliste stehen die „Big Five", also Firmen wie Apple, Google, Facebook, Amazon und Microsoft. Es fallen auch die Namen von Bill Gates, Steve Jobs und Mark Zuckerberg. Bei längerem Nachdenken fällt uns eine EU-Kommissarin ein, die aktuell wirksam den Datenschutz stärkt und auch die Macht der Big Five begrenzen will; auch Edward Snowden und andere Whistleblower, Wikileaks, der Chaos Computer Club, der übrigens früher zu meiner Zeit noch als subversive Kraft eingeschätzt wurde, heute aber Banken und Regierungen zur Datensicherheit und Cybersicherheit berät. Sandro Gaycken etwa leitet gegenwärtig einen Think Tank zum Cyberwar, und Constanze Kurz ist journa-

listisch als Kolumnistin u. a. der FAZ tätig und weiterhin politisch als Sprecherin der kritischen Bewegung unterwegs.

Zusammen bilden sie eine bunt gemischte Schar von Akteuren. Sie lässt sich zunächst nach Einzelakteuren und kollektiven Akteuren wie Organisationen oder Bewegungen differenzieren. Es wäre nun genauer zu fragen: Wer von diesen Akteuren verfügt über welche Form von Gestaltungsmacht?

Akteure

Die erste Gruppe der Gestalter besteht aus den Visionären und Pionieren der Informatik. Das sind die Wissenschaftler und Forscherpersönlichkeiten, die ganz früh schon darüber nachgedacht haben: Was kann man später mit den Techniken der Informatik und der Künstlichen Intelligenz an unvorstellbaren und nützlichen Dingen alles anfangen? Diese theoretische Vorstellungskraft ist in ihrer orientierenden Gestaltungswirkung nicht zu unterschätzen: Die leitenden Paradigmen der Wissenschaftler und die experimentellen Proben der Entwickler bleiben primäre Einflussgrößen.

Die zweite Gruppe der Gestalter unterscheidet sich von den ersteren dadurch, dass sie zu wirtschaftlichen Unternehmern geworden sind. Bill Gates, Steve Jobs und Mark Zuckerberg gehören zur Gruppe der Schumpeterschen Unternehmer. Mit den neuen Geschäftsmodellen disruptiver Innovation krempeln diese kreativen Kapitalisten ganze Wirtschaftszweige radikal um. Letztlich sind es die Unternehmen, die kollektiven und organisierten Akteure, die auf diesem ökonomischen Feld die Gestalt der Techniken massiv prägen. Ähnliches hat es auch in früheren Gründerzeiten gegeben: Siemens war auch zuerst visionärer Forscher und experimentierender Techniker, und erst später entwickelte er aus der kleinen Werkstatt ein Weltunternehmen. Damals wie heute gab es auch andere wirtschaftliche Formen, etwa Genossenschaften und Entwicklergemeinschaften, aus deren kollektiver Experimentierpraxis dann alternative Technikgestaltungen hervorgingen.

Die dritte Gruppe der oben angeführten Gestalter übt Einfluss im politischen Bereich aus: Dazu zählen die politischen Regulierer und Protestierer, als Einzelpersonen, jedoch überwiegend als politische Bewegungen oder Organisationen. Regulation auf nationaler oder europäischer Ebene sollte man nicht in seiner Gestaltungswirkung unterschätzen. Gerade in Zeiten der Globalisierung und neu entfachter Nationalismen sind sie ein unverzichtbarer Bestandteil in der verteilten Machtkonstellation.

Eine vierte Gruppe der Gestalter wurde lange Zeit nicht wahrgenommen, wurde auch von den Informatikern anfangs wenig berücksichtigt: Das sind die Nutzer und Anwender, heute meist allgemein als *User* bezeichnet. Zunächst befinden sie sich auf der schwachen Seite einer Machtbeziehung: In der kapitalistischen Industrie schon mussten sich die Arbeitskräfte an die fremd und fertig gestaltete Maschinerie anpassen. Beim Massenkonsum mussten sich die Verbraucher mit der vom Produktdesign vorgegebenen Gestalt abfinden. Aus der Geschichte der Arbeiterbewegung kann man für heutige Techniknutzer lernen, wie eigene Gestaltungsmacht zurückgewonnen werden kann: durch kollektive Organisation, durch Mobilisierung, durch Mitbestimmung im Unternehmen und Kampf um die Gestaltung der Arbeitsbedingungen. Damals wurde der Unfallschutz eingeführt; heute haben wir Verbraucher- und den Datenschutz, als eine Bewegung, durch die Gegen-Regulation und alternative Gestaltungsmacht ausgeübt wird.

Was gestaltet?

Wenn man das Gestaltungshandeln aus dem soziologischen Blickwinkel auf seine Strukturen hin betrachtet, dann kann man sehen, dass die bisher analysierten Akteure nicht nur für das „Wer" der Gestaltung stehen: Gleichzeitig stehen sie für ein „Was", nämlich für Wissenschaft und Technik, für den wirtschaftlichen Bereich, für Staat und politische Bewegungen oder für die Kultur. Die Gesellschaft ist offensichtlich differenziert in bestimmte Bereiche und Felder. Diese haben eigene institutionelle ‚Logiken', welche der Gestaltung jeweils eine bestimmte Richtung geben: Wenn man sich im Wirtschaftsbereich bewegt, muss man Gewinne machen. Man kann auch die Gewinne verteilen, z. B. in Genossenschaften, aber trotzdem muss man Gewinne machen. Die ‚taz' ist so ein Alternativunternehmen; aber auch sie muss sich trotzdem am Gewinnziel orientieren und bestimmte Investitionen in dieser Hinsicht kalkulieren und tätigen. Wenn sie politisch wirkt, in die Öffentlichkeit hinein, dann ist sie zwar ein journalistisches Unternehmen, aber sie bleibt letztlich doch ein Wirtschaftsunternehmen. Im politischen Bereich geht es um Machtgewinn; Parteien und auch soziale Bewegungen streben mehr Macht und Einfluss an: Das geschieht nicht nur durch Wählen und Wahlkämpfen; manchmal müssen sich Menschen dazu auch einmal auf Bäume setzen und abtransportieren lassen. Folglich können staatliches Regulieren, Lobby- und Meinungsbildung sowie Protestieren und Demonstrieren unter dem System der Politik zusammengefasst werden; darunter verbinden sich all die verschiedenen Formen, die an Machtgewinn und Gegenmacht orientiert sind.

Beim vierten Bereich der Kultur lässt sich am wenigsten eine eindeutige Gestaltungsrichtung bestimmen. Denn die Logiken der kulturellen Orientierung sind so fluid und mit den anderen vermischt, dass sie am unsichersten festzulegen sind. Kulturelle Bewegungen signalisieren die jeweiligen Wert- und Lebensstilorientierungen. Gegenwärtig haben wir es mit einer Vielfalt von Identität stiftenden und sich von Benachteiligung emanzipierenden Minderheitsbewegungen zu tun; aber auch die vielen großen anerkannten Bewegungen – von der Arbeiter-, Bürgerrechts-, Frauen- bis hin zur Ökologiebewegung – gestalten über ihre Wertvorstellungen die Produkte und Systeme der Informatik mit. Dazu gehören aber auch die aktuell wieder sprießenden rechtsnationalen und anderen radikalen Bewegungen, die mit den etablierten Spielregeln und Werten brechen. Dabei sollte man nicht vergessen, dass es auch in den alternativen und grünen Basis- oder Graswurzelbewegungen zu Anfang eine seltsame Mischung widersprüchlicher Orientierungen gab: von stockkonservativ bis ökodiktatorisch, von rechtsnational bis linksradikal.

Man kann also zum Verhältnis von Akteuren und institutionellen Logiken festhalten: Es bedarf natürlich immer der individuellen Akteure, um etwas in Gang zu setzen, um eine Vision zu entwickeln und dafür alle Kräfte zu mobilisieren. Es sind dann jedoch eher die kollektiven Bewegungen und institutionalisierten

Akteure, welche die Projekte verstärken, die Mobilisierung organisieren und die Gestaltung längerfristig ausrichten. Schließlich sind es die Strukturen, die aus diesen verschiedenen und verteilten Gestaltungshandlungen hervorgegangen sind. Im politischen System sind dann Parteien, beispielsweise die Grüne Partei, dann eine Strukturgröße, ausgestattet mit finanziellen Ressourcen, mit geübter Mobilisierungsfähigkeit und programmatischen Richtungsentscheidungen, die dann insgesamt eine größere Gestaltungsmacht ausübt als einzelne Personen. Das kann immer mal wieder in die andere Richtung umkippen, wenn charismatische Personen oder ‚Influencer' mit viel Gefolgschaft im Netz zum Beispiel die Machtkonstellation verschieben. Bisher hat sich jedoch gezeigt, dass das ‚Crowd Sourcing' über das Netz meistens nur kurzfristig Massen zu mobilisieren vermag; längerfristig bedarf es dann doch einer sozialen Bewegung und ihrer Infrastruktur, um nachhaltig unter Beteiligung körperlich anwesender Menschen Gestaltungsmacht auszuüben.

Gestaltete Strukturen, die gestalten

Mit der Frage „Was gestaltet" wird die strukturelle Macht angesprochen, die auf etwas Einfluss nimmt, selbst institutionell gefestigt ist und in bestimmten Strukturen niedergelegt ist: Verfassungen, Gesetze, Parteiordnungen, Wirtschaftsformen und Verfahren, wie etwas gemacht wird. Sie betrifft natürlich auch die materiell-sachlichen Strukturen, wie Verkehrswege, Gebäude, Fahrzeuge und vieles mehr. Dazu gehören eben auch die Produkte der Informatik: Mit ihrer in Architekturen und Programmen fixierten Gestalt wird festgeschrieben, wie etwa welche Funktionen aufgeteilt sind oder wer Zugang zu was hat. Und diese Formen, die vergegenständlicht und als Gestalt versachlicht sind, üben selbst Gestaltungsmacht aus. Das lässt sich leicht am gestalteten Raum, in dem wir uns hier befinden, demonstrieren: Er ist mit seinem bühnenartigen Podest und der fest eingebauten Klapp-Bestuhlung als großer Hörsaal gestaltet. Diese Raumgestaltung und Sachfixierung lassen es nicht mehr zu, dass wir uns in einen kleinen Seminarkreis setzen und uns dabei ohne Mikrofon und mit Blickkontakt intimer verständigen können.

Die zweite Form der Gestaltung geht ebenfalls von den Produkten aus: Das Gestaltete determiniert nicht überall bis ins letzte Element hinein; vielmehr gestaltet es etwas vor, etwa offene Räume und Rahmen, die etwas ermöglichen, aber auch begrenzen. Und erst die verschiedenen und kumulierten Formen der praktischen Nutzung können dann zu neuen verfestigten Strukturen führen. Das kann an der Entwicklung des Internet gut beobachtet werden: Am Anfang weckte es die Illusion vollkommener Freiheit; man dachte, es ermögliche alles, befreie von den Zwängen und Beschränkungen der realen Welt. Es sollte ein herrschaftsfreier Raum sein – und mit der Zeit der praktischen Nutzung merkte man immer mehr, dass sich diese paradiesische Anarchie auch in wilden Kapitalismus und nationalstaatlichen Autoritarismus verwandeln kann. Man hatte zu gern und zu naiv den utopischen Vorstellungen der Hippie-Bewegung in Kalifornien getraut.

Eine wichtige Quelle für die populärreligiösen Visionen der ersten Akteure waren der Buddhismus, die indische Mystik und die Meditation – analog zum Protestantismus, den Max Weber für die Gründerzeit des Kapitalismus als entscheidenden Einfluss ausgemacht hat. Große gesellschaftliche Transformationen fangen häufig mit religiösen Innovationen an: Deren Gründerfiguren entwickeln abseits der alten Gesellschaft und ihrer Zwänge ihre davon radikal abweichenden Ideen und Utopien, indem sie zum Beispiel „in die Wüste gehen", lange Zeit fasten, sich in Einsiedeleien oder Klöster zur Meditation zurückziehen. Wenn ihre von der bedrückenden Normalität stark abweichenden Visionen und Werteideale eine wachsende Anhängerschaft finden – sie also nicht sofort als Sektierer verfolgt und als Ketzer verbannt oder verbrannt werden –, dann können die neuen Haltungen und Praktiken der Lebensführung mit Hilfe neuer Medien, etwa der Apostelbriefe, des Buchdrucks oder aktuell des Internets, einen mächtigen strukurbildenden Einfluss gewinnen: In letzter Konsequenz können daraus Weltreligionen oder auch Weltkonzerne entstehen. Einmal aus kleinen Alternativen in offenen Räumen der gesellschaftlichen Orientierung entwickelt, können diese kulturellen und wirtschaftlichen Makrostrukturen den alten institutionellen Rahmen radikal umwälzen und den neu gestalteten Handlungsraum wiederum begrenzen.

Das Konzept verteilten Handelns

Drei Begriffe von „verteilt" unterscheide ich in meinen Analysen. Für mich ist „Verteiltes Handeln" das Schlüsselkonzept, um das Zusammenspiel von technischen und menschlichen Einheiten in Operations- und Handlungszusammenhängen in der Gesellschaft zu verstehen und zu erklären. Dieser dritte Ansatz der „Distributed Agency" [6], an dem ich schon längere Zeit arbeite, beruht sowohl auf dem ersten, dem soziologischen Konzept sozialen Handelns und dem zweiten, dem informatorischen Modell der Verteilten Künstlichen Intelligenz.

Zwischen sozialen Akteuren

Das Soziale wird relational gedacht. Es entsteht aus Interaktionen und den Interpretationen der beobachteten Reaktionen auf Aktionen. Im Sozialen sind Handlungen wie Kaufen, Konstruieren oder Regieren auf mehrere Instanzen verteilt: auf verschiedene Akteure, auf verschiedene Ebenen und auf kollektive Akteure, die Machtkämpfe führen, die Dinge aushandeln. Auch in den jeweiligen gesellschaftlichen Strukturen schlägt sich diese Verteilung nieder. In den institutionellen Strukturen der Politik sehen wir, beispielsweise in den USA, wie die Verteiltheit der Macht, „the balance of power", noch funktioniert, so dass auch das Handeln krass regelbrechender Politiker noch in gewisser Weise eingerahmt wird.

Zwischen sozialen Institutionen

Das zweite Verständnis von „verteilt" betrifft die Institutionenkomplexe in der Gesellschaft: Zwischen den getrennt institutionalisierten Bereichen von Politik, Wissenschaft, Kultur, Ökonomie u. a. entstehen zunehmend gemischte Innovationsfelder verteilten Handelns, etwa Kompromisse zwischen Ökonomie und Ökologie, Interaktionen zwischen Wissenschaft und Kunst und neuerdings auch gemeinsam geteilte Plattformen, an denen sich alle Akteure beteiligen: Experten, Politiker, Unternehmer, Wissenschaftler, oder ein Think Tank: immer wieder auch ein

‚Summit' zum Klima, zur Elektromobilität, zur Künstlichen Intelligenz. Meine These ist, dass diese Art von Verteiltheit zunimmt, auch bei den institutionellen Akteuren: Die Wirtschaft kann nicht mehr allein agieren, die Politik kann nicht mehr allein regieren, und auch die Wissenschaft kann ebenfalls nicht mehr allein agieren. Auch unsere Exzellenzinitiativen in der Wissenschaft basieren auf vielen Koalitionen, Kompromissen und Bündnissen.

Verteilte technische Systeme

Bisher haben wir uns mit den zwei Auffassungen von „verteiltem Handeln" befasst, die sich auf soziale Handlungszusammenhänge beziehen, verteilt auf die sozialen Akteure und verteilt auf mehrere institutionelle Bereiche im Gefüge der Gesellschaft. Daneben gibt es noch das „verteilte Operieren" von technischen Systemen, etwa dem arbeitsteiligen und gleichzeitigen Nutzen von Rechnerkapazitäten beim ‚Distributed Computing' und auch bei der auf mehrere Instanzen verteilten Performanz von Systemen der ‚Distributed Artificial Intelligence'. Techniken sind dann nicht mehr geschlossene Systeme, wenn sie nicht mehr aus einzelnen gekapselten Systemen bestehen, sondern aus vielen und unterschiedlichen Systemen, die miteinander mehr oder weniger locker gekoppelt sind. Das wären dann verteilte Systeme aus Aktor-, Motor-, Sensor-, Regelungs- und Nachrichtensystemen, wie etwa komplexe cyber-physikalische Systeme digitalisierter Fertigung, autonomen Fahrens oder intelligenten Transports. Wegen der bedingten Umweltoffenheit, der Rückkopplungen und der Komplexität der Interaktivitäten sind diese als komplexe Systeme [8] nicht mehr im strengen Sinn zentral kontrollierbar. Sie bedürfen zusätzlicher Abstimmungs-, Eingrenzungs- und Kontrolleinrichtungen – menschlicher oder technischer Art –, um folgenreiche Pannen und unvorhersehbare Interferenzen einzugrenzen. Dadurch werden allerdings die Komplexität und die Fehleranfälligkeit wieder erhöht.

Als Technik galten bisher nur solche maschinellen und automatischen Systeme, wenn man sie eindeutig und sicher für einen bestimmten Zweck in einem vorgegebenen Operationsrahmen gestalten, einsetzen und kontrollieren konnte. Wenn sie durch Wahlmöglichkeiten, schlußfolgernde Regelbildung oder Maschinenlernen immer mehr Freiheitsgrade bei ihren Operationen erhalten, dann nähern sich diese technischen Installationen in ihrem Funktionieren schon graduell gesellschaftlichen Institutionen und sozialen Systemen an, die man auch nicht im strengen Sinn determinieren und kontrollieren kann.

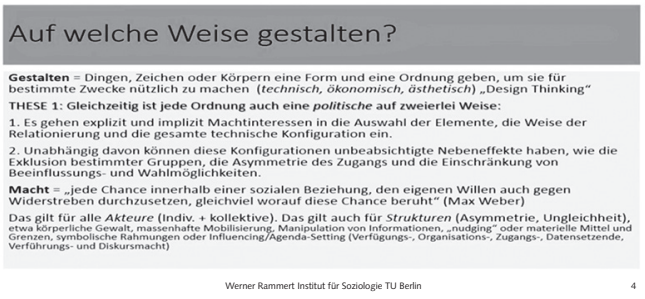
Verteilte heterogene Konstellationen

Diese technische Verteiltheit ist nach der sozialen Verteiltheit mit ihren beiden Varianten die zweite Form verteilter Prozesse, die wir kennen. Beide entstammen jeweils verschiedenen Disziplinen und ihrer besonderen soziologischen oder technologischen Perspektive. Es macht bei der gegenwärtigen engen Verflechtung von menschlichen, maschinellen, medialen und zeichenprozessierenden Aktivitäten Sinn, eine dritte Form der Verteiltheit als hybride Perspektive zu entwickeln. Sie zeichnet sich dadurch aus, dass sie die komplexen und gemischten Konstellationen insgesamt in den analytischen und gestalterischen Blick nimmt. Es geht da – wie häufig so bezeichnet – um ‚soziotechnische Systeme'. Aber der Systembegriff ist dabei zu wenig spezifisch und irreführend. Der System-Begriff suggeriert nämlich – zumindest bei den Technikwissenschaftlern – durchgängige technische Regelbarkeit.

Treffender und detaillierter spreche ich lieber von heterogenen und komplexen Konstellationen [8]: Sie bestehen aus Interaktivitätsbeziehungen zwischen sozio-institutionellen Gebilden und technischen Systemen, zwischen menschlichen Akteuren und technischen Agenten. Sie finden ihren gemeinsamen Gestaltungsrahmen in technischen und gesellschaftlichen Infrastrukturen, in rechtlichen Verfassungs- und technischen Systemarchitekturen, in denen die Aktivitäten, Interaktionen und Interaktivitäten ermöglicht, koordiniert und eingeschränkt werden. Daher bilden diese Konstellationen mit ihrer Form der hybriden Verteiltheit und ihren unterschiedlich gestaltbaren Balancen von Einwirkung, Autonomie und Kontrolle gegenwärtig die relevanten Einheiten für die Analyse und Gestaltung technologischer Innovationen und gesellschaftlicher Transformationen. Wenn es etwa um ‚Smart Cities' geht, um all die damit verbundenen neuen Mobilitäts-, Kommunikations-, Ver- und Entsorgungsstrukturen, dann sind natürlich alle Gestaltungsmächte einzubeziehen, welche die Entwicklung der Konstellation an den verschiedenen Ecken und Kanten beeinflussen: Das sind die verteilt handelnden sozialen Akteure wie auch die verteilt wirkenden technischen Agenturen; das sind ebenso die verteilten institutionellen Logiken wie auch die verteilten technischen Systeme. Vor allem betrifft es die vielen Schnittstellen und Koppelungen dazwischen.

Man kann sich jetzt gut vorstellen, dass diese gesamte Konstellation nicht mehr als einheitliches System kontrolliert und zentral gesteuert werden kann, wie das jeder Maschinen-, Motorbau- und vielleicht auch Softwareingenieur für die jeweils eigenen abgekapselten Systeme noch gelernt hat.

Was auf welche Weise gestalten?



Was heißt gestalten und was wird gestaltet: Dinge und Zeichen lassen sich erst einmal unterscheiden. Informatiker arbeiten meistens mit Zeichen oder an Zeichensystemen und Verfahren der Zeichenverarbeitung, aber auch mit Dingen. Man denke an Algorithmen, Programme, Compiler, Computer- oder Netzarchitekturen. Soziologen und Psychologen sind daran beteiligt, wenn es um die Gestaltung von Schnittstellen zwischen Technik und Mensch geht. Neben die technisch funktionale Gestalt treten die leichte, möglichst intuitive Bedienbarkeit, der ästhetische Reiz und das kulturelle Prestige. Design heißt in diesem mehrfachen Sinne, einem Ding, einem Prozess, einem Zeichen oder einer Schnittstelle eine bestimmte Form und Ordnung zu geben, um sie für bestimmte Zwecke – technische, ökonomische, kul-

turelle, ästhetische – nützlich zu machen. Beim ‚Bauhaus'-Design war es die Verbindung zwischen Kunst, Handwerk, Industrie und Ökonomie. Bei der Apple-Design-Strategie von Dieter Rams und Steve Jobs hieß es, erst dann auf den boomenden PC-, Player- oder Smartphone-Markt zu gehen, wenn man in der technischen Funktionalität hoch überlegen ist, in Usability und ästhetisches Design genügend investiert hat und man dann dafür den dreifachen Preis nehmen und eine exklusive Nutzer-Community bedienen und begründen kann. Das vom Hasso-Plattner-Institut propagierte ‚Design Thinking' verallgemeinert diese Design-Prinzipien auf alle Bereiche: die Gestaltung von Websites wie auch von Arbeitsabläufen, die Kuratierung von Museumsausstellungen und die Inszenierung von Konferenzen und Verhandlungsergebnissen.

Das Design von Dingen und technischen Artefakten ist nicht neutral, sondern immer auch wertbezogen und politisch orientiert. Erstens können die Gestalten explizit oder implizit auf unterschiedliche Machtinteressen bezogen sein; es betrifft etwa die Auswahl, welche Elemente wie aufeinander bezogen werden und letztlich die gesamte technische Konfiguration. Explizit heißt: Manches macht man ausdrücklich, und dann ist es auch häufig sichtbar. Implizites wird erst sichtbar, wenn erst später die nicht explizit eingebauten Möglichkeiten der Kontrolle genutzt werden. Bei den ersten elektronischen Kassen von Nixdorf für den Einzelhandel war man explizit an der Rationalisierung des Rechnungs- und Bestellsystems interessiert. Die Entwickler wussten noch nicht, dass damit gleichzeitig die Leistung und die fehlerhaften Eingaben der Kassiererinnen kontrolliert werden können. Heute bei den Lagerarbeitern von Amazon ist es von vorne herein klar: Jeder bekommt so ein Tablet, nicht nur als Instrument für die Abwicklung der Bestellungen, sondern auch zur Kontrolle für Fehler und zu lange Toilettenzeiten.

Ein zweiter Aspekt des Politischen zeigt sich darin, dass diese Konfigurationen auch insgesamt Nebeneffekte erzeugen: etwa die Exklusion bestimmter Gruppen, eine Asymmetrie von Zugängen, die Einschränkung von Beeinflussungs- oder Wahlmöglichkeiten, die wir jetzt überall bei sozialen Medien und beim Umgang mit unseren Daten [7] erleben und erst durch Whistleblower, Wikileaker und Hacker rechtzeitig aufgedeckt bekommen. Auch diese Design- und Konfigurationseffekte müssen nicht unbedingt von Anfang an beabsichtigt sein. Je mehr man darüber weiß, desto mehr nutzen manche Akteure diese Lücken im Design, Löcher in der Firewall und Schieflagen der Einflussmöglichkeiten aus: Das machen Geheimdienste, das machen Firmen, das machen Kriminelle, und das machen politisch bewusste Hacker.

Macht

Der klassische soziologische Begriff von Macht besagt, dass sie in der Chance besteht, innerhalb einer Beziehung den eigenen Willen auch gegen das Widerstreben des Anderen durchzusetzen – gleichviel, worauf die Chance beruht, Gewalt, Belohnung, Autorität oder Verführung … Das gilt für alle Beziehungen: Eltern gegenüber Kindern, Männer gegenüber Frauen, Chefs gegenüber Beschäftigten – und umgekehrt auch. Mit der Macht ist es nicht so einfach und einseitig, wie man häufig unterstellt. Wenn sich beispielsweise Arbeiter, Bürger, Jugendliche zusammentun und organisieren, dann entsteht eine Gegenmacht, die es dem übermächtigen Unternehmen, einem autoritären Staat oder einer saturierten älteren Generation erschweren kann, bestimmte Dinge weiterhin ohne Widerspruch zu tun oder zu unterlassen.

Macht ist soziologisch immer eine zweiseitige Beziehung, wie klassisch schon diejenige von Herr und Knecht, wie sie von Hegel schon beschrieben worden ist: Der Herr ist darauf angewiesen, dass der Knecht die Unterwerfung mitmacht. Wenn er sich auflehnt – das sehen wir schon beim römischen Sklavenaufstand – gerät die Herrschaft ins Wanken. Wichtig sind also die in der Beziehung aufrechterhaltene Asymmetrie und die Beteiligung beider Seiten daran. Aufklärung und Emanzipation können dafür sorgen, dass Schwächere, Benachteiligte, Unterdrückte oder im Schatten stehende Gruppen sichtbarer werden und die Legitimität der Ungleichheit in Frage stellen. Aktuell schaffen im Internet solche Emanzipationsbewegungen wie #MeToo Sichtbarkeiten tradierter Machtverhältnisse.

Neben diesen Machtunterschieden zwischen Individuen gibt es auch die strukturelle Macht. Sie hängt davon ab, wie die Institutionen schon vorstrukturiert sind, dass bestimmte Verfassungen und Gesetze einigen Gruppen mehr oder weniger Rechte und Schutz gewähren. Das gilt auch für die Verfasstheit technischer Architekturen und Infrastrukturen: Dort ist in die Systeme eingebaut und in Programme eingeschrieben, wer die Agenda setzen kann, wer Zugang zu bestimmten Daten und Regelsetzungen hat [7], wer gegenüber anderen Führungsmacht oder Diskursmacht hat. Die Medien und das Netz sind heute neue Machtverstärker, aber sie selbst sind eigentlich keine Macht, nur die in sie eingeschriebenen asymmetrischen Zugangs- und Verteilungsstrukturen. In dieser Hinsicht sind die neuen Produkte der Informatik, etwa die eingebaute Künstliche Intelligenz, die ‚Deep Learning'-Schnittstellen oder das Internet der Dinge genauer zu untersuchen.

Diese Entwicklung zur Transformation des Sozialen durch die Produkte der Informatik war schon vor 20 Jahren absehbar. Derzeit hatte ich in einem Vortrag zur ‚Zukunft der Künstlichen Intelligenz' drei Tendenzen vorhergesagt: Die KI wird interaktiv, verteilt und verkörpert sein. All das sehen wir heute: ‚Embodied Intelligence' bei Robotern und autonomen Fahrsystemen in vollem Vormarsch; die Verteiltheit der Systeme, der Aktivitäten und Interaktivitäten zwischen den Systemen nimmt enorm zu; und die Interaktivitäten zwischen Mensch und Technik wachsen rasant an. Sie verändern sich mit zunehmenden Dialogen, Schnittstellenmedien und Datensammlungen. Beim ‚Deep Learning' entsteht sogar eine tiefe Wechselseitigkeit, die gar nicht sichtbar ist, ähnlich wie bei der Interaktion zwischen Menschen. Man weiß eben nicht, was sich der andere dabei denkt und wie er es interpretiert. Dadurch können Freundschaften, aber auch Feindschaften, Fachkollegschaften oder auch politische Gefolgschaften entstehen. Solche technisch vermittelten Interaktionen können durch ihre Verstärkung und Intransparenz auch Macht in dem Sinne erzeugen, dass sie politische Fraktionierungen und öffentliche Meinungsbildung stark in eine Richtung lenken.

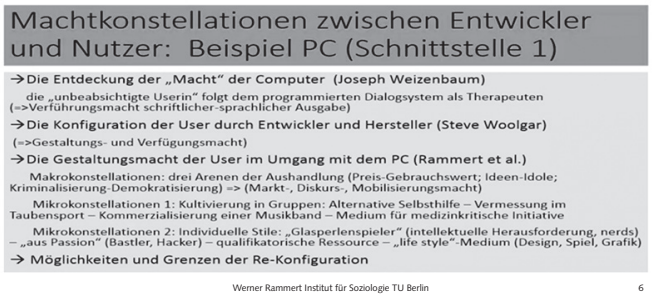
Gestaltungsmacht im Wandel: Beispiele

Wolfgang Coy hat in seiner Vorlesung vom letzten Jahr „Von den Enden der Informatik" eindrucksvoll von den Fortschritten

der Speicher zu Beginn der Informatik gesprochen. Er zeigte Bilder von Computerspeichern aus den 50er Jahren in den USA, die mehrere große Säle ausfüllten. Die damaligen Speichermedien erzeugten eine große Hitze und fielen auch dauernd aus, mussten immer wieder mühsam ausgewechselt werden. Heute ist die gleiche Speicherkapazität von Großrechnern des MIT oder des Defense Department schon in jedem unserer Laptops enthalten. Dazu kommen die Riesensäle mit Servern, in Felsenhöhlen gekühlt und gesichert, in denen die Kapazitäten für die ‚Clouds' vorgehalten werden. Wie zu Anfang schon erwähnt: Es geht um Zeichen und Dinge. Software für Speicherung, Verarbeitung und Nachrichtenübermittlung, aber immer auch noch um solide Hardware von Servern, Kabeln und Satelliten, die an Orten auf der Erde und im Weltraum konzentriert und geschützt werden. Dieses Faktum ist nicht zu überschätzen: Bei Krieg, bei Spionage oder bei den zunehmenden ‚Cyberwar'-Aktivitäten sind das gegenwärtig die entscheidenden strategischen Orte – es geht nicht nur um Atomraketen und deren stationäre und mobile Träger, sondern es geht jetzt auch um informationelle Kriegsführung, Trojaner, Viren und Firewalls.

In meinem kurzen historischen Überblick möchte ich mich weder nur auf Hardware- noch auf Software-Produkte, auch nicht nur auf deren Erweiterungen, konzentrieren: Im Fokus stehen die Schnittstellen und die Veränderungen der gesamten Konstellation von auf Menschen, Maschinen, Medien und Programme verteilten Handelns. Gefragt wurde in den jeweiligen Studien, wie sich dadurch die Gestaltungsmacht verändert.

Beispiel 1: Individuelle Akteure – Entwickler und Nutzer beim PC



Akteure, üblicherweise der Entwickler, aber auch der Nutzer von PCs und Softwareprogrammen. Die Macht der Entwickler gegenüber Nutzern war in den Anfängen der Entwicklung selbst einem so gewissenhaften Forscher und erfolgreichen Entwickler wie Joseph Weizenbaum [1] nicht so bewusst. Er hat für die Entwicklung eines Dialogsystems namens ELIZA einfach die Frage- und Antworttechnik einer psychiatrischen Methode übernommen: Der Psychiater fragt und der Patient antwortet, der Arzt greift ein Wort aus der Antwort heraus und baut es in die anschließende Frage ein, und so weiter, ohne wirklich ein Gespräch zu führen. Trotzdem fühlt sich der Patient anschließend besser, weil er glaubt, dass er verstanden wird. Erst als Weizenbaum seine Sekretärin dabei beobachtet, wie sie das technische Dialogsystem ernsthaft benutzt, bemerkt er die unbeabsichtigte Macht des Entwicklers und seines Produkts. Allerdings muss man auch hervorheben, dass erst der User – hier also die ausprobierende Sektretärin – ebenfalls unbeabsichtigt aus diesem technischen Dialogsystem eine funktionierende therapeutische Technik gemacht hat, die sie akzeptiert. Dahinter steckt auch keine geheime „Macht des Computers" und seiner Meisterentwickler. Es ist hier ganz offensichtlich die Verführungsmacht von schriftlich-sprachlicher Rede bei der Ausgabe: Wenn auf dem Bildschirm etwas geschrieben steht, denkt man automatisch, da steckt eine menschliche Person dahinter, die antwortet und einen versteht. Verstehen und Verstanden werden fühlen sich großartig an.

Die Gestaltungsmacht ist in diesem Fall – und beispielgebend auch für Schnittstellen bis heute hin wie Alexa, Siri u. a. – auf mehrere Instanzen verteilt: auf die Softwareentwicklerin, auf den deutenden und umnutzenden Nutzer und auf eine Schnittstellendesignerin, die bei der Gestaltung der Ausgabe von Rechen-‚Ergebnissen' das natürlich-menschliche ‚Antwort'-Verhalten nachahmt. Sie lässt den Output nicht mehr in abstrakter Form als Lochkarte oder als Band kaum lesbarer Zeichenskripte edieren.

Der zweite Fall betrifft dann eine deutliche Verschiebung der Gestaltungsmacht. Der britische Soziologe Steve Woolgar [2] hat in einer teilnehmenden Untersuchung herausgefunden, wie Hersteller und Entwickler von PCs absichtlich die technische Konfiguration des Geräts und der Schnittstelle so gestalten, dass die Nutzer in ihren Möglichkeiten eingeschränkt und ihren Nutzungsweisen beeinflusst werden. Hersteller und Entwickler legen durch die technische Konfiguration von vornherein fest, wozu und wie der PC genutzt werden soll und kann. Über die Gestaltung der technischen Struktur konfigurieren sie auch gleichzeitig den Nutzer: Es wird vorstrukturiert und vorprogrammiert, wovon er ausgeschlossen wird, was er nicht wissen soll, wie er damit erwartungsgemäß umgehen soll und was seiner Bequemlichkeit dient. Es handelt sich hier um eine andere Macht, nämlich die Gestaltungs- und Verfügungsmacht der Hersteller.

Mikro- und Makrokonstellationen der Gestaltungsmacht

Die Gestaltungsmacht verteilt sich auf verschiedene Ebenen, beschränkt sich nicht auf die Mikro-Konstellationen von Entwickler-Nutzer-Beziehungen. Diese Verteilung habe ich schon in den 1980er Jahren im Rahmen des Programms ‚Sozialverträgliche Technikgestaltung' in einem größeren Forschungsprojekt zum ‚Umgang mit Computern im Alltag' [3] empirisch untersucht. Es wich von den damals üblichen Projekten dadurch ab, dass es sich nicht nur mit männlichen und jugendlichen Computernutzern beschäftigte, sondern männliche und weibliche, jüngere und ältere Nutzer von PCs in einer kontrastierenden Stichprobenauswahl einbezog. Außerdem beschränkte es sich nicht auf die verschiedenen individuellen Nutzungsformen der damaligen Zeit, in der sich eine sinnvolle Nutzung des PC zuhause noch nicht abzeichnete und auch von den Herstellern noch nicht vorgeprägt war. Daher dehnten wir die Untersuchung auf die höheren Ebenen von Machtkonstellationen aus, die den alltäglichen Nutzungssituationen vorgelagert waren.

Insgesamt konnten von uns drei solcher Ebenen identifiziert werden: Gestaltungsmacht wurde erstens von institutionellen Akteuren in Makro-Konstellationen auf der gesamtgesellschaft-

lichen Ebene, zweitens von Gruppen oder sozialen Bewegungen in mittleren Konstellationen kollektiver Aneignung und drittens von einzelnen Personen in Mikro-Konstellationen der Mensch-Technik-Interaktion ausgeübt werden.

Auf der Makroebene konnten wir drei gesellschaftliche Arenen der Aushandlung zwischen den kollektiven und organisierten Akteuren unterscheiden: In der techno-ökonomischen Arena wurde damals über den neu entstehenden Markt für PCs die Beziehung zwischen ökonomischem Preis und sozialem Gebrauchswert ausgehandelt. Das können wir bis heute bei den smarten Neugeräten beobachten. In der soziokulturellen Arena wurden die Diskurse über Sinn und Unsinn geführt, wobei kreative Ideen der Nutzung ins Spiel kamen, aber auch Ideologiekritik am Computermythos und an den Folgen geübt wurde. In der politisch-rechtlichen Arena ging die gesellschaftliche Debatte und politische Willensbildung um Fragen der Verfassungsverträglichkeit und der gesetzlichen Gestaltung: Sind abweichende Nutzungsweisen wie etwa das ‚Hacken' eher kriminell? Wann fördern oder gefährden bestimmte Praktiken die Demokratie? Das sind Fragen, die auch den heutigen Diskurs um das Internet und die sozialen Medien bewegen. Als Ergebnis können wir für die Makroebene der institutionellen Akteure folgende drei Formen der Gestaltungsmacht festhalten: die ökonomische Marktmacht, die kulturelle Diskursmacht und die politische Mobilisierungsmacht.

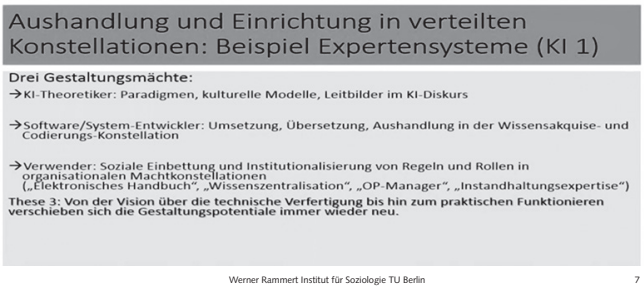
Auf der mittleren Ebene sozialer Gruppen und kultureller Bewegungen stellten wir fest, dass zumindest in dieser Anfangsphase kreative und alternative Konstellationen die Gestaltung und Richtung der Nutzung mitbeeinflussten. Die User – weibliche und ältere eingeschlossen – waren damals mehr als heute gefragt, selbst auszuprobieren, was man mit dem Computer zuhause und für den alltäglichen Gebrauch überhaupt sinnvoll machen kann. Zu dieser Zeit hat man Rezepte gesammelt, Briefmarkensammlungen geordnet, Taubenflugzeiten eingegeben, den Computer also mehr als Archiv benutzt. Wir interessierten uns eben auch für die kollektiven Formen der Computernutzung. So konnten wir für die damalige Zeit überraschend feststellen, dass Gruppen den Computer etwa für die Organisation einer alternativen Selbsthilfe-Initiative, für Reisezeitmessungen und Leistungsverbesserungen im Taubensportverein – man denke an heutige Selbst-Vermessungen – und auch für die Abstimmung der Instrumente untereinander in einer Musikband nutzten, so dass die Mitglieder allein üben und dann die Strips zu einem Stück zusammenführen konnten – was heute übrigens seit der Techno-Musik in der Musikszene eine ganz übliche Praxis ist. Wir fanden auch eine medizinkritische feministische Gruppe, die den PC für den Aufbau einer sozialen Bewegung nutzte, was heute ja überall üblich ist, etwa bei den virtuellen Patientenkollektiven.

Diese frühen Nutzungsformen haben die Gruppen, die User und die Computerbewegungen, zum großen Teil erst erfunden; die Hersteller, Entwickler und Gestalter in der Konstellation wussten davon noch nichts, nahmen diese Gestaltungseinflüsse von den Nutzern auf. An diesen Fällen zeigt sich, dass auch diejenigen über Gestaltungsmacht verfügen, die sich neue Nutzungsformen ausdenken, rumtüfteln und ausprobieren und dann diese von den üblichen Praktiken abweichenden Formen entwickeln und zu einer gesellschaftlich relevanten Praxis verbreiten.

Das bedeutet dann auch für die dritte Ebene der Mensch-Computer-Interaktion, dass in diesen persönlichen Nutzungskonstellationen die einzelnen Individuen ganz unterschiedliche Beiträge leisten und die Gestaltung in ganz verschiedene Richtungen der Nutzung vorantreiben können. Entgegen der damals gängigen Annahme waren nämlich – wie wir durch unsere erweiterte Untersuchung herausfanden – nicht alle Nutzer junge, männliche, blasse, pickelige ‚Nerds' mit ‚Maschinencharakter'. Da beobachteten wir schon eine Vielfalt von Nutzertypen und Nutzungsstilen: etwa die ‚Glasperlenspieler', die den Umgang mit dem PC eher als intellektuelle Herausforderung sahen, oder die ‚Lifestylisten', die sich mit allen möglichen ästhetisch designten Geräten und Zubehörteilen, etwa ‚slim' und ‚schwarz' gestylten Stationen und Kopfhörer ausstatteten. Da gab es auch die ‚Bastler' und ‚Schrauber', die immer wieder neue Teile einbauten und andere Konfigurationen ausprobierten und Freude am ‚Tunen' der Leistungsparameter hatten, ebenso auch ‚Aufstiegsorientierte', die sich am PC weiterbildeten, um die Kompetenzen später beruflich nutzen zu können.

Man kann zusammenfassen: Auch auf der persönlichen Ebene der Nutzungskonstellation bleiben User immer an der Ausgestaltung mitbeteiligt, vor allem in Einführungsphasen, in denen man neue Möglichkeiten der Nutzung erfinden und ausprobieren und auch vorliegende Formen um-konfigurieren kann; in späteren Phasen gibt es durch die eingespielten, institutionalisierten und technisch verfestigten Formen immer mehr Grenzen für eine echte Mit- und Umgestaltung. Allerdings besteht dann immer noch die Möglichkeit, auf den beiden anderen Ebenen der Konstellationsgestaltung, den institutionalisierten Konfliktarenen und der sozialen Bewegungen, Widerstand auszuüben und Verhandlungsmacht für eine Umgestaltung zu gewinnen: Kritik und Gegenpositionen kann eine Plattform gegeben werden, Gegenmacht kann durch politische und kulturelle Bewegungen verbreitet und organisiert werden; sie kann sich durch politisch-rechtliche Interventionen Gehör verschaffen, und sie zeigt noch stärkere Wirksamkeit, wenn sie durch gesellschaftliches Experimentieren mit technischen und ökonomischen Alternativen ihre Machbarkeit zeigt.

Beispiel 2: Organisationen und Professionen bei Expertensystemen



Beim zweiten Beispiel geht es um die Verteilung der Gestaltungsmacht von Akteursgruppen bei der Konstruktion und Anwendung von wissensbasierten Systemen [4]. Solche Expertensysteme wurden in den 1990er Jahren entwickelt, um das Expertenwissen von Instandhaltern in der Autoindustrie, von Sachbearbeitern in Versicherungsunternehmen oder von Herzchirurgen in einer Klinik, die Organtransplantationen durchführt, zu erheben und in wissensbasierte KI-Systeme zu überführen. Man ging damals davon aus, dass man das Wissen einer Domäne

in seiner Gesamtheit, Strukturierung und Regelbasiertheit akquirieren und dann mit Hilfe schlussfolgernder Mechanismen nachahmen könnte. Das menschliche Expertenwissen sollte auf diese Weise für die Organisationen sichtbar gemacht, rationalisiert, perfektioniert und dauerhaft angeeignet werden können, um die Verhandlungsmacht der fachlichen Experten und Professionsmitglieder einzuschränken und sie auf die Dauer zu ersetzen.

In vier verschiedenen Fällen haben wir als Techniksoziologen im Rahmen eines Verbunds für Technikfolgenabschätzung der Künstlichen Intelligenz an den Entwicklungs- und Gestaltungsprozessen konstruktiv teilnehmen und diese Prozesse und ihre Implikationen zugleich auch beobachten können. Wir haben uns gefragt: Wodurch wird der gesamte Konstruktionsprozess in seinem Verlauf – von der leitenden Idee der künstlichen Intelligenz über ihre technische Umsetzung beim Bau eines Expertensystems bis hin zur organisatorischen Implementation – tatsächlich beeinflusst? Es herrschte damals allgemein die Annahme vor, dass das wissenschaftliche Leitbild der KI die Anwendung unmittelbar bestimmte. Der kritische Diskurs um die Chancen und Grenzen der KI, der fast ausschließlich von Vertretern der KI, Linguisten und Philosophen, also nur mit spärlicher Beteiligung von empirisch forschenden Soziologen geführt wurde, verstärkte diese Position. Die zugrundeliegende Ansicht, dass Technik einfach als angewandte Wissenschaft aufgefasst werden könne, war allerdings nach dem Stand der Wissenschaftsforschung längst nicht mehr gültig. Wir konnten zwar feststellen, dass sich die Systemgestalter in ihren Begründungen und Rechtfertigungen für bestimmte Vorgehensweisen auf eines der verschiedenen Paradigmen künstlicher Intelligenz bezogen und dadurch in ihrer Arbeit motiviert wurden, sie in ihren wissensbasierten Systemen umzusetzen. Allerdings blieb im Prozess der Umsetzung davon wenig übrig.

Wendet man nämlich die Aufmerksamkeit weg von denjenigen Vertretern der KI, die den Diskurs in den wissenschaftlichen Medien und in der breiteren Öffentlichkeit maßgeblich gestalten, hin zu der zweiten Gruppe, welche die Expertensysteme für eine Domäne entwirft und vor Ort wirklich gestaltet, dann zeigen sich andere und komplexere Konstellationen von Gestaltungsmächten als in den KI-Diskursen. Die Software- und Systementwickler, die die Expertensysteme bauen, müssen sich mit den Professionen und Experten in den jeweiligen Wissensfeldern und auch mit den unterschiedlichen Organisationen auseinandersetzen. In der von Kenntnissen in empirischer Sozialforschung unberührten ‚Wissensakquise' versuchen sie das Fach- und Erfahrungswissen von Instandhaltern, von Herzchirurgen, Sachbearbeiterinnen oder Verkäufern komplex konfigurierter Produkte abzufragen und wie einfache Rohstoffe zu bergen. Dann folgt die Codierung des expliziten Wissens und der expliziten Regeln, dann die Umsetzung in Programme, etwa welche medizinischen Indizien für eine vordringliche, welche für eine immunverträgliche Herztransplantation sprechen, aber auch welche personalen Kriterien für eine erfolgreiche, nachhaltige oder besonders förderliche Durchführung einbezogen werden sollen. Letztlich sollte durch dieses wissensbasierte System die Reihenfolge der Herzoperationen objektiviert werden.

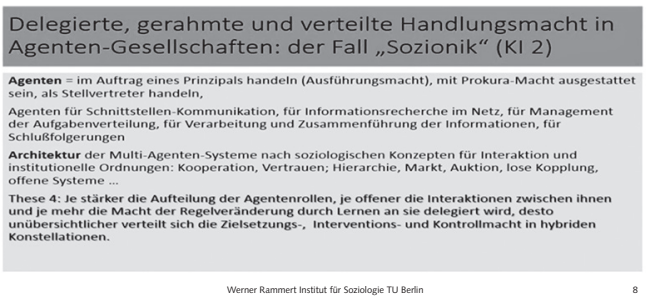
In dieser Konstellation setzen Informatiker nicht einfach das relevante Wissen der Experten um, in diesem Fall der besten Herzchirurgen und Transplantationsexperten. Wir konnten durch die Auswertung der Interviewprotokolle aller Sitzungen nachweisen, dass ein asymmetrischer Übersetzungsprozess stattgefunden hatte: Die Informatiker hatten gegenüber den Experten letztlich die entscheidende Gestaltungsmacht, weil sie den anderen ihren ‚Frame' aufgezwungen haben. Die Systementwickler können nämlich nur die explizit formulierten Wissensstücke und Wissensregeln benutzen, die sie formalisieren und als Algorithmen formulieren können. Immer, wenn Herzchirurgen etwas aus guten Erfahrungsgründen ambivalent formuliert hatten, mussten sie sich entgegen ihrer Haltung irgendwann auf eine eindeutige Form festlegen, weil die Informatiker aus programmierlogischen Gründen darauf bestanden. Auch heute noch spüren wir die Macht, die von fremden ‚Frames' ausgeht, etwa beim der Gestaltung des „Like"-Knopfs bei Facebook. Da hätte man sich gerne eine Konstellation gewünscht, bei der Soziologen oder Psychologen Gestaltungsmacht gehabt hätten. Mindestens eine symmetrische „I like not"-Option, wenn nicht gar eine Fünfer-Skala von „Sehr gut – Mittelgut – Unentschieden – Schlecht – Sehr schlecht" würden diese ärgerliche und zu emotionalen Steigerungs- und Verbreitungseffekten stimulierende Asymmetrie aus der Welt schaffen.

Schließlich entdeckten wir noch eine dritte Gestaltungsmacht, welche sich im Implementationsprozess neuer Techniken in den jeweiligen Organisationen, also auch beim Einsatz der Expertensystemtechnologie bemerkbar macht. Das sind die Verwender, die letztlich über Erfolg oder Misserfolg bestimmen. In unserem Fall waren es zwei industrielle Großunternehmen, ein Versicherungskonzern und eine Spezialklinik für Herztransplantation. In der Mehrzahl wurde hier letztlich nach der Enttäuschung über die großen Ansprüche und die geringe Performanz festgestellt, dass die Expertensysteme gescheitert sind. Das Expertensystem zum Konfigurieren von 700 Autoteilen für Verkauf und Produktionsplanung scheiterte in seiner Beratungsfunktion, wurde am Ende nur noch zum Ausdrucken des Beratungsergebnisses und für die Rechnung verwendet. Der OP-Manager für Transplantationen scheiterte, weil die Regeln und Indikatoren nicht so klar formuliert werden durften, die bestimmten, wann wer in der Warteschlange an die Reihe kommt. Ob man etwa Bundestagsabgeordnete vorziehen kann, wie die medizinischen Indikatoren gewichtet werden sollen, wie Alter, Gesundheitsverhalten oder Konkurrenz von Nachbarkliniken zu Buche schlagen, das war nicht klar zu priorisieren. Vorher hat man das mit dem Karteikasten besser gemacht, da konnte man einfach die jeweilige Patientenkarte umstecken. Das war zwar intransparent für die Patienten, folgte aber impliziten Fairness-Regeln, die man untereinander situativ aushandelte. Aber eine programmierte allgemeine Regel, dass Bundestagsabgeordnete um fünf Stellen vorrücken, das war und ist nicht akzeptabel.

Dieser Fall zeigt, dass die angemessene Mischung von Kriterien und ihre situationsgerechte Gewichtung nicht durch formalisierte Systeme vorgenommen werden können, sondern ein Aushandeln zwischen den beteiligten Akteuren und das Finden von Kompromissen erfordern. Der OP-Manager scheiterte zwar als Expertensystem der Klinik, wurde aber weiterhin vom mitentwickelnden Chirurg als persönliches Assistenzsystem verwendet, um seine eigenen Entscheidungen auf Lücken oder Fehler hin zu überprüfen. Bei der Versicherung sorgte die klare Überlegenheit der Managermacht dafür, dass das Expertensystem erfolgreich als Rationalisierungsinstrument eingesetzt werden konnte; beim mitbestimmten Großunternehmen wurde das Expertensystem für die Instandhaltung aufgrund der stark organisierten Gegenmacht abgelehnt.

Anhand der differenzierten Betrachtungen bei diesem Beispiel konnte gezeigt werden, dass sich auch im Verlauf der Entwicklung und Durchsetzung einer neuen Technologie der Informatik die Konstellationen jeweils verändern. Von der Vision einer KI über die Fertigung eines KI-Systems bis hin zum praktischen Funktionieren in einem Verwendungskontext verschieben sich die Gestaltungspotenziale und verändern sich die beteiligten Gestaltungsinstanzen.

Beispiel 3: Sozionik und verteilte Handlungsmacht



Als drittes Beispiel sei zum Schluss noch ganz kurz der Fall der Sozionik erwähnt. Er setzt einerseits das Paradigma der ‚Verteilten Künstlichen Intelligenz' fort, indem das Konzept der sozialen Verteiltheit mit Hilfe der Agenten-Technologie [5] auf die Gestaltung von Informatik-Systemen selbst angewandt wird. Er geht darüber noch hinaus, indem die Interaktivitäten zwischen den sozial und technisch verteilten Systemen als eine hybride Konstellation erforscht und gestaltet werden. Softwareprogramme werden nach dem Modell agiler und mobiler Agenten entwickelt: Es entsteht eine Agenten-Gesellschaft mit einer delegierten, gerahmten und verteilten Handlungsmacht. An die einzelnen, verteilt operierenden und koordinierenden Software-Agenten wird wirklich Macht abgegeben, wenn sie einen Auftrag ausführen. Vorbild sind die menschlichen Agenten, die es schon immer in Gesellschaften gegeben hat. Sie handeln im Auftrag eines Herrschers oder im Auftrag eines Unternehmens, erhalten die ‚Prokura'-Macht, was so viel heißt, dass sie Verträge abschließen und verbindlich unterschreiben können. In der Soziologie wird diese Beziehung als Stellvertreterhandeln bezeichnet. Dabei besteht grundsätzlich das ‚Principal-Agent'-Problem: Die stellvertretend Ausführenden haben Ausführungsmacht, entscheiden also, wie es gemacht wird. Sie müssen aber letztlich im Rahmen der Vorgaben durch den Principal bleiben.

Diese Ausführungs-Macht kann man ebenso an technische Systeme delegieren. Dort können Agenten unterschiedliche Aufgaben übernehmen, etwas überwachen, Grenzüberschreitungen melden, Informationen besorgen, vergleichen, auswerten, schlussfolgern und schließlich auch dem Nutzer in einer gewünschten Form kommunizieren. Außerdem können die verschiedenen Agenten miteinander kooperieren, Aufgaben an andere Agenten delegieren und die verteilten Operationen koordinieren. Schließlich kann man institutionenanaloge Strukturen dafür konstruieren, die sich an soziologischen Konzepten wie offene Gesellschaft, Gemeinschaft, Markt, hierarchische Strukturen, Plattformen, Öffentlichkeit orientieren, um dem verteilten Handeln eine Infrastruktur zu geben. Die Nutzung soziologischer Konzepte für die Gestaltung solcher Systeme macht analog zur Bionik die Sozionik aus. Die sozionischen Systeme sind gesellschaftsähnlich gebaut, aber sie sind für sich allein nicht Gesellschaft. Erst in der Perspektive der hybriden Konstellation werden sie zu einem Bestandteil der so verstandenen Gesellschaft.

Die Gestaltungs- und die Auftragsmacht liegt natürlich zunächst wie bei allen technischen Systemen bei den bisher beschriebenen gesellschaftlichen Konstellationen auf Seiten der menschlichen Akteure und der von ihnen institutionalisierten Regeln und Rahmen. Es bleiben weiterhin delegierte Macht und gefestigte Strukturen – so wie eingerichtet – bestehen. Aber sobald diese Systeme lernen, im Rahmen ihrer Aufträge selbständig ihre Regeln zu verändern, je weniger die Gründe für diese besseren Anpassungen nachvollzogen werden können und je mehr sie durch Deep-Learning-Schnittstellen über einen riesigen Datenschatz über das Verhalten aller Elemente, auch des menschlichen Verhaltens, verfügen, desto eher kann die Situation eintreten, dass sie irgendwie unbemerkt von uns und auch noch in unserem Auftrag die überlegene Gestaltungsmacht übernehmen. Auf jeden Fall kann sich dann auch die Zielsetzungsmacht verlagern, da vom System schon die Bewertung der Zielvarianten mitgeliefert und die optimalen Ziele schon vorstrukturiert sind. Es könnte sich die menschliche Interventionsmacht verringern, weil die komplexen Folgewirkungen gar nicht mehr kontrolliert werden könnten. Und es könnte sich ungewollt die Kontrollmacht zum System hin verschieben, da die menschlichen Akteure aus mangelnder Kompetenz und fehlender Kenntnis der komplexen inneren Entscheidungsabläufe dazu immer weniger in der Lage sein könnten.

Auf jeden Fall wird das System künstlicher Intelligenzen nicht eigenmächtig oder gar bewusst die Kontrolle übernehmen, wie es uns die Science-Fiction-Filme prophezeien. Umso mehr müssen wir in der Zukunft darauf achten, ab welchem kritischen Punkt und für welche Bereiche wir selbst die Gestaltungs- und Kontrollmacht aus Bequemlichkeit anderen sozialen Akteuren oder den smarten Systemen überlassen.

Was können wir für die zukünftige Gestaltung lernen?

Als erste Erkenntnis steht fest: Die Nutzer gestalten immer mit. Dafür wurden viele Beispiele gezeigt. Die Mitnutzung wird jedoch auch immer schwieriger gemacht, da Formate und fixierte Formen schon grundlegend den Freiraum einschränken. Anfangs beteiligt man die Nutzer, indem man sie zum Beispiel Beta-Versionen testen lässt, sogar im Netz Plattformen anbietet, an denen sich die Nutzer als Entwickler in offenen Foren einbringen können. So nutzt man natürlich auch viele junge Informatikerinnen und Informatiker aus, die ihr Wissen in eine vermeintlich freie und offene Community in der Hoffnung hineingeben, ihre höhere Kompetenz zu beweisen und dadurch in Ansehen und Stellung aufzusteigen. Von den Architekten wissen wir allerdings schon lange, dass nur ein geringer Prozentsatz auserlesen wird und dass die Illusion der kreativen Klasse auf eine spätere freie und sichere Betätigung ausgenutzt wird. Die Gründung eigener oder genossenschaftlicher Plattformen ist dazu eine bessere Alternative.

Mit Blick auf die untersuchten Fälle ist deutlich geworden, dass überall – ganz gleich ob absichtlich durch die Akteure oder unabsichtlich durch die gestalteten Strukturen – Verschiebungen

und Ungleichheiten der Gestaltungs- und Nutzungsmöglichkeiten entstehen: Offensichtlich gibt es in vielen Fällen – wie auch in anderen Bereichen der Gesellschaft – einen kapitalistischen Bias auf Kosten einer allgemeinen gesellschaftlichen Nützlichkeit, einen Management-Bias gegenüber den Beschäftigten, einen Mittelschicht-Bias zu Ungunsten der unteren Schichten, einen Männer-Bias zum Nachteil der Frauen, einen Jugend-Bias zu Lasten der Älteren und einen ‚Urbanen Bias' gegenüber der Landbevölkerung. Ob schon in der Konstruktion oder erst in der Verwendung: überall, soweit ich das bisher beobachten konnte, schaffen und verstärken die Systeme vorhandene Ungleichheiten.

Weiterhin kann festgehalten werden: Es sind immer mehr und verschiedene Akteure am gesamten Prozess der Entwicklung, Gestaltung und Nutzung beteiligt. Auch dort ist folglich die verteilte Machtgestaltung zu beachten. Es sind die jeweiligen institutionellen und organisatorischen Rahmungen, die verschiedenen Leitmodelle wie Paradigmen und auch die unterschiedlichen Interessen der Professionen zu reflektieren, deren Wissen nicht nur sachlich neutral abgebildet, sondern angeeignet wird, um es für die Rationalisierung oder Substitution professioneller Arbeit zu verwenden. Für die Einschätzung der Organisationskontexte gilt zu klären, ob sie die Prozesse zentralisieren, ob sie eher für eine offene Nutzung votieren, ob sie alle Akteure daran partizipieren lassen und ob das gesamte Vorhaben auch für Außenstehende Kunden, Klienten und betroffene Bürger transparent gemacht wird.

Und die vierte Erkenntnis betont den Sachverhalt: Die Technik selbst gestaltet mit. Damit sind alle aufgewiesenen Gestaltungsmächte gemeint: die an einzelne Agentenprogramme delegierte Macht, die an Architekturen delegierte strukturelle Macht und die in Schnittstellen eingeschriebene und vorschreibende Macht. Sie sorgen dafür, dass die Nutzung sich in einem begrenzten Rahmen abspielt und auf die Dauer auch zu bestimmtem Gestalten führt, die sich wiederholen und verfestigen können, wie auch Institutionen und Gesellschaft, Normen und Wertvorstellungen durch Wiederholen von Handlungen und Interaktionen sich festigen. Wenn man sie nicht wiederholt, dann verschwinden sie. Dieser Wandel ist normal für Gesellschaften. Bei der Technik ist er begrenzt und muss bewusst initiiert und gestaltet werden: Es ist also im Rahmen der hybriden Konstellation verteilter Gestaltungsmacht letztlich darauf zu achten, wie weit verschiedene Techniken die angesprochenen Möglichkeiten eröffnen, aber auch sinnvoll mit guten Gründen schließen, um nicht Ungleichheiten entstehen zu lassen. Ebenso wenig sollten ungewollte Verselbständigungen zugelassen werden, seien sie von bestimmten Akteuren in ihrem Interesse absichtlich gewollt oder auch durch zugelassenes Lernen und eigenständiges Anpassen entstanden.

Technisches Gestalten geschieht in hybriden Konstellationen, auf Menschen, Medien, Maschinen und Programme verteilten Handelns. Demzufolge ist auch die Verantwortung für bestimmte Formen und Folgen der Gestaltung kaum noch einzelnen Akteuren oder Strukturelementen zuzurechnen. Es gilt die verschiedenen Verteilungen der Gestaltungsmacht im Rahmen unterschiedlicher Konstellationen genauer zu analysieren.

Referenzen

[1] Weizenbaum J (1978) Die Macht des Computers und die Ohnmacht der Vernunft. Frankfurt/M.: Suhrkamp

[2] Woolgar S (1990) Configuring the user: the case of usability trials; in: J. Law (ed): A Sociology of Monsters: Essays on Power, Technology and Domination, Vol.38, Sociological Review Monograph Series, 58-99

[3] Rammert W, Böhm W, Olscha C, Wehner J (1991) Vom Umgang mit Computern im Alltag. Fallstudien zur Kultivierung einer neuen Technik. Wiesbaden: Westdt. Verlag

[4] Rammert W, Schlese M, Wehner J, Weingarten R (1998) Wissensmaschinen. Zur Konstruktion eines technischen Mediums – Das Beispiel Expertensysteme. Frankfurt/M.: Campus

[5] Rammert W (2000) Die Gesellschaft der „Heinzelmännchen". Zur Soziologie technischer Agenten und Systeme verteilter künstlicher Intelligenz; in: Malsch T Hg (2000) Sozionik. Zur Erforschung und Gestaltung artifizieller Gesellschaft. Berlin: Sigma

[6] Rammert W (2003) Technik-in-Aktion: Verteiltes Handeln in soziotechnischen Konstellationen; in: Christaller T, Wehner J Hg (2003) Autonome Maschinen. Berlin: Sigma

[7] Rammert W (2008) Die Macht der Datenmacher in der fragmentierten Wissensgesellschaft; in: Gaycken S, Kurz C Hg. (2008) 1984.exe: Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. Bielefeld: transcript

[8] Rammert W (2015) Unsicherheit trotz Sicherheitstechnik? Das Kreuz mit komplexen Konstellationen; in: Zoche P, Kaufmann S, Arnold H Hg (2015) Sichere Zeiten? Gesellschaftliche Dimensionen der Sicherheitsforschung. Berlin: LIT

Anmerkung

1 *Der Text beruht auf einem Vortrag auf der FIfFKon 2018. Für den Mitschnitt und eine transkribierte Zusammenfassung bedanke ich mich bei einem anonymen Helfer aus dem Organisations-Team.*

Werner Rammert

Werner Rammert ist ein Pionier der Technik-Soziologie und Professor am Institut für Soziologie der TU Berlin. Dort hat er einen Studiengang *Soziologie technikwissenschaftlicher Richtung* und das DFG-Kolleg *Innovationsgesellschaft heute* begründet. 2002 hat er mit Ingo Schulz-Schaeffer das Buch *Können Maschinen Handeln?*, 2006 mit Cornelius Schubert Zur *Mikrosoziologie der Technik* herausgegeben. 2016 ist sein grundlegendes Buch *Technik – Handeln – Wissen* erschienen. U. a. hat er mit Informatikern zu Menschen-zentrierter Kommunikation, Sozionik, Technikentwicklung und -folgen geforscht und dabei u. a. mit der TA-SWISS und der Akademie für Technikwissenschaften zusammengearbeitet.

Besser steuern durch Daten? Zur Performativität soziotechnischer Systeme und der Quantifizierung der sozialen Welt

Verschriftlichung des Vortrags von Judith Hartstein, Anne K. Krüger und Felicitas Hesselmann

Während die Einen von der Lösung gravierender Menschheitsprobleme träumen, warnen Andere vor einer allumfassenden Überwachung durch die neuen Möglichkeiten soziotechnischer Systeme. Doch steht sowohl hinter der Utopie des Solutionismus als auch hinter der Dystopie totaler Überwachung die Frage, warum, wofür und wie die dazu notwendigen Daten überhaupt produziert und genutzt werden.

Lassen sich durch viele neue Daten jetzt ganz viele alte Probleme lösen? Oder werden wir alle von den Daten gegen unseren Willen fremdbestimmt? In ihrem Beitrag gehen die Autorinnen aus einer soziologischen Perspektive heraus den Problemen der neuen Möglichkeiten von Datenproduktion und -nutzung nach und fragen danach, was passiert, wenn wir soziale Wirklichkeit nur noch durch die Daten sehen, die durch soziotechnische Systeme produziert werden.

Judith Hartstein, Anne K. Krüger und Felicitas Hesselmann steuerten mit ihrem Vortrag eine soziologische Perspektive auf die Möglichkeiten soziotechnischer Systeme bei, da sie im Austausch zwischen Sozialwissenschaftlerinnen und Informatikerinnen große Potenziale sehen. Die drei Wissenschaftlerinnen forschen zu Bewertungsverfahren in der Wissenschaft am Deutschen Zentrum für Hochschul- und Wissenschaftsforschung beziehungsweise der Humboldt-Universität Berlin und dem Lehrbereich Wissenschaftsforschung. Da aber gerade diese Frage nach Bewertungsverfahren heutzutage eine hohe Relevanz in sehr vielen anderen Bereichen hat, behandelte der Vortrag generalisiert Fragen, die Kategorisierung, Klassifizierung und Quantifizierung der sozialen Wirklichkeit ansprechen, anstatt sich konkret auf das Thema Wissenschaft zu beziehen.

Anne K. Krüger am Rednerpult

Gerade vor dem Hintergrund der wachsenden Möglichkeiten, vielerlei Daten mittels neuer soziotechnischer Systeme für die NutzerInnen wissentlich oder unwissentlich zu erzeugen, liegt der Ausgangspunkt in den Fragen: Warum, wofür und wie werden heutzutage eigentlich Daten produziert? Konkret ausformuliert bedeutet das: Erstens, was sind die aktuell gesehenen Probleme über die Daten produziert werden? Zweitens, welche Lösung wird mit der Nutzung dieser Daten verbunden? Und drittens, wie werden diese Daten überhaupt erzeugt?

Es wird gezielt von der Datenproduktion und nicht von der Datenerhebung gesprochen, weil nicht davon ausgegangen wird, dass ein Datenschatz irgendwo herumliegt und nur ermittelt oder gehoben bzw. erhoben werden muss, sondern, dass jegliche Form der Datenerhebung aus der Wirklichkeit immer auch ein Prozess der sozialen Konstruktion von Wirklichkeit ist. Dahinter steht insgesamt die allgemeinere und für uns alle relevante Frage: Wenn wir Wirklichkeit nur noch durch die Daten sehen, die durch soziotechnische Systeme produziert werden, was für eine Wirklichkeit sehen wir dann überhaupt noch? Anne Krüger unterfüttert die Aussage mit einem Beispiel: Auf der EASST, das ist die wichtigste Wissenschaftsforschungskonferenz Europas, hat sie zwei Vorträge zum Einsatz von mobilen Devices in der Medizin gehört. Der eine Vortrag, von der Finnin Maiju Tanninen, stellte die Perspektive von Versicherungen dar. Versicherungen versuchen durch den Einsatz von solchen Devices wie z. B. Fitnessarmbändern ihre Versicherten dazu zu animieren, sich gesündere Verhaltensweisen anzueignen. Gleichzeitig verfolgen sie damit natürlich aber auch das eigene Ziel, Daten über das Gesundheitsverhalten von bestimmten Personengruppen zu erzeugen und auf diese Weise dann auch Risikoprofile zu entwickeln. Das heißt, sie versuchen einerseits mittels dieser durch Fitnessarmbänder produzierten Daten das individuelle Verhalten ihrer Kunden zu erfassen. Andererseits benutzen sie diese Daten, um daraus über die Einzelperson hinaus ein allgemeines Bild dessen zu generieren, wie gesundheitsbewusst oder gesundheitsschädlich sich Menschen mit einem bestimmten Profil verhalten. Sie produzieren also Daten, um darauf bestimmte Aussagen über die Wirklichkeit zu treffen, auf denen sie dann ihr eigenes strategisches Handeln aufbauen. Es gibt dabei zwei Probleme: Erstens, dass Menschen diese technischen Devices sehr unterschiedlich benutzen. Der eine sehr regelmäßig, bei der anderen ist ständig die Batterie leer, was natürlich bedeutet, dass die Produktion der Daten auf jeweils ganz unterschiedlichen Voraussetzungen basiert, die allerdings nicht mit erhoben werden. Das zweite Problem sind die technischen Begrenzungen der Möglichkeiten der Datenproduktion, die beispielsweise dazu führen können, dass zurückgelegte Distanzen von einem Fitnessarmband erfasst werden können, auf dem Laufband zurückgelegte Kilometer aber nicht. Es gibt also eine unvermeidbare Abweichung zwischen Modell und Realität.

Der andere Vortrag kam von der Juristin Margo Bernelin. Auf Grundlage von Fällen in Frankreich und Großbritannien hat sie im Vortrag deutlich gemacht, dass es Überlegungen gibt, Menschen im Rahmen staatlicher Gesundheitsversorgung dazu zu verpflichten, solche Devices zu benutzen, sofern sie medizinisch indiziert sind. Die produzierten Daten sollen als Nachweis dienen, dass die Person sich auch an ärztliche Verordnungen hält. Das heißt dann erstens, dass die bis dato vertrauliche Kommunikation zwischen Ärztin und Patient aufgehoben wäre, weil auch andere Personen Einsicht in diese Art der Daten bekommen. Zweitens ist jedoch auch alles andere als klar, wie belastbar und damit aber auch, wie justiziabel diese Daten sind, die von diesen technischen Geräten produziert werden. Kann man dann also zum Beispiel tatsächlich Personen verklagen, die sich nicht gesundheitlich adäquat verhalten und damit dann das öffentliche Gesundheitssystem ausgebeutet zu haben, wenn das die Datenlage so zeigt? Hieran verdeutlicht sich die Gefahr, dass technische Lösungen als verpflichtend eingeführt werden und damit Aussagen über die Wirklichkeit treffen, auch wenn sie nicht zufriedenstellend funktionieren.

Im aktuellen Diskurs werden sowohl in der Forschung als auch in gesellschaftlichen Debatten vor allem zwei Narrative bedient. Es gibt einerseits die Dystopie einer allgegenwärtigen Überwachung und eines allumfassenden *Social Sortings*, das die individuellen Lebenschancen unmittelbar bestimmt. Andererseits wird aber auch über nichts Geringeres gesprochen, als über die Utopie der ultimativen Lösung gravierender Probleme der Menschheit. Um diese zwei Narrative bildlich zu machen, verweist Anne Krüger auf die Serie *Black Mirror*. Im Vortrag wird ein kurzer Ausschnitt aus der Folge „Abgestürzt" – oder „Nosedive" auf Englisch – gezeigt. In dieser Folge geht es um Lacie. Lacie lebt in einer Welt, in der sich Menschen permanent wechselseitig bewerten und sozialer Aufstieg tatsächlich nur durch positive Bewertungen möglich wird. Denn an diesen persönlichen Bewertungsscore sind alle möglichen Formen von Lebenschancen geknüpft, wie zum Beispiel die Traumwohnung, die Lacie sehr gerne hätte, aber die sie erst ab einem persönlichen Score von 4,5 erreichen kann. Deshalb lässt sie sich beraten. Der Ausschnitt demonstriert, wie permanent die Bewertung jeglichen Handelns sowohl als externe Überwachung des eigenen Handelns in Form eines für jeden einsehbaren Punktesystems wirkt, als auch zur Internalisierung der Einhaltung bestimmter kollektiver Normen führen kann. An den französischen Soziologen und Philosophen Michel Foucault anschließend drängen sich hier Überlegungen in puncto einer Disziplinargesellschaft auf, wonach das Wissen um eine externe permanente Beobachtung zu einer internalisierten Überwachung durch sich selbst führt. Die Beobachtung und Bewertung jeglichen Handelns ist gleichzeitig durchdrungen von bestimmten Vorstellungen davon, was gutes und richtiges Handeln ausmacht. Lacie hat diese Vorstellung vollkommen internalisiert und ihr individuelles Handeln vollkommen darauf ausgerichtet. Es zeigt sich außerdem, dass diese permanente Selbstkontrolle vor dem Hintergrund von Prozessen dieses schon anfangs angesprochenen Kategorisierens und Klassifizierens erfolgt. Im Videoausschnitt wird deutlich, dass dieser Prozess sowohl das festlegt, was bewertet wird – also eine bestimmte Form des sozialen Umgangs miteinander – als auch das, wofür der Bewertungsscore einer Person dann wichtig ist. Im Falle von Lacia die Wohnung, die sie erst ab 4,5 bekommen kann. Es wird nicht nur festgelegt, was bewertet wird, sondern auch, wie es bewertet wird.

Dass das individuelle Verhalten klassifiziert wird, wird besonders deutlich in dem Moment, in dem Lacie ihrem Kollegen begegnet, dem aufgrund fehlender Punkte der Eintritt zum Arbeitsplatz verwehrt wird. Er bittet um eine positive Bewertung von Lacie, die sie ihm jedoch verweigert, da sie Angst vor negativen Konsequenzen für ihren eigenen Score hat. Zur Wiederholung: der Versuch der Steuerung hin zu einer besseren Gesellschaft liegt erstens darin zu definieren, worauf geschaut und was bewertet werden soll, und zweitens in der Festlegung der Bewertung selbst, die das jeweilige Handeln dann in besser und schlechter klassifiziert. In dem Videoabschnitt wird auch deutlich, dass Menschen klassifiziert und in ihren Lebenschancen determiniert werden, was der kanadische Soziologe David Lyon als Social Sorting bezeichnet. Es geht hier gerade nicht um Taten oder individuelle Eigenschaften, sondern den Hintergrund der eigenen Herkunft. Durch ihren Hintergrund hat Lacie wenig Kontakte zu hoch bepunkteten Menschen, wodurch sie Probleme hat, Bewertungen zu bekommen, die ihr dann selber zum sozialen Aufstieg verhelfen könnten.

Das Entscheidende an diesen Bewertungen ist, dass wir selbst beginnen, unser Handeln auf die vorgegebenen Kategorien und Klassifikationsschemata anzupassen. Der Soziologe Ulrich Bröckling hat dies als unternehmerisches Selbst bezeichnet. Er zeigt am Beispiel des *Total Quality Managements*, dass das Individuum nicht nur von außen dazu gezwungen wird sich bestimmten Normen zu unterwerfen, das heißt, sich normieren zu lassen, sondern vielmehr dazu gebracht wird, selbst nach einer Anpassung an die aktuell vorherrschenden Normen zu streben. Das heißt, sich selbst permanent zu optimieren und nach einer Verbesserung der eigenen Fähigkeiten und Möglichkeiten entsprechend der vorherrschenden Normen zu streben. Bröckling formuliert das sehr schön: „Der Unternehmer seiner Selbst führt sein Leben als permanentes Assessment-Center."

Auf die Spitze getrieben wird diese Selbstoptimierung durch Technologien, die ein permanentes Self-Tracking ermöglichen. Die selbst ernannte *Quantified-Self*-Bewegung spricht davon, dass es einerseits um die Ermächtigungen über das Wissen über sich selber geht, das man dann durch das permanente Self-Tracking ermöglicht. Ihr Slogan lautet dementsprechend „Self Knowledge through Numbers". Andererseits wird hier jedoch auch die Möglichkeit geschaffen, dieses Wissen über sich selbst immer auch mit den Kennzahlen anderer zu vergleichen. Die Vortragende Anne Krüger stellt diese Möglichkeit des Vergleiches als das zentrale Element heraus. Denn wie bei Lacie aus *Black Mirror* gesehen wurde, ermöglicht die Umwandlung der Bewertung ihrer Handlungen in eine allgemeine Bewertungsskala überhaupt erst das Vergleichen mit anderen Leuten, ganz unabhängig davon, ob Startvoraussetzungen oder Eigenschaften ähnlich sind. Die Soziologin Bettina Heintz spricht hier von der Gleichheitsunterstellung bei gleichzeitiger Differenzbeobachtung. Das heißt, dass ganz unterschiedliche Dinge miteinander vergleichbar gemacht werden, indem sie in einem ersten Schritt derselben Kategorie zugehörig definiert werden. Es wird damit Gleichheit unterstellt, die die Basis für jeden Vergleich stellt. Angewendet auf das Beispiel des Self-Tracking durch Gesundheitsdevices, bedeutet das, dass angenommen wird, dass die dadurch produzierten Daten alle vor demselben Nutzungshintergrund entstanden wären, was in der vorher erwähnten Studie als falsch herausgestellt wurde. Wichtig ist es, es mit ver-

gleichbaren Einheiten zu tun zu haben, bzw. eine Vergleichbarkeit zu behaupten, denn nur dann kann man versuchen, Differenzen und Unterschiede zu beobachten.

Vergleichbarkeit ist dabei am einfachsten gegeben, wenn spezifische Handlungen und Eigenschaften in Zahlen ausgedrückt werden können. Dabei kann es sich dann entweder um den konkret erfassbaren Zahlenwert handeln, z. B. „Wie viele Schritte bin ich heute gelaufen?" oder es verschwinden Primärdaten hinter einem bewertenden Zahlenwert, der nicht mehr direkt interpretierbar ist im Bezug auf was beobachtet, gemessen oder gezählt wurde. Dieser Bewertungsscore von Lacie ist dafür ein sehr gutes Beispiel. Der Bewertungsscore, der sie mit anderen Personen vergleichbar macht, ist nicht klar in die einzelnen Handlungen aufschlüsselbar, die sie über den Tag vollzogen hat, sondern kommt auf unklare Weise zustande. Was hier geschieht – Estland und Stevens haben dazu geforscht – wird als Quantifizierung bezeichnet. Quantifizierung meint die Überführung qualitativer Eigenschaften in quantitative Metriken. Die soziale Wirklichkeit wird in Zahlen übersetzt, aus denen wiederum neue Zahlen dann generiert werden können.

Und vor diesem Hintergrund geht es nun um die soziotechnischen Systeme und die aktuellen Entwicklungen. Soziotechnische Systeme erfordern oftmals genau diesen Prozess der Quantifizierung und leisten damit den Möglichkeiten dieses klassifizierenden Vergleichens entscheidenden Vorschub. Die Systeme basieren erstens darauf, Daten zu produzieren, indem sie bestimmte Dinge zählen oder in Zahlen umwandeln, und zweitens sind sie gleichzeitig in der Lage, diese Daten auch sofort selbst zu nutzen, indem sie eine Klassifizierung vornehmen. Das heißt, produzierte Primärdaten anhand vorgegebener automatisierter Verfahren umzuwandeln in Daten, mit denen dann ein Wert dieser Primärdaten ermittelt wird. Der von Ihnen produzierte Zahlenwert wird auf diese Weise sofort in eine Form der quantitativen Bewertung überführt. Das lässt erkennen, warum diese gesellschaftliche Entwicklung so wirkmächtig ist. Anne Krüger sieht dort einen mittlerweile vollständig als selbstverständlich institutionalisierten Glauben an eine objektive Erhebung und Bewertung von Leistung durch die Umwandlung von individuellen Handlungen in miteinander vergleichbare Zahlen. Dieser institutionelle Glaube an die Objektivität von Zahlen trifft aktuell auf technische Möglichkeiten zu, mittels derer nicht nur massenhaft Daten produziert werden, um individuelles Handeln erfassbar und abbildbar zu machen, sondern gleichzeitig auch noch die Möglichkeiten vorliegen, Rückschlüsse über spezifische Zusammenhänge und gesellschaftliche Muster zu ziehen. Diese haben dann wiederum unmittelbaren Einfluss darauf, was wir als soziale Wirklichkeit wahrnehmen. Die Wahrnehmung unserer Wirklichkeit hängt dementsprechend ganz fundamental mit dieser Form der Datenproduktion zusammen, welche gleichzeitig wieder darauf wirkt, wie wir Wirklichkeit erleben. Das schürt einerseits Ängste hinsichtlich einer allumfassenden Überwachung und Erfassung des Einzelnen, andererseits – und das ist eigentlich so interessant an dieser Entwicklung – werden damit auch Hoffnungen auf neue Nutzungs- und Steuerungsmöglichkeiten verknüpft.

Nun soll es um die zweite Vision gehen, wie bereits angekündigt: die Utopie. Es wird erneut ein kurzer Videoausschnitt aus einem Interview mit Mark Zuckerberg vom 16. August 2016 im *Y Combinator* gezeigt. Der *Y Combinator* ist ein kalifornisches Gründerzentrum, das gegen eine gewisse Beteiligung versucht, Internet-Start-ups zum Durchbruch zu verhelfen. Mark Zuckerberg sieht verschiedene Herausforderungen für die nächsten zehn, zwanzig Jahre. Er spricht davon, dass erstens mehr digitale Vernetzung hergestellt werden muss, um die größten Herausforderungen der Welt zu meistern, wodurch dann allen die Chance gegeben werde, sich daran zu beteiligen. Weiterhin spricht er von einem Mehr an Künstlicher Intelligenz und beschreibt wie das, was Sie bei Facebook entwickeln, auch dazu genutzt werden kann, um Leben zu retten. Sein Beispiel ist hier eine selbstlernende Applikation zur Bestimmung von Hautkrebs, durch die jede Person auf der Welt zur besten Ärztin werden könne. Zuckerberg spricht also davon, dass die neuen technischen Möglichkeiten dazu führen werden, Menschenleben zu retten und die Herausforderungen der Zeit zu meistern. Gravierende Menschheitsprobleme können durch neue Technologien angegangen und beseitigt werden. Er zeigt sich außerdem etwas betroffen davon, dass es Kritiker gibt, die diese Aussicht nicht teilen. Einer dieser Menschen, die sich sehr kritisch mit den Heilsversprechen neuer Datenproduktions und -nutzungsmöglichkeiten auseinandergesetzt haben, ist der Publizist Evgeny Morozov. Morozov spricht vom sogenannten *Solutionismus*. Er sagt, dass es nicht allein die Lösungen sind, die Widerspruch hervorrufen, sondern bereits die Definition der Probleme, für die diese Lösung gedacht sind. Morozov hat vor diesem Hintergrund auch sich einer bestimmten Terminologie der *wicked problems* bedient, die aus den Verwaltungswissenschaften der 1970er Jahre stammen. Bereits damals wurde diese Terminologie dazu genutzt, um der damaligen Planungs- und Steuerungseuphorie und -utopie in gewisser Weise entgegenzuwirken. *Wicked problems* sind nach den Planungswissenschaftlern Horst Rittel und Melvin Webber als gravierend empfundene, komplexe soziale Problemlagen zu definieren, die tatsächlich nicht bis ins letzte Detail abschließend definiert werden können. Sie deuten damit an, dass das, was als Problem betrachtet wird, von der jeweiligen Perspektive abhängt, von der das Problem betrachtet wird. Unterschiedliche Personen sehen dementsprechend unterschiedliche Probleme bzw. betrachten bestimmte Sachverhalte auf ganz unterschiedliche Weise, woraus dann unterschiedliche Problemdefinitionen und natürlich auch Lösungsansätze resultieren. Die sogenannte Flüchtlingskrise oder auch das, was aktuell im Hambacher Forst passiert, sind dafür sehr gute und aktuelle Beispiele. Morozovs Kritik unter der Bezeichnung eines Solutionismus ist von den Soziologen Oliver Nachtwey und Timo Seidl aufgegriffen worden. Sie haben einschlägige Dokumente aus der High-Tech-Industrie analysiert und bestätigen das, was Morozov in seiner Kritik diagnostiziert. In dem von Morozov als Solutionismus bezeichneten Konstrukt sehen sie eine neue Form der Rechtfertigung eines kapitalistischen Wirtschaftssystems. Sie stellen dar, dass neben Zuckerberg beispielsweise auch Googles Eric Schmidt oder Teslas Elon Musk Heilsversprechen auf Grundlage neuer Formen der Datenproduktion und Datennutzung treffen. Google beschreibt es zum Beispiel als „Produkte zu entwickeln, die das Leben so vieler Menschen wie möglich verbessern." Diese neue Rechtfertigungsordnung im Kapitalismus trägt dazu bei, dieses Wirtschaftssystem auch unter den gegenwärtigen Bedingungen gegenüber seinen Kritikern aufrechtzuerhalten. Während wir so vordergründig eine Argumentation sehen, die auf die Lösung gravierender Menschheitsprobleme, zum Beispiel im Gesund-

heitswesen abhebt, wird dahinter immer das Problem zu hoher Kosten diagnostiziert. Es geht also um Kosteneinsparung, die einerseits durch neue Mittel und Wege der Datenproduktion und Datennutzung erreicht werden sollen. Gleichzeitig wird aber das Ziel einer besseren Gesundheit aller Menschen damit gerechtfertigt, dass dadurch geringere Kosten anfallen. Die Weltverbesserung bemisst sich demnach immer an dem ökonomischen Benefit, der dahinter steht. Denn nicht zuletzt kommen neue Technologien zur Rettung der Menschheit nur auf den Markt, wenn in ihre Produktion investiert wird und das hängt natürlich davon ab, ob sich diese Technologien auch ökonomisch rentieren. Der Solutionismus legt zudem nahe, dass eigentlich jegliche Formen der gesellschaftlichen Probleme auf technologische Probleme reduziert werden könnten. Das Interessante daran ist, dass es sich hierbei um eine Steigerung dessen handelt, was in der Literatur bereits als evidenzbasierte Politik beschrieben wurde. Evidenzbasierte Politik duldet in gewisser Weise keinen Widerspruch und setzt keine von politischen Wertvorstellungen getriebene Diskussion voraus, da evident und eindeutig ist, wo Probleme liegen und daraufhin alternativlos, was dagegen getan werden muss. Das Interessante ist, dass, während evidenzbasierte Politik zumindest noch vorgab, sich aus dem Wissen und den Erkenntnissen wissenschaftlicher ExpertInnen abzuleiten, hier wiederum argumentiert wird, dass die Daten selbst für sich sprechen. Sie müssen nicht erst in wissenschaftlichen Studien erhoben werden, sondern werden von den objektiv arbeitenden digitalen Technologien präsentiert und vorgegeben. Die Definition des Problems und die Suche nach entsprechenden Lösungen wird damit weitgehend dem politischen Diskurs tatsächlich entzogen.

Die aktuellen Möglichkeiten der Datenproduktion und Datennutzung spannen damit sowohl den Raum für Dystopien einer allumfassenden Überwachung als auch für Utopien der Lösung gravierender Menschheitsprobleme auf. Doch liegen hier tatsächlich zwei gravierende Probleme vor, die einerseits die Dystopie der allumfassenden Überwachung ein bisschen entschärfen – oder vielleicht sogar in ihren Konsequenzen eher noch verschärfen können – und andererseits aber auch die Utopie der Lösung der Menschheitsprobleme in der Definition von Problem und Lösung vor Herausforderungen stellen. Erstens, das Problem der Daten ohne Erkenntnisgewinn. Morozov spricht hier zum Beispiel von Googles *Enlightened Business* hinter dem der Anspruch steht: „Die Informationen der Welt zugänglich und nutzbar zu machen für alle Menschen zu jeder Zeit." Dieses Verständnis von Datenproduktion als Wissensproduktion wird bereits als neuer Empirismus diskutiert. Es stellt sich hier zudem die Frage, welches Wissen tatsächlich in diesen Daten steckt und durch sie dann auch sichtbar gemacht wird. Denn nur, weil Daten existieren, die Informationen bereitstellen, heißt es noch lange nicht, dass tatsächlich auch bekannt ist, was aus diesen Daten erfahrbar ist. Der Philosoph Byung-Chul Han spricht deshalb auch von Big Data als digitalem Dadaismus. Auf das zweite Problem, die Performativität soziotechnischer Systeme, ist Werner Rammert schon intensiv eingegangen. Es stellt sich die Frage nach Gestaltungsfreiheit und Machtmustern in soziotechnischen Systemen. Bei soziotechnischen Systemen geht es immer um die Verbindung von Mensch und Maschine. Einerseits programmiert der Mensch seine Wertvorstellungen, Sichtweisen und Machtverhältnisse in die automatisierten Verfahren von Maschinen hinein. Dadurch geben dann technische Systeme vor, wie Wirklichkeit überhaupt erfasst und Tätigkeiten ausgeführt werden können. Daraus entfaltet sich eine gewisse Eigendynamik, indem die Systeme Sachen ermöglichen oder nicht ermöglichen, mit denen Nutzer und Nutzerinnen umgehen müssen und darauf reagieren. Diese beiden Formen der Performativität soziotechnischer Systeme beeinflussen also maßgeblich, wie Daten produziert und ausgewertet werden können und dabei müssen wir uns abermals davon verabschieden, dass wir es hier mit objektiven Daten zu tun haben. Wir müssen anerkennen, dass sowohl der Mensch als auch die technischen Systeme selbst einen entscheidenden Einfluss auf die Datenproduktion und Datennutzung haben. Aufkommende Steuerungsphantasien der Gesellschaft sind demnach übersteigert und müssen debattiert werden. Andererseits greifen dadurch auch Dystopien einer totalen Durchleuchtung und Steuerbarkeit der Individuen zu kurz, weil auch hier schlussendlich begrenzt ist, was in Daten abgebildet werden kann. Das große Problem ist, dass diese neuen Technologien trotzdem genau dafür genutzt werden und maßgeblichen Einfluss darauf ausüben, wie die soziale Wirklichkeit wahrgenommen wird und welche Entscheidungen getroffen werden. Und dies geschieht trotz des bekannten Risikos einer problematischen Darstellung der Wirklichkeit aufgrund von den Algorithmen eingeschriebenen Mo-

Judith Hartstein, Felicitas Hesselmann und Anne K. Krüger

Judith Hartstein hat Wirtschaftsmathematik an der Hochschule für Technik und Wirtschaft Berlin und Wissenschaftsforschung an der Humboldt-Universität zu Berlin studiert. Sie arbeitet am Deutschen Zentrum für Hochschul- und Wissenschaftsforschung (DZHW) im Bereich Wissenschaft und Gesellschaft zu Regimen der Wissensproduktion (wie Zitier-Kartellen), Bewertungen und Forschungsfolgen als Governance-Instrumenten.

Felicitas Hesselmann ist am Deutschen Zentrum für Hochschul- und Wissenschaftsforschung und an der Humboldt-Universität zu Berlin beschäftigt und forscht dort zu wissenschaftlichen Bewertungsverfahren. In Ihrem Promotionsprojekt setzt sie sich aus einer devianzsoziologischen Perspektive mit Umgangsweisen und Reaktionen auf wissenschaftliches Fehlverhalten auseinander.

Anne K. Krüger arbeitet als promovierte Soziologin an der Humboldt-Universität zu Berlin und am Deutschen Zentrum für Hochschul- und Wissenschaftsforschung. Im Mittelpunkt ihrer Forschung steht die theoretische und empirische Analyse der Zunahme und Veränderung von Bewertungsprozessen und ihrer gesellschaftlichen Konsequenzen.

dellen oder zugrunde liegender Datenlage. Trotzdem wird auf diese Form der Datenproduktion und Datennutzung weiterhin als Ausgangspunkt für ökonomische, soziale oder auch politische Entscheidungen zurückgegriffen.

Zum Schluss wird noch einmal der Austausch zwischen Soziologie und Informatik in den Vordergrund gestellt: In drei wesentlichen Punkten wird mehr Zusammenarbeit benötigt. Erstens geht es darum, konkrete Verfahren der Datengenerierung und -verarbeitung für SozialwissenschaftlerInnen begreifbar und zugänglich zu machen, damit diese aufzeigen können, wo mit welchen Konsequenzen Probleme durch die digitale Produktion von Daten und Nutzung entstehen. Nur durch die Klarstellung, mit welchen Daten und Datenverarbeitungsmodellen gearbeitet wird, kann beurteilt werden, welche Fragestellungen sich mit diesen Daten beantworten lassen und welche Probleme aus einer unreflektierten Nutzung resultieren können. Zweitens ist es wichtig die Rolle der Sozialwissenschaften zu betonen. Anne Krüger beschreibt einen Trend zu Stellenausschreibungen für Data Analysts, und dass solche Stellen nicht an SozialwissenschaftlerInnen, sondern an InformatikerInnen vergeben werden. Das sieht sie als problematisch, da es nicht nur darum geht, Strukturen und Muster zu suchen, sondern auch um eine Fragestellung, mit der wir an Daten herangehen können und auch ein Wissen darüber, mit welchen Daten sich überhaupt welche Fragestellungen beantworten lassen und wie man dann auch tatsächlich über den Produktionskontext von Daten und Datenqualität reflektiert. Und drittens betont sie daher die Notwendigkeit der engen Zusammenarbeit der beiden Disziplinen, insbesondere im Hinblick auf die Frage wie die Performativität soziotechnischer Systeme erforscht werden kann. Es muss eine gemeinsame Arbeit daran geben, die Reflexion über die Veränderungen und die Möglichkeiten der Datenproduktion und Datennutzung zu stärken und dadurch auch ihre Objektivität immer wieder zu hinterfragen.

Der Einsatz dieser soziotechnischen Systeme wird und soll nicht mehr rückgängig gemacht werden. Es ist aber unabdingbar, die scheinbare Objektivität dessen, was dort passiert, immer wieder infrage zu stellen, um die Vision ihrer Allmacht sowohl im Positiven als auch im Negativen immer wieder aufbrechen zu können.

FIfF-Konferenz 2018

Empire and Power: The Forgotten History of the Internet as a Weapon – From the Vietnam War to Donald Trump

Verschriftlichung des Vortrags von Yasha Levine

Yasha Levine, Autor des Buches Surveillance Valley *sprach auf der FIfFKon über die vermeintliche „weaponization of the internet", der angeblich zunehmenden Nutzung des Internets als Waffe. Er ist überzeugt, dass das Internet eine Waffe ist. Auf Grundlage seiner historischen Forschung und journalistischen Arbeit zieht er jedoch die Schlussfolgerung, dass das Internet schon immer eine Waffe gewesen ist und von Anfang an als eine solche gestaltet wurde.*

Menschen haben auf ein mal Angst vor dem Internet bekommen

Die Art und Weise, wie in der Populärkultur über das Internet geredet wird, hat sich innerhalb der letzten paar Jahre drastisch verändert. Die Vorstellung, dass das Internet eine Technologie ist, die trotz aller Makel und Limitationen eine progressive Kraft für mehr Demokratie und Egalitarismus ist, wird immer mehr auf den Kopf gestellt. Nahezu absurd ist, was man momentan in den USA über das Internet in den Medien erfährt. Es wird so ziemlich für alles verantwortlich gemacht. Auf das Internet wird momentan geschaut als sei es eine einst demokratische Technologie, die von düsteren Mächten gekapert wurde und zu einer Waffe nahezu grenzenloser Macht gemacht wurde. Mit nur minimalem Einsatz von etwa 50.000 Dollar in Werbeanzeigen auf Facebook könne man im Grunde genommen eine Wahl gewinnen – als so mächtig und gefährlich wird das Internet gesehen. Täglich liest man von beängstigenden Geschichten, bei denen man das Gefühl bekommt, das Internet sei immer mehr eine Bedrohung für die Demokratie, und es gäbe Einigkeit darüber, dass es mehr Kontrolle und Beschränkung unterliegen müsste, dass es mehr mit dem Sicherheitsapparat durchdrungen werden müsste, um sicherzustellen, dass es sich dem nationalen Sicherheitsbedürfnis unterwirft. Diese Entwicklung der Betrachtung ist eine fast 180°-Kehrtwende, denn noch vor wenigen Jahren galten Freiheit und Offenheit des Internets als Tugend und wurden als *die* entscheidenen Gründe angesehen, warum das Internet so erfolgreich war – diese Freiheit erklärte das demokratische Potenzial des Netzes. In Amerika hätte man jedes Land beschimpft und es als eine Art totalitäre Tendenz angesehen, wenn es versucht hätte, seine eigenen nationalen Gesetze

und kulturellen Vorstellungen über das Internet innerhalb seiner eigenen Grenzen zu vermitteln.

Ein anderer bemerkenswerter Aspekt dieses Wandels ist, dass die Leute so handeln, als wäre es etwas vollkommen Neues, dass fremde Mächte oder der Staat das Internet nutzen, um Menschen, Politik und Kultur zu beeinflussen. Als wäre, bis Trump gewählt und als Präsident installiert wurde, das Internet naiv und neutral gewesen, als wären dann erst böse Mächte gekommen, die es korrumpiert und in eine Waffe verwandelt hätten.

Die Anfänge des Internets fanden unter Protest statt

Dass das Internet zur Waffe gemacht wurde stimmt – jedoch nicht erst vor Kurzem. Bereits in den 1960ern wurde es vom Pentagon und dem amerikanischen Militär als Informationswaffe, als Managementwaffe für globale, aber auch inländische Militärpräsenz gestaltet. Wohin sich diese anfänglichen Ideen entwickelt haben, sehen wir heute. Das Internet durchdringt alles, berührt jeden Aspekt unserer Gesellschaft, und hat auf diese Weise noch viel mehr das Potenzial, als Waffe genutzt zu werden als zu Beginn, als das Internet lediglich ein Netzwerk war, das Daten transportieren konnte.

Als der Anfang des Internets in den 1960er Jahren geschaffen wurde, war den Leuten sehr bewusst, dass es sich dabei um eine Waffe handelte. Es wurde darüber geredet und es wurde dagegen protestiert. Die Proteste umfassten viel, worüber man sich heutzutage Sorgen macht. Das Wissen über die Umfangreiche Kritik ist heute jedoch aus dem kulturellem Gedächtnis verschwunden.

1969 brachen an der Harvard-Universität Proteste aus. Mehrere hundert Studierende marschierten zum Campus, besetzten Gebäude und weigerten sich, diese wieder zu verlassen. Ähnliche Proteste gab es auch am MIT. Die Campus waren übersät mit Flyern, Plakate prangerten „computerisierte Menschenmanipulation“ an und warnten davor, dass ein neuer High-Tech-Kolonialismus auf dem Campus entwickelt werden würde, der die Menschen versklavte. Protestiert wurde gegen das ARPANET, das militärische Netzwerk, das Dekaden später das Internet werden sollte.

Aus historischer Perspektive waren diese Proteste sehr überraschend, da diese nicht nur bereits einen Monat, bevor der erste ARPANET-Knoten in Stanford im Oktober 1969 überhaupt online ging, stattfanden, sondern auch weil die Kritik, die geäußert wurde aus heutiger Perspektive schon sehr weitsichtig und umfangreich war. Das ARPANET wurde von den Protestierenden schon damals als Informations- und Managementwaffe angesehen, um die Macht des US-Militärs und großer Kooperationen im Inland und weltweit weiter zu erhöhen. Die Technologie wurde als Bedrohung für progressive und linke Bewegungen und für die ganze Gesellschaft wahrgenommen.

Der Grund, dass die Protestierenden in der Lage waren, ein so tiefgehendes Verständnis über das ARPANET und das Internet, von dem sie gar nicht so genau wussten, dass es gerade geboren wird, entwickeln konnten, war die Tatsache, dass sie Zugang zu dem kontroversen und geheimen Vorschlag des sogenannten *Cambridge Projektes* hatten, dessen Autor der Gründer des ARPANET, J. C. R. Licklider war. Licklider war ein Manager, der eingeladen wurde, das ARPANET-Programm im Wesentlichen aufzusetzen.

Das Projekt, das er vorschlug und ins ARPANET anschließend integrierte, war so etwas wie die 8-Bit-Version oder eine Atari-Version dessen, was Palantir heute macht. Es sollte als *Distributed Service* auf dem ARPANET laufen, so dass jeder, der ein ARPANET-Terminal und Zugang zu diesem Dienst hatte, sich bei ihm anmelden konnte. Es war damit das am besten entwickelte, verteilte Datenbank- und Datenbankmanagementwerkzeug zu damaliger Zeit. Ein Analyst konnte jede Art von Daten hochladen, die er hatte; diese konnten in einer Datenbank strukturiert werden, so dass die Daten dann auf jede erdenkliche Weise manipuliert und analysiert werden konnten: Überwachungsdossiers, Finanztransaktionen, Meinungsumfragen und vieles mehr.

Diese konnten genutzt werden, um Voraussagemodelle zu generieren, soziale Beziehungen zu kartieren oder Datenbanken anzulegen, die allen mit entsprechendem Zugang zur Verfügung standen – um also all die Aufgaben zu übernehmen die heutzutage als selbstverständlich angesehene Aufgaben eines Computers sind. Lickliders Cambridge-Programm hatte das konkrete militärische Ziel, die Anti-Aufstandsmission der US-Regierung zu unterstützen, die damals die amerikanische Militärpolitik dominierte. Es sollte dem Militär ermöglichen, einen besseren Überblick darüber zu bekommen, was vor sich ging. Man konnte Daten über politische Bewegungen aufnehmen, sie mit Meinungsumfragen und Umfragen verketten, versuchen, Konflikte vorherzusagen und eine mögliche Revolution zu brechen. Man konnte also in die Bevölkerung hineinblicken, um zu sehen, was passierte, wer die Akteure waren und wie diese zusammenhingen.

Yasha Levine

Yasha Levine ist ein in Russland geborener US-amerikanischer Investigativjournalist und Autor des Buches *Surveillance Valley – The Secret Military History of the Internet*

Die wenigsten sahen Computer damals als ein Werkzeug zur Befreiung, sondern als ein Werkzeug der Machterhaltung und des Machtausbaus. Die Verbindung zwischen Computern und Macht war offensichtlich, denn Computer waren riesig und teuer und konnten nur von großen Institutionen angeschafft und genutzt werden. Die Studenten erkannten also, dass das Cambridge-Project als Netzwerk für Überwachung und politische Kontrolle designt war, und Teil des größeren Trends war, an Universitäten überall in den USA militärisch zu forschen. Das ARPANET war zu diesem Zeitpunkt also Teil einer größeren Sorge, so dass die Studenten des MIT forderten, das Projekt zu schließen und diese Art von Forschung nicht stattfinden zu lassen. Sie haben zwar nichts erreicht, haben aber Recht behalten. Das Cambridge-Project lief fünf Jahre und entwickelte sehr robuste Plattformen, die es Analysten erlaubte, auf immer größer werdenden Datensätzen zu arbeiten.

1976, sechs Jahre nach den Protesten, strahlte NBC zur Prime Time eine Serie von Berichten zu einem Überwachungsprogramm aus, das Millionen von AmerikanerInnen ausspioniert hatte. Akten die über Kriegsprotestierende, Bürgerrechtsführer und alle die mit dem linken Flügel oder progressiven Organisationen in den USA zu tun hatten, vom Militär illegal angelegt worden waren, wurden, statt sie zu vernichten (wie vom Kongress angeordnet) für das ARPANET und das Camebridge-Project digitalisiert und so der NSA, dem CIA und dem Weißen Haus zugänglich gemacht. Dies war ein riesiger Skandal, der von Millionen Menschen über mehrere Tage auf NBC verfolgt werden konnte. Die Berichte stiegen sehr tief in die Thematik und auch die Architektur des ARPANET ein. Was die Leute wirklich schockierte, war die Tatsache, dass die eine große, zentrale Datenbank, über die man sich Sorgen gemacht hatten, gar nicht in dieser zentralen Form notwendig war. Es gab in der Tat eine Reihe von Vorschlägen, solche zentralen Datenbanken anzulegen, doch weil so viele Menschen darüber besorgt waren, wurden sie wieder stillgelegt, da eine solche Maßnahme wohl zu offensichtlich gewesen wäre. Die Berichte über das ARPANET zeigte den Leuten, dass der Knackpunkt die Vernetzung zwischen vielen kleinen Datenbanken war und diese von jedem Punkt im Netzwerk genutzt werden konnten. Die Berichte konnten also zum einen die Sorgen der protestierenden Studenten bestätigen und außerdem die Weiterentwicklung der Überwachungsarchitektur aufzeigen.

Zwei Flügel des gleichen Kampfes

Um zu verstehen, warum das Internet schon damals eine Waffe war, ist es wichtig, das kulturelle und politische Umfeld zu betrachten, in dem es gebaut wurde. In den 1960ern waren die USA noch immer ein relativ neues Imperium, das die zunehmend chaotischer werdende Welt überblicken musste. Es kämpfte gegen Aufstände auf der ganzen Welt, von Südostasien bis Lateinamerika und es sah sich einer zunehmend feindlichen innenpolitischen Situation gegenüber. Da waren die Antikriegsbewegung, die Bürgerrechtsbewegung und Gruppen, die staatliche Gebäude bombten. Es schienen Revolutionen sowohl global als auch intern stattzufinden. Militärplaner und Politiker sahen diese als zwei Flügel des gleichen Kampfes – beide dieser Stachel wurden als untereinander und auch mit der Sowjetunion verbunden angesehen. Während die Sowjetunion den Kalten Krieg mit traditionellem amerikanischem Militär und den Atomstreitkräften kämpfte, kämpfte sie auch gegen Amerika, indem sie Aufstände auf der ganzen Welt und Protestbewegungen und Oppositionsbewegungen in Amerika finanzierte.

In bestimmten militärischen Kreisen wurde in der Zeit geglaubt, dass man zur Bekämpfung dieser neuen Art von Krieg eine neue Art von Waffe brauchte, eine neue Art von Verwaltungswaffe, die es Militärplanern, Generälen und Politikern ermöglichen würde, die Welt in Echtzeit zu sehen. So viel wie möglich zu haben, das war der Traum.

Damals gab es bereits Beispiele, dass diese Ideen umgesetzt wurden. In den 1950er Jahren wurde das erste computerisierte Frühwarnradarsystem namens SAC gebaut, das später zu Norad wurde. SAC war ein umfangreiches System, mit riesigen IBM-Computern in Bunkeranlagen. Dies zeigte, dass der Bau eines Überwachungsnetzwerkes möglich ist, das auf dem Gipfel der Welt sitzt und diese in Echtzeit überwacht und diese Informationen enorm heruntergebrochen auf Bildschirmen darstellen konnte. Analysten waren in der Lage, tausende Kilometer Grenzgebiet zu überwachen. Die nächste Stufe dieser Bemühung war, die Möglichkeiten auszuweiten und nicht nur den Himmel sondern die Gesellschaft generell zu überwachen.

Auch J. C. R. Licklider hatte für das SAC-Programm gearbeitet. Er arbeitete an den GUIs für die Radar Displays. Davon Inspiriert, kam er zum ARPANET, glaubte jedoch daran, wenn man ein neues Command-and-Control-System aufbauen will, müsste man auf einem weitaus fundamentaleren Level beginnen. Man müsste erst die grundsätzlichen Teilstücke umsetzen, um daraus dann ein Gesamtsystem zu bauen, um nicht jedes Einzelsystem von Grund auf neu entwerfen zu müssen, wie es bis dahin gemacht wurde. Es war aus seiner Sicht nötig, einen generischen Computer und ein universelles Netzwerksystem zu bauen, mit dem man beliebige digitale Nachrichten austauschen könnte. Licklider war überzeugt, man bräuchte viel universellere Computer und deren Vernetzung, die mit minimalem Aufwand angepasst werden könnten, um damit praktisch jede Aufgabe zu erfüllen, ob das Raketenverfolgung, Verhaltensstudien, Datenbanken oder Analyse von gesprochener Kommunikation sei.

Benötigte Basiskomponenten waren eine intuitive graphische Benutzungsoberfläche, ein universelles Betriebssystem für Anwendungen und, um mit anderen Systemen verbunden zu werden, eine ausfallsichere Netzwerkkomponente. Dies war es worauf Licklider abzielte, als er bei ARPA mit dem anfing, was später das Internet wurde, das wir heute nutzen.

Das Internet, dessen Infrastruktur und die angrenzenden Institutionen, all das wurde geboren aus dem Wunsch, ein modernes Command-and-Control-System zu bauen. Es wurde vorangetrieben von militärischen Bedürfnissen – früher und auch heute noch. Auch wenn es um einiges an Komplexität gewonnen hat und viele kommerzielle Dienste darauf aufgebaut wurden, ist der Kern immer noch militärisch.

Was brauchen wir als Zivilgesellschaft eigentlich für eine Art von Netzwerk und was für eine Technik hätten wir denn gerne?

Verschriftlichung des Vortrags von Christian Grothoff

„All governments should be pressured to correct their abuses of human rights." – Richard Stallman

Im Vortrag von Christian Grothoff wurden die politischen Anforderungskataloge für das GNU-Name-System und GNU-Taler vorgestellt. Danach wurde gezeigt, wie diese Anforderungen technisch umgesetzt wurden.

Was die Projekte, mit denen Grothoff sich beschäftigt, verbindet, ist der Wunsch nach einer liberalen Gesellschaft, der sich an vielen Stellen wiederfindet. In der Allgemeinen Erklärung der Menschenrechte steht im Artikel 12 „Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden." So ziemlich alle Nationen haben dieses Dokument ratifiziert und das sagt ganz klar, der Staat darf nicht in private Kommunikation eingreifen. Die ist ein schöner Anspruch, den man auch in einem Netzwerk haben sollte, so Grothoff.

Einen weiteren Anspruch, im sozialen Bereich, findet man in Artikel 22:

> *„Jeder hat (...) das Recht auf soziale Sicherheit und Anspruch darauf, (...) in den Genuss der wirtschaftlichen, sozialen und kulturellen Rechte zu gelangen, die für seine Würde und die freie Entwicklung seiner Persönlichkeit unentbehrlich sind."*

So wie Grothoff den Kapitalismus bisher erlebt hat, passiere die Umsetzung solcher Ansprüche nicht von alleine. Man benötigt einen Sozialstaat, der durchaus die Pflicht hat, in die Wirtschaft einzugreifen und dafür zu sorgen, dass allen zumindest eine gewisse gesellschaftliche Teilhabe möglich ist. Auf diese Grundwerte haben wir Menschen uns bis auf ein paar Ausnahmen global geeinigt – Sie stehen dementsprechend nicht zur Debatte. Was technisch heutzutage umgesetzt wird, findet seine Grenzen jedoch nicht durch politische Gesetze und Grundwerte. Der tiefe Staat macht, was er möchte und findet Grenzen nur noch darin, was die Technik erlaubt und was nicht. Das Internet wird weitestgehend überwacht, die technische Grenze dieser Überwachung ist Kryptographie. Kann diese nicht gebrochen werden, kann nicht überwacht werden, ansonsten wird es jedoch gemacht.

Ebenso hat es sich im Wirtschaftlichen entwickelt. Das Internet hat dafür gesorgt, dass die Wirtschaft globalisiert ist. Weil sich Konzerne und Firmen über staatliche Grenzen sehr leicht hinwegsetzen können, wird es dem Staat schwierig gemacht, sie zu kontrollieren. Insofern muss der Anspruch gestellt werden, dass die Technik dem Staat die Steuerungsmechanismen wieder in die Hand gibt, um die sozialen und freiheitlichen Ziele zu erreichen.

Die Realität sieht jedoch nicht danach aus. Von Edward Snowden haben wir gelernt, dass Briten und Amerikaner, wie man historisch schon gesehen haben kann, mit Hilfe von Überwachung

alles wissen und alles kontrollieren wollen. Auf der „corporate-sozialen Schiene" erkennt man es z. B. an Amazon. Ein massiv profitables Unternehmen, eines der größten der Welt, zahlte in Amerika im Jahr 2017 ‚null' Steuern.

Design-Ziele von GNUnet

So wie beschrieben kann es nicht bleiben, also muss von den InformatikerInnen, die für Technikentwicklung zuständig sind, eine Änderung kommen. Mit dem GNU-Projekt und insbesondere mit dem GNUnet-Projekt ist es der Anspruch, ein Netzwerk zu erschaffen, das besser ist und wird. Angefangen wurde dabei nicht etwa mit militärischen Zielen wie denen des DARPA-Netzes (siehe Vortrag von Yasha Levine auf Seite 33), sondern mit eigenen Zielen und Ansprüchen.

Da das GNUnet ein GNU-Projekt ist, ist der erste Anspruch natürlich, dass es als freie Software implementiert sein muss, nicht von irgendeiner Firma kontrolliert werden soll, sondern allen gehört. Das Grundkonzept ist *privacy-by-design*, wie es die DSGVO vorgibt. Es darf also nur die minimal notwendigen personenbezogenen Daten preisgeben. Es soll außerdem komplett verteilt und sowohl resistent gegen externe Angreifer als auch gegen böswillige Teilnehmer sein, da man davon ausgehen muss, dass nicht alle Leute wohlwollend sind. Es muss selbstorganisierend und nicht von Administratoren zentral verwaltet sein. Das Problem bei der Rolle der Administratoren ist, dass diese nicht nur die Macht über die Menschen haben, deren Strukturen sie verwalten, sondern es sie auch zu Zielpersonen werden lässt. Wenn Administratoren gehackt werden, dann trifft es im gleichen Zuge auch all diejenigen, die von ihnen ab-

Design-Ziele für zivile Netze

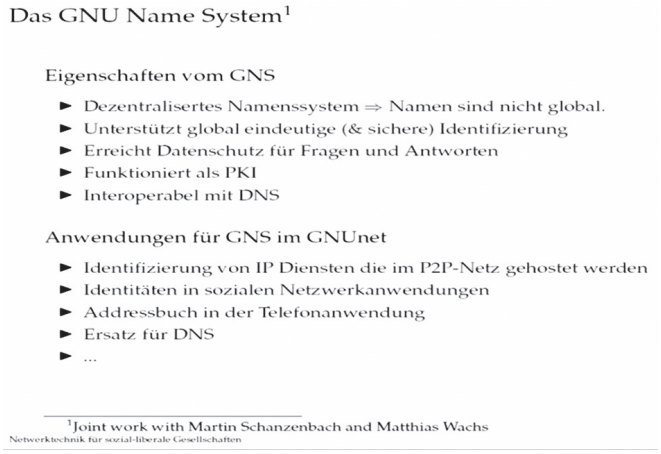
1. *GNUnet muss als Freie Software implementiert sein.*
2. *GNUnet darf nur die minimal notwendigen personenbezogenen Daten preisgeben.*
3. *GNUnet muss komplett verteilt und resistent sowohl gegen externe Angriffe als auch gegen bösartige Teilnehmer sein.*
4. *GNUnet muss selbstorganisierend und nicht von Administratoren oder zentraler Infrastruktur abhängig sein.*
5. *GNUnet muss den Benutzer informieren, wem vertraut werden muss, wenn private Kommunikationskanäle etabliert werden.*
6. *GNUnet muss ein offenes Netz sein, dem neue Peers beitreten können.*
7. *GNUnet muss ein breites Spektrum an Anwendungen und Geräten unterstützen.*
8. *GNUnet muss sensitive Daten durch Kompartimentierung schützen.*
9. *Die GNUnet-Architektur muss Ressourcen effizient einsetzen.*
10. *GNUnet muss Anreize schaffen, dass Peers mehr Ressourcen bereitstellen als sie selber verbrauchen.*

hängig sind. GNUnet will, dass idealerweise gar keine Administratoren mehr nötig sind und es selbstorganisierend ist. Die Idee ist, die eigene Hardware unter eigener Kontrolle zu haben und dann nichts weiter machen zu müssen. Anfragen an einen Administrator nach Accounts oder Passwörtern sollen dadurch unnötig werden.

Wenn ein sicherer Kommunikationskanal aufgebaut wird, kann es durchaus sein, dass dies über Infrastruktur Dritter geschieht, und vielleicht haben diese Dritten geholfen, einen Schlüssel zu verifizieren oder ähnliches. Wenn irgend jemandem vertraut werden muss, damit die eigene Kommunikation sicher ist, muss diese Tatsache bekannt gemacht werden. Es muss ein offenes Netz sein, das nicht einer kleinen, geschlossenen Community vorbehalten bleibt. Es sollen viele Anwendungen und Geräte unterstützt werden und es soll dafür gesorgt werden, dass die Daten nur dort vorliegen, wo sie wirklich benötigt werden, und nicht woanders. Ressourcen sollen effizient und damit umweltfreundlich eingesetzt werden, nicht etwa wie bei Bitcoin, für deren Betrieb enorme Mengen an Energie verbraucht werden. Und nicht zuletzt sollen Anreize gesetzt werden, dass Teilnehmende Ressourcen bereit stellen, damit das Netzwerk funktionieren kann und „freeloader" nicht einfach das Netz „DDOSsen" können. Die Design-Zielliste beinhaltet also sehr viel bezüglich Datenschutz und sehr viel zu Sicherheit und Verschlüsselung. Bei den Anforderungen fürs ARPANET fand man als einziges richtiges Sicherheitsziel etwas zu Verfügbarkeit – das Netz sollte lediglich ausfallsicher sein.

Für GNUnet wurden inzwischen verschiedene Anwendungen gebaut. Mit *Conversation* wurde ein sicheres, dezentrales Telefonieren implementiert. Es gibt Möglichkeiten für anonymes und nicht-anonymes Publizieren, ein IPv6–IPv4 Protokollübersetzer und Tunnel und viele andere Projekte, die auf dem GNUnet aufbauen. Es ist zu hoffen, dass die Liste noch viel länger wird. Zwei Anwendungen, nämlich das GNU-Name-System (GNS) ein zensurresistenter Ersatz für DNS und GNU-Taler, ein System für datenschutzfreundliches Bezahlen, sollen hier vorgestellt werden.

Das GNU-Name-System (GNS)



Das GNU-Name-System ist für das GNUnet ein zentraler Teil, genauso wie das Domain-Name-System (DNS) ein zentraler Teil für das Internet ist. Wenn DNS ausfällt, müssen IP-Adressen von Hand erfragt und eingetippt werden, das macht nur wenigen Freude.

Das GNU-Name-System ist im Gegensatz zum hierarchischen Namenssystem DNS ein dezentrales Namenssystem. Beim hierarchischen DNS sitzt ganz oben die ICANN, die z. B. die Top-Level-Domain *.de* an die DENIC oder *.ch* an die SWITCH vergibt. Die DENIC wiederum gibt Auskunft darüber dass, z. B. die Domain TU-Berlin.de von der TU in Berlin verwaltet wird. DNS ist also so durchhierarchisiert, dass umgesetzt werden könnte, das dem Administrator X aus Land Z die Rechte weggenommen werden können oder das ganze Land Z blockiert werden kann. Die Schweizer bauen als Teil ihres SCION Projektes an der ETH Zürich momentan ein System namens RAINS auf. Es soll ein nationales Netz entstehen, mit einem nationalen DNS, einer nationalen Zertifizierungsstelle und einer nationalen Blockierliste. Damit man „die ganzen Bösen" draußen halten kann, so Grothoff.

Wünscht man sich wie bei GNS nun ein dezentrales Namenssystem ohne Hierarchie, hat man den Nachteil, dass die Namen nicht mehr wirklich global sind. Man kann nun nicht mehr sagen, das der eine oder die andere bestimmt. Was man dabei aber trotzdem haben kann, sind eindeutige Identifizierer. Es handelt sich dabei dann jedoch nicht mehr um Namen, sondern genau genommen Public Keys. Diese sind nicht zwar nicht mehr leicht zu merken, aber es funktioniert.

Die wichtigste Eigenschaft neben der Dezentralisierung ist für Grothoff, dass Datenschutz für Anfragen und Antworten inner-

halb dieses Namenssystems umgesetzt wird. Dies geschieht auf eine Art und Weise, die man sich zunächst ersteinmal kaum vorstellen kann: Beim GNS ist es möglich, eine Frage nach der Auflösung eines Namens verschlüsselt zu stellen. Diese Anfrage kann an eine Gruppe gestellt werden, von der ein beliebiges Mitglied auf seiner Festplatte die Antwort gespeichert hat. Dieses Mitglied kann dabei zwar weder die Frage noch die Antwort entschlüsseln, kann aber mit Sicherheit sagen, dass die zur Verfügung stehende Antwort garantiert die Antwort auf die gestellte Frage ist, und kann die Antwort dann über Dritte weiterleiten. Auch alle Weiterleitenden können nur die verschlüsselte Frage und Antwort sehen, dabei aber verifizieren, dass die Antwort tatsächlich auf die Frage passt. Nur wer die Anfrage gestellt hat, kann die Antwort letzten Endes entschlüsseln. Es handelt sich dabei also um eine Art *Private Information Retrieval* – ein schöner kryptographischer Trick.

Da man auf diese Weise immer nur die richtigen Antworten bekommt, kann dieses Prinzip auch als *Public Key Infrastruktur* genutzt werden. Konzepte, die man von x.509, *Web of Trust*, DNSSec oder Ähnlichem kennt, können damit also nachgebildet werden. GNUnet hat das Verfahren sogar so gestaltet, dass es interoperabel mit DNS ist, so das es sogar einen Migrationspfad von DNS zu GNS gibt.

Vorstellbare Anwendungen sind das Adressieren beliebiger Dienste im *Peer-to-Peer*-Netz, Authentifizierung in sozialen Netzwerken oder Adressbücher. Ein Adressbuch der GNUnet-Telefonanwendungen ist z. B. im Wesentlichen eine Zone im GNU-Name-System. GNS könnte DNS somit langfristig ersetzen.

GNU-Taler

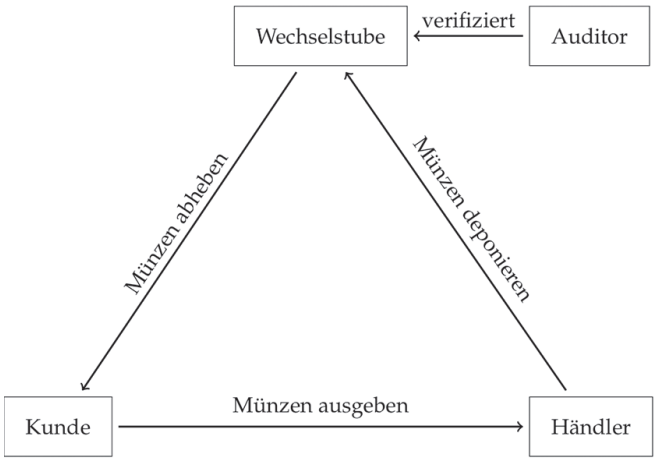
Nach den Grundsätzen des GNU-Projekts fehlte es außerdem auch an einem sozial orientierten Bezahlsystem, was Systeme, die hinter Buzzwörtern wie Blockchain und Bitcoin stehen, nicht leisten. Bestehende Systeme wie das Kreditkartensystem folgen dem Prinzip der Überwachung. Mit Kreditkarte kann man getrackt werden, egal wo man ist, ob man sich ein Busticket kauft, irgendwo essen geht oder ein Hotelzimmer bucht. Das ist unerwünscht und so entstand die Idee, etwas Bargeldähnliches digital, dabei aber auch sozial verträglich, nachzubauen.

Das GNU-Taler oder kurz Taler genannte System soll dafür sorgen, dass Einnahmen komplett transparent, Ausgaben jedoch komplett anonym bewerkstelligt werden. Zwar sollen Einkommen vom Staat gesehen werden, so dass Steuern drauf erhoben werden können oder festgestellt werden kann, wenn etwas nicht legal war. Der Staat soll in die Wirtschaft eingreifen können, aber gleichzeitig soll man Ausgaben komplett anonym machen können. Dieses Prinzip soll selbstverständlich als freie Software umgesetzt werden.

Die Designziele von Taler sind also anders als die aus der Parallelwelt der Blockchains und Cryptowährungen. Einige aus diesen Bereichen meinen, dafür zu sorgen, dass Einkommen besteuert werden können, sei eine unerwünschte Idee. Die Folge davon sind Menschen, die andere mit Crypto-Trojanern erpressen. Bei GNU-Taler wäre so etwas kaum möglich, da erpresstes Geld bei einer Steuerprüfung zum Vorschein kommen würde.

Der Staat soll also die Wirtschaft regulieren dürfen, dabei aber ansonsten nur die minimal notwendigen Daten verarbeiten. Dabei muss das System trotzdem einfach zu benutzen sein, da es sich sonst nicht durchsetzen würde. Es sollte außerdem effizient sein, da sonst wieder hohe – nicht nur finanzielle – Kosten entstehen.

Als Metapher ausgedrückt ergab sich daraus folgendes Prinzip für Taler: Wir haben eine Wechselstube, die mit der Bank interagiert, von der ich als Kunde Münzen abheben kann. Diese Münzen kann ich bei einem Händler ausgeben. Der Händler muss sie anschließend bei der Wechselstube deponieren und der Wechselstube Bescheid geben, dieses Geld gerade von einem Kunden bekommen zu haben. Der Händler weiß nicht, wer der Kunde war, da beim Bezahlen ein anonymer Kanal genutzt werden kann – zum Beispiel (aber natürlich nicht zwingend) Tor. Der Kunde muss sich beim Bezahlen also nicht identifizieren. Er gibt wie beim Bargeld dem Händler digitale Münzen, der sie aber nicht gleich zum Kaufen weiterbenutzen kann. Taler ist im Gegensatz zu Bargeld also nicht transitiv. Den Wert der Einnahmen kann der Händler nur wieder nutzen, wenn er es bei der Wechselstube einlöst, das Geld auf seinem Konto gutgeschrieben bekommt und für einen weiteren Kauf erneut abhebt. Taler soll nicht mit einer der bestehenden Cryptowährungen funktionieren, sondern mit ganz normaler Währung, wie Euro, Franken oder Dollar.

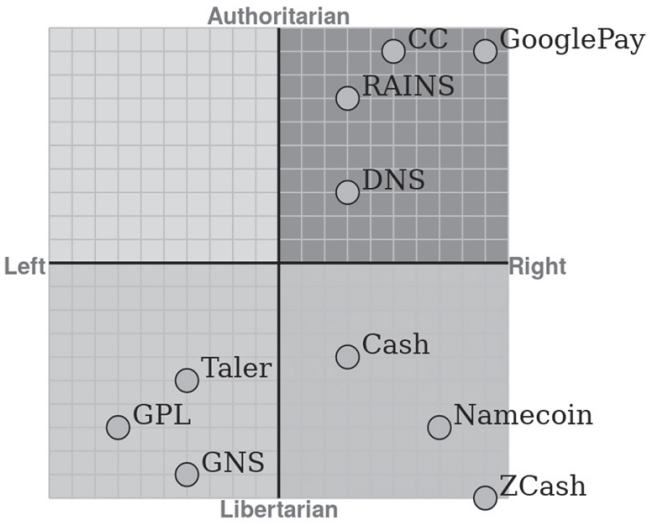


Eine Demo des Prinzips wurde auf der FIfFKon gezeigt und kann jederzeit unter *https://demo.taler.net* nachvollzogen werden: Auf der Website findet man ein kleines Ökosystem bestehend aus einer Bank, einigen Händlern. Mit wenigen Klicks ist dort ein Digitales Portemonnaie ein sogenanntes „Wallet" als Browser-Plug-In installiert und ein Bankkonto mit einem kleinen Startguthaben in der eigenen Währung KUDOS eröffnet. Bei der Bank kann man gegen eine kleine Gebühr einen gewünschten Betrag abheben, der dann nach der Eingabe einer TAN im Wallet im eigenen Browser landet und zuzüglich einer kleinen Gebühr vom Bankkonto abgezogen wird. Nun kann man sich aus der Bank ausloggen und sich über eine beliebige anonyme Verbindung auf die Website eines Händlers begeben, der etwas gegen Bezahlung anbietet. In der Demo handelt es sich um die fiktive Plattform „Essaystore" mit zu bezahlenden Artikeln. Will man sich nun, nach dem man den Teaser gelesen hat, einen Artikel vollständig zu Gemüte führen, ist nur ein Klick auf den Bezahlknopf nötig, und der Artikel ist aus dem digitalen Portemonnaie bezahlt und sofort freigeschaltet.

Alle die an Bezahlvorgänge mit Kreditkarten gewöhnt sind, sind an dieser Stelle überrascht, mit wie wenig Hindernissen und wie schnell das Bezahlen abläuft. Das ganze funktioniert, trotz Crypto, und selbst über langsame Netzanbindung, blitzschnell. Obendrein ist der ganze Bezahlvorgang überaus leicht zu verstehen. Letzten Endes wird diese Einfachheit beim Bezahlen nur durch die Crypto ermöglicht, da man eben nicht beim Bezahlen beweisen muss, wer man ist, sondern dies bereits beim Geldabheben geschehen ist. Beim Bezahlen muss nicht erst noch eine TAN per SMS eingetippt, ein Account erstellt, ein Gesicht in die Kamera gehalten werden oder dergleichen; man benötigt lediglich das eigene Endgerät, das das eigene abgehobene Geld verwaltet. Das Gerät signiert dann mit den eigenen Münzen und bezahlt.

Politische Einordnung

Wie in der Abbildung zu sehen ist, kann man die verschiedenen Bezahlsysteme politisch verorten.



Oben finden sich die autoritären Prinzipien: Kreditkarten, Militär, Google Pay, Schweizer Domain-Name-System – diese wollen die totale Kontrolle haben: Libertärer Kapitalismus ohne Regeln. Name-Coin ist der DNS-Ersatz für Blockchains. Dieses System ist nicht mehr autoritär, aber es ist sehr kapitalistisch gestaltet: Wer einen Namen haben will, muss zahlen. Rechts unten findet man ZCash, ein Bezahlsystem bei dem sowohl anonym ist, wer Geld bekommt als auch, wer bezahlt. ZCash beruht auf der Blockchain-Technik, ist sehr langsam, schlecht zu benutzen und sehr geeignet für kriminelle Aktivitäten. Grothoff findet sich politisch im Spektrum unten links wieder, und darum verortet er auch seine eigenen Projekte dort. GPL hält er für linkslibertär, so auch GNS und Taler. Leider gebe es in diesem Bereich noch zu wenig Technik.

GNS ist Cyberpeace

Bei einem Workshop zum Thema Cyberpeace traf Grothoff auf die „üblichen Leute von den Geheimdiensten", die der Meinung waren, Cyberpeace müsse irgendwo im oberen, also autoritären Bereich gemacht werden, und man Accountability bräuchte, um bei der Forensik feststellen zu können, wer es war, um dann „zurückschießen" zu können. Grothoff vertritt hingegen die Meinung, Cyberpeace mache man mit GNS, und eben gerade dadurch, dass man nicht mehr wisse, wer, würde eine Friedensgrundlage gelegt. GNS soll ein Allgemeingut – ein Commons – werden, das nicht irgendjemandem gehört, das allen gehört, das nicht einem Staat dient, einer Organisation, einer Firma oder einer Person, das nicht weiß, wem es dient. Es kann nicht sagen, was es es für eine Anfrage beantwortet hat, ob es eine deutsche, russische oder amerikanische Frage gelöst hat. Das kann es nicht wissen – die Crypto verhindert das. Wenn man Privatsphäre hat, hat man eine neutrale Infrastruktrur, deren Angriff keinen Sinn ergibt, weil man sich dabei selbst schadet, da man sie ja auch nutzt.

Spieltheoretisch, kann man, wenn man Accountability hat, immer sagen, man kann jemandem durch einen Angriff auf eine Sache schaden, die einem nicht selbst gehört. Wenn es aber allen gehört, so wie unsere Atmosphäre, greift man es nicht kriegerisch an. Da wären alle dagegen, da wir die Atmosphäre alle atmen.

Cyberpeace kommt also durch Privatsphäre. Wenn unbekannt bleibt, wer die Anfrage stellt, kann niemand mehr sagen, *dich* blockiere ich. Wenn unbekannt bleibt, für wessen Dienst ich eine Antwort speichere und weitergebe, kann ich demgegenüber nur neutral sein. Wenn alle die Infrastruktur nutzen, werden auch alle sie verteidigen. Wenn man hingegen dahingeht, etwas als die eigene Infrastruktur zu sehen, wie eine „Festung Europa", erst dann kann man sagen, ich grenze mich ab, dann kann man kriegerisch aktiv werden. Wenn wir Frieden haben wollen, bekommen wir das nur umgesetzt durch guten Datenschutz, Dezentralisierung und Commons. Und das heißt natürlich auch – durch freie Software.

Hinweis: Wer mehr über die Crypto von GNUnet und Taler erfahren will, findet Vorträge von Christian Grothoff auf media.ccc.de.

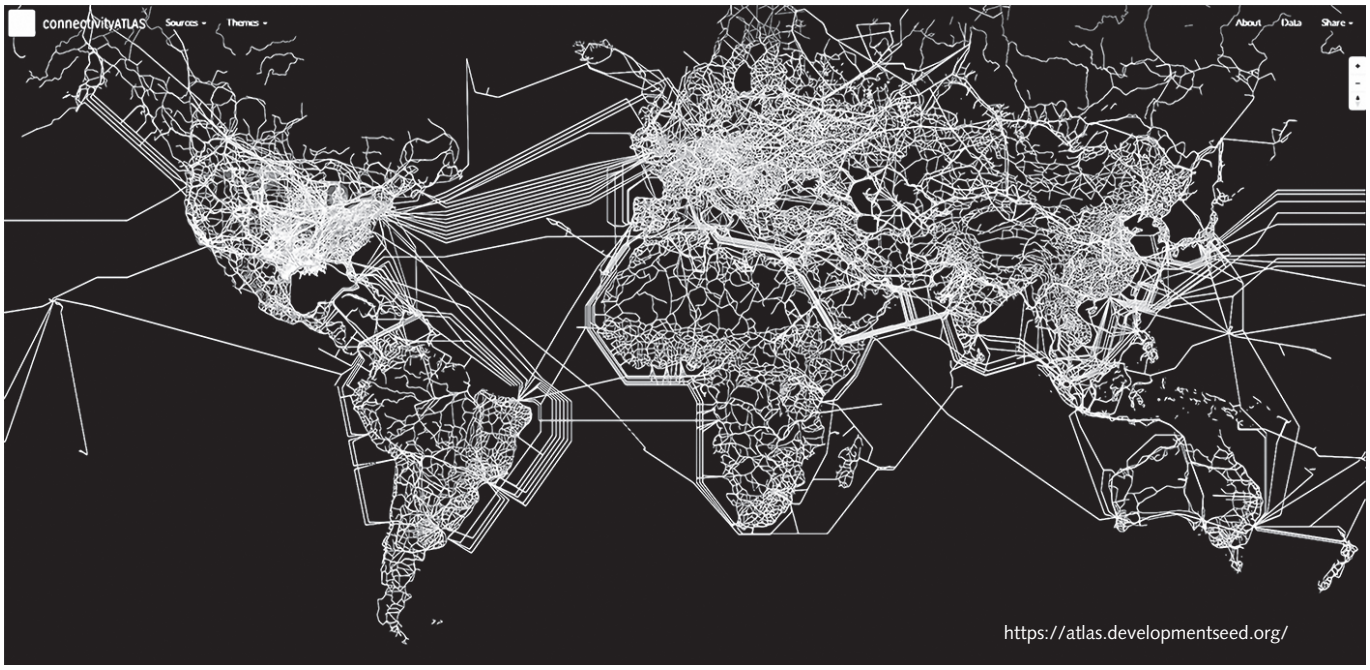
Christian Grothoff

Christian Grothoff, Softwarearchitekt, IT-Security, Privacy, GNUnet/GNU-Taler, ist Professor für Informatik an der Berner Fachhochschule. Er ist Ashoka Fellow und Maintainer von GNUnet.

Völkerverständigung ist Volksmacht plus Vernetzung der ganzen Welt – Von technischen Medien und dem Gebrauch, den wir von ihnen und sie von uns machen

Verschriftlichung des Vortrags von Volker Grassmuck

Das Versprechen jeder Kommunikationsverbindung vom Telegraphen über das Radio bis zum Internet ist, dass die Angeschlossenen durch ihren Austausch zu einem gemeinsamen Verständnis kommen. Heute ist die Welt global vernetzt wie nie. Doch statt Horizonterweiterung und Neugier auf Vielfalt erleben wir Xenophobie, Grenzschließungen und eine Internationale der Nationalisten. Die Koevolution von technischen, psychischen und sozialen Systemen läuft selten wie geplant. Wie kann da die Informatik ihrer Selbstverpflichtung nachkommen, Handlungsalternativen im Hinblick auf die absehbaren Wirkungen und möglichen Folgen ihrer Systeme aufzuzeigen?



Folie 1

Was wir hier sehen [Folie 1], ist eine Infrastruktur-Weltkarte, und man sieht die Untersee-IP-Kabel, Straßen, Eisenbahnen, Gaspipelines usw. Auf der Karte sind keine Ländergrenzen oder Grenzen von Kontinenten enthalten, aber die Weltkarte, die man sieht, emergiert aus der Infrastrukturkarte. „Wir formen unsere Infrastrukturen und dann formen unsere Infrastrukturen unsere Welt", könnte man in Abwandlung eines fälschlicherweise Marshall McLuhan zugesprochenen Diktums sagen. Heute ist die Welt global vernetzt wie nie. Das Versprechen jeder Kommunikationsverbindung ist, dass die Angeschlossenen sich etwas zu sagen haben und durch den Austausch zumindest die Chance haben, zu einem gemeinsamen Verständnis zu kommen. Doch statt Horizonterweiterung und Neugier auf Vielfalt erleben wir heute Xenophobie, Grenzschließungen und eine Internationale der Nationalisten. Die Errungenschaften des grenzenlosen Europa, also des Schengen-Raumes, wird zurückgedreht; wir sehen Europagegner im Europaparlament, UK isoliert sich, „USA first", ebenso Polen, Ungarn, Italien „first". Das Netz hat die Öffentlichkeit demokratisiert und zugleich ein Sprachrohr geschaffen für Menschenverachtung, Wissenschaftsverweigerung, Verschwörungstheorien, Propaganda und „Fake-News". Kräfte, die die Wahrheit systematisch unterminieren und durch Affekte wie Patriotismus und starke Führer ersetzen wollen, können Fuß fassen. Algorithmen und Personalisierung verstärken Filterblasen und Polarisierung.

Als Mediensoziologe ist das ein anhaltendes großes Rätsel, warum mehr Kommunikationschancen nicht auch zu mehr kommunikativer Verständigung, wenn nicht gar Rationalität in der Welt führen. Möglicherweise sitze ich da aber auch, trotz aller Bemühungen, in meiner Habermasianischen Filterblase. Dabei habe ich mich in meiner Dissertation beschäftigt mit einem Land, das sich über 250 Jahre maximal von der Kommunikation mit der Außenwelt abgeschottet hat, gleichwohl über das Nadelöhr Nagasaki ein ziemlich akkurates Bild dieser Außenwelt konstruieren konnte, nämlich Japan in der Zeit von 1603 bis 1868.

Luhmanns Idee, dass soziale und psychische Systeme, also Menschen, nicht kommunizieren, sondern einander irritieren, fand ich beim ersten Lesen skandalös irritierend. Je länger ich jedoch darüber nachdenke, desto plausibler erscheint sie mir. Die Erfahrung lehrt uns, dass eine gelingende Kommunikation selbst ohne technische Medien dazwischen die seltene Ausnahme ist. Nicht die Kanäle, sondern die innere Verfasstheit eines Systems entscheidet darüber, ob es sich von Signalen aus seiner Umwelt irritieren lässt oder nicht. Gehen wir also gemäßigt von einer Ko-

Evolution von technischen, psychischen und sozialen Systemen aus. Dabei unterliegen technische Entwicklungen durchaus ihren Eigenlogiken. Ob sie zu Aushärtungen, Pfadabhängigkeiten, Netzwerkeffekten führen, hängt aber von weiteren sozialen, ökonomischen, psychischen Faktoren ab, nicht zuletzt. Dabei ist der Lauf der Welt nicht technodeterministisch vorbestimmt. Er hätte so, aber immer auch anders sein können. Was zu der kontrafaktischen, aber gleichwohl für das Denken von Alternativen lehrreichen, Frage führt: Was wäre, wenn ...

… die Feinmechanik in den 1830ern so präzise gewesen wäre, dass Charles Babbage seine Differentialmaschine und danach seine Analytical Engine tatsächlich hätte fertigstellen können? Das Modell hier [Folie 2] ist 150 Jahre später, in den späten 1980ern gebaut worden, im Londoner Science Museum, das ist die Difference Engine No. 2, und die ist voll funktionstüchtig. 2011 begann dann das Projekt auch die Analytical Engine nachzubauen. Wenn das so gewesen wäre, vielleicht sähen unsere Arbeitplätze heute so aus. Und unsere Alexas so [Folie 3]. Und die Flugtaxis, die Dorothee Bär uns versprochen hat, so [Folie 4].

Die Analytical Engine war die erste universell programmierbare, Turing-mächtige Rechenmaschine. Lochkarten-gesteuert und kurbel- oder dampfbetrieben, wie bei den Webstühlen in der Zeit üblich. Dafür entwickelte Ada Lovelace die ersten Programme und legte damit nicht nur die Grundlage für Programmiersprachen sondern sah bereits Anwendungen über Zahlen hinaus voraus. Sie stellte sogar damals bereits die Frage, die uns heute so intensiv beschäftigt: Die Frage nach einer möglichen Künstlichen Intelligenz – die sie verneinte. Die Maschine könne nichts Originelles hervorbringen.

100 Jahre später widersprach ihr Alan Turing in *Computing Machinery and Intelligence*, im Jahr 1950 geschrieben. Da argumentierte er, der Computer könne Menschen sehr wohl überraschen, da dieser die Folgen verschiedener Tatsachen nicht erkennen könne. Außerdem habe er Lovelace neue Erkenntnisse voraus, die zeigten, dass das Gehirn einem Computer ähnele.

Was wäre, wenn die Analytical Engine damals gebaut worden wäre und ihre Erbauer überrascht hätte? Und dann z. B. das Deutsche Reich gleich nach seiner Gründung KI als Schlüsseltechnologie erkannt und 1880 eine nationale Künstliche-Intelligenz-Strategie gestartet hätte?

Gehen wir zurück zum Beginn der IKT. Der Techniker und Geistliche Claude Chappe experimentierte Ende des 18. Jahrhunderts mit dem optischen, elektrischen und akustischen Übermittlungsverfahren von Zeichen. 1793 verwendete er für die erste Teststrecke zwischen Paris und Lille einen Semaphor, einen schwenkbaren Signalarm, der mit Fernrohren gelesen wurde. Das Argument, mit dem Josephe La Canal das Konvent zur Finanzierung eines solchen Telegraphennetzes brachte, war die Einheit der Nation. Chappe bedankte sich nach der Vorführung seines Systems in einem Brief an La Canal für dessen „geniale Idee, an die ich gar nicht gedacht hatte. Die Einrichtung des Telegraphen ist in der Tat die beste Antwort auf jene Publizisten, die Frankreich für zu großflächig halten, um eine Republik zu werden." Mit dem Telegraphen schrumpfen die Entfernungen, riesige Bevölkerungsmassen werden gewissermaßen an einem Punkt versammelt.

Folie 2

Folie 3

Folie 4

Dass während der ersten 50 Jahre der Telegraph fast ausschließlich für militärische und polizeiliche Zwecke eingesetzt wurde, bestätigt Friedrich Kittlers Diktum von Medien als Missbrauch von Heeresgut. Für den Zeigertelegraphen wurde die Übertragungsgeschwindigkeit von 135 Kilometer pro Minute angegeben.

Die Eigenschaften von Elektrizität waren Ende des 18. Jahrhunderts weitgehend bekannt, seit der britische Physiker Steven Grey gegen 1730 gezeigt hatte, dass sie entlang eines Drahtes sich fortpflanzen kann, tauchten bereits erste Spekulationen darüber auf, dass sich damit Informationen übertragen ließen. 1834 ermittelte der Engländer Wheatstone eine Fortpflanzungsgeschwindigkeit der Elektrizität von 280.000 Meilen pro Sekunde. Die hohe Geschwindigkeit der Elektrizität sprengte den Denkrahmen der Nation und erweckte die Vorstellung, man könne damit über Tausende von Meilen mit dem Kaiser von China eine Unterhaltung führen. Es wurde deutlich, dass der elektrische Telegraph die ganze Welt umspannen müsse, 1848

schrieb Marx: „Das Bedürfnis nach einem stets ausgedehnteren Absatz für ihre Produkte jagt die Bourgeoisie über den ganzen Erdball." Die neue technische Möglichkeit passte also zum damals wütenden Kolonialismus.

Im 19. Jahrhundert werden die nationalen Netze zusammengeschaltet, 1850 wird ein Telegraphenkabel zwischen Dover und Calais gelegt, und acht Jahre später über den Atlantik. Das ist die Verbindung von Irland zu British America. Am 16. August 1858 weiht US-Präsident Buchanan das Transatlantikkabel ein, indem er Grüße mit Queen Victoria austauscht. Die Botschaft lautete: „Europa and America are united by telegraphy. Glory to God in the highest, on earth peace and goodwill towards man."

Der Rausch der Verbindung schürte die Hoffnung, eine universelle Durchsetzung der Prinzipien der Offenheit, wie Max Weber sie als Voraussetzung für den Markt identifizierte. Frieden, Freiheit, Gleichheit, Legalität. Medieninnovationen lassen die Angeschlossenen sich als Weltenbürger vorstellen. Das zeigte sich für die Schrift bei Diogenes und Demokrit und für den Buchdruck bei Danton. Das, was damals ein Kosmopolit hieß, formuliert sich am Weltpostsystem mit einem Wort von Siegert als „universelle Verbrüderung". Diese Hoffnung wurde im 1. Weltkrieg jedoch gründlich enttäuscht. Auch das Radio schürte in den Roaring Twenties Hoffnungen auf eine materielle Grundlegung eines Völkerbundes, die im 2. Weltkrieg dann enttäuscht wurden. Nur, um anhand des Fernsehens in der Nachkriegszeit dann erneut formuliert zu werden. Dem Glauben an eine universelle Menschlichkeit entspricht die komplementäre Vorstellung, dass die räumliche Trennung ein Übel sei, das an Konflikten, Hass und Missverständnissen schuld sei, und auch an sozialen Ungleichheiten. Wenn aber der Schrecken der Distanz und der Fremdheit die guten Menschen nicht gut sein lässt, dann wird die Selbstabschließung z. B. Chinas und Japans auch zu einem ethischen Skandal. Und seine militärische Öffnung mit Opiumkrieg und Commodore Perris schwarzen Schiffen, 1853 in der Bucht von Yokohama, ist gerechtfertigt. Übrigens im Interesse des Walfangs damals.

Giddens schrieb, die Moderne ist in ihrem inneren Wesen auf Globalisierung angelegt. Dahrendorf argumentierte, dass es notwendig eine Weltbürgergesellschaft geben müsse, weil es keine offene Gesellschaft in einem Land geben könne. Dieser Gedanke beerbt die expansive Dynamik von Christentum und Islam, die auf virtuell vollständige Konversion der Menschheit zielt. Er beerbt ferner die Logik des Kapitalismus und des Sozialismus, wobei dieser die Formulierung der Unmöglichkeit des „Sozialismus in einem Land" geprägt und jener in seiner Entgrenzung gesiegt hat. Das gleiche gilt von universalistischer Wahrheit, also keine Wissenschaft und keine Technologie in einem Land und universalistischer Ethik, keine Menschenrechte in einem Land und schließlich gilt in gleichem Sinne, keine Post, kein Telefon und kein Internet in einem Land.

Im Zeitalter der Kolonisierung gehört das Spektrum zu den am spätesten entdeckten Kontinenten. Erst 1868 gelang Heinrich Hertz der experimentelle Nachweis von elektromagnetischen Wellen. Ihr wichtigster Eroberer war zehn Jahre später Guillermo Marconi, der die Hertz'schen Wellen mit Patenten und einer Reihe von Unternehmen für die drahtlose Telegraphie nutzbar machte, vor allem für die Kommunikation mit Schiffen. Er bereitete damit den Weg für das Radio, und, wenn man den binären Morsecode als digitalen Datenfunk versteht, auch für WLAN und Mobilfunk. Anfangs war diese Ressource Spektrum unreguliert, Marconi hatte das Monopol für die Durchführung des Seefunks in England, baute sein eigenes weltweites Netzwerk auf, von dem er andere mit Hilfe von Patenten ausschloss.

Da sich Funkwellen nicht an Länder- und Unternehmensgrenzen halten, wurde die Notwendigkeit einer internationalen Koordinierung deutlich. Der Untergang der Titanic spielte dabei eine wichtige Rolle. Schon auf der zweiten internationalen Funkkonferenz 1906 war die diskriminierungsfreie Durchführung von Funkverkehr, unabhängig vom verwendeten Funksystem, festgelegt worden; das funktionierte aber offensichtlich nicht besonders gut. Die dritte Konferenz 1912 stand dann ganz im Zeichen der Titanic. Einer der Gründe für ihren Untergang war, dass mit Marconi-Geräten ausgerüstete Stationen nur untereinander kommunizieren konnten. Krisenhaft eine Lektion gelernt, lebenswichtige Kommunikationsinfrastruktur und Technologiemonopole gehen nicht gut zusammen.

Neben Punkt-zu-Punkt-Kommunikation eröffnen Funkwellen erstmals auch die Möglichkeit einer Zentrum-an-alle-Kommunikation. Auch der Rundfunk entsteht zunächst unreguliert. In den 1910er Jahren war der Selbstbau von Sendern und Empfängern ein beliebtes Hobby. Amateurfunkzeitschriften lieferten die Anleitungen. Leute verabredeten sich zu bestimmten Zeiten auf bestimmten Frequenzen um zu plaudern; einige Medienhistoriker sprechen von einem „Internet im Äther", das ebenfalls Raum für interessante „Was wäre, wenn"-Überlegungen bietet.

Doch es kam anders. In den USA wurde 1912 das erste Rundfunkgesetz erlassen; die öffentliche Ressource Spektrum durfte nur nutzen, wer eine Lizenz des Wirtschaftsministeriums beantragte. Dieser Ordnungsrahmen brach zusammen, als ein Gerichtsurteil im April 1926 entschied, dass das Wirtschaftsministerium gar keine Macht habe, die Radionutzung zu regulieren. Danach erhielt jeder Bewerber eine Sendelizenz ohne irgendwelche Auflagen über Frequenz, Sendestärken oder Sendezeit. In dieser Zeit der Konfusion und des Chaos, wie es hinterher genannt wurde, entstanden über 500 neue Radiostationen. Die meisten von ihnen strahlten mit Sendeleistungen von hunderten Kilowatt, um alle anderen zu übertönen, mit dem Ergebnis, dass niemand mehr zu hören war, Drahtzäune elektrisiert wurden und Menschen mit ihren Plomben Radio hörten. Die Zeit endete, als im Februar 1927 ein neues Funkgesetz erlassen wurde. Keine Regulierung ist also offensichtlich auch keine Lösung. In Deutschland wurde der Rundfunk in den frühen 1920ern zweifach reguliert: Für die störungsfreie technische Durchführung, also den Betrieb der Sendeanlagen, war die Reichspost zuständig, die Durchführung von Programmen wurde schon damals in der Kulturhoheit der Bundesländer gesehen. Ihre Zentralisierung unter den Nazis hatte bekanntlich böse Folgen. Nach 1945 entstand das Rundfunksystem daher wieder föderal, aber staatsfrei und unter der Kontrolle der Gesellschaft in Form der Rundfunkräte. Kommerziellen Rundfunk gab es in Europa erst mit der Vervielfachung der Übertragungskanäle durch Kabel und Satelliten ab Mitte der 1980er.

Ab Mitte der 1990er geht der Rundfunk ins Internet, also das soziotechnische System der Informatik schlechthin. Ich möchte hier nur auf den aktuellen Entwurf des 23. Rundfunkänderungsstaatsvertrags hinweisen; die Konsultation dazu endet heute

(30. September 2018, d. Red.). Darin werden neben Medienplattformen erstmals auch Medienintermediäre reguliert, also Suchmaschinen, Soziale Netze und User-Generated-Content-Portale, wie immer, bei allem, was aus dem Artikel 5 GG hervorgeht mit dem Ziel, vorherrschende Meinungsmacht zu verhindern und Meinungsvielfalt zu sichern. Auch hier zeigt sich, dass dem Entwurf mehr informatischer Sachverstand gutgetan hätte. Beispielsweise bei der Bestimmung der Aufgreifgrenzen für den sogenannten Bagatellrundfunk. Und für viele weitere Fragen ist ein solcher Sachverstand hilfreich, z. B. ist ein großes Thema heute die Aufmerksamkeitssteuerung, Empfehlungssysteme, die idealerweise ohne Personendaten auskommen und Filterblasen durchkreuzen.

Seit den Tagen der Konfusion und des Chaos werden Funkfrequenzen für Rundfunk, Polizeifunk, Radar usw. von den nationalen Regulierungsbehörden zugewiesen. Relativ früh, nämlich 1959, kam bereits die Idee auf, dass der Markt das vielleicht besser machen könnte; der britische Wirtschaftswissenschaftler Ronald Coes schlug vor, Frequenzbänder für die gesellschaftlich wertvollsten Nutzungen zu allozieren, das könne der Markt viel besser als eine staatliche Verwaltung. Damals musste er sich von der FCC, der damaligen Regulierungsbehörde, fragen lassen, ob sein Vorschlag ein großer Scherz sei. Ende der 1980er war die neoliberale Zeit dafür reif. Die Privatisierung der vormals öffentlichen Telcos und die zeitgleiche Mobilmachung der Telekommunikation löste eine Goldgräberstimmung aus. Internationale Konsortien ehemaliger staatlicher Telcos drängten in jeden sich öffnenden nationalen Markt. 1989 fand in Neuseeland die erste Versteigerung von Funkfrequenzen statt, die USA folgten 1994, in Europa fand die erste Spektrumsauktion 1996 in Deutschland statt, das bezog sich auf den Pager-Dienst ERNES, 1999 folgte dann die Versteigerung von Spektrum im 1.800-MHz-Band für GSM, den ersten digitalen Mobilfunkstandard.

Was wäre, wenn … es keinen Neoliberalismus und damit auch keine Liberalisierung z. B. des Telekom-Marktes gegeben hätte? Die Bundespost wäre voraussichtlich weiter für ICT zuständig. Statt TCP/IP hätten wir heute X.25ff. und ein ordentliches OSI.

Das dritte Modell bezeichnete die FCC auch als Spectrum Commons. Dafür gab es Vorbilder bereits 1938; interessant wurde es dann aber 1985, als die FCC drei Frequenzbänder, darunter das um 2,4 GHz für lizenzfreie Nutzung als sogenanntes ISM-Band freigab – für Industrial, Scientific, Medical – in der Branche auch als „Schrottband" bezeichnet. Mit Auflagen für zulässige Sendestärken und Antennenleistung, deren Einhaltung die FCC in ihrem Zulassungsverfahren für Geräte sicherstellt. Also keine Lizenzvergabe für Frequenzen sondern eine Zulassung von Geräten, die diese Frequenzen nutzen. Das führte nicht etwa zu Konfusion und Chaos sondern zu einer Fülle von Anwendungen wie drahtlose Telefone, Babyphones, Fernbedienungen und WLAN-Produkten. Die waren anfangs untereinander nicht kompatibel, bis eine Arbeitsgruppe der IEEE einen herstellerunabhängigen Standard für den Datenfunk entwickelte: Die 802.11-Familie, deren erster Vertreter 1997 erschien.

Ohne Monopol bilden sich Protokolle für ein einvernehmliches Miteinander auf einer geteilten öffentlichen Ressource. Innovationen in der effizienten digitalen Funknutzung werden gefördert.

Die Freigabe des 5-Ghz-Bandes wurde dann von allem von Apple in einem Verband der WLAN-Geräte-Hersteller, aber auch schon mit Unterstützung der nationalen Verbände der Bibliotheken und der Bildungsforschung vorangetrieben und 1997 erteilt. In Deutschland erfolgte die Allgemeinzuteilung des 2,4-GHz-Bandes 1995 und für das 5-GHz-Band 2002. Ich erzähle das nicht nur aus historischen Gründen. Die Spannung zwischen Versteigerung und Freilizensierung beschäftigt uns weiterhin. Im April 2019 steht die Versteigerung des 5-GHz-Frequenzspektrums an, die ist auf der World Radio Conference bereits beschlossene Sache. Offen ist, was nach der absehbaren Abschaltung von DVB-T2 mit diesem Filetstück im 700-MHz-Bereich passiert. Wird es wieder exklusiv an Mobilfunker versteigert oder frei lizensiert? Darüber wird auf der World Radio Conference Ende 2019 verhandelt. Mit bewährter TV-Whitespace-Technologie ist dieses Band ideal für Richtfunkstrecken um den „letzten Bauernhof" zu versorgen, ein Ziel, das die Bundesregierung offensichtlich bereits aufgegeben hat, da das auch mit 5G wieder nicht möglich sein wird, wie mit allen vorherigen Mobilfunktechnologien versprochen aber nicht eingelöst. Hier geht es also um Fragen von großer gesellschaftlicher Tragweite, die jedoch so kompliziert sind, dass nur Ingenieure, Nachrichtentechniker, Netzwerker oder Informatiker Argumente mit Gewicht in die Waagschale werfen.

Zugleich geht es um Fragen, in was für einer Gesellschaft wir leben wollen. In einer neoliberalen, in der der Markt als beste Lösung für alle Fragen gesehen wird, einschließlich für die Allokation öffentlicher Güter? In der Monopolisten zentralistische Systeme bauen und das öffentliche Interesse nur bei Marktversagen eingreifen darf? Oder in einer Welt mit Protokollen für ein Miteinander in dezentralen Systemen, in der wir Solidarität üben mit Schwachen und Bedürftigen – hier den letzten Bauernhöfen – und Entscheidungen im Gemeinwohlinteresse und nicht im Interesse von Unternehmen und Finanzinvestoren getroffen werden? Informatiker sind hier in ihrer Schlüsselrolle privilegiert, zu sprechen. Dazu müssen sie das eigene und das gemeinschaftliche Handeln im gesellschaftlichen Diskurs kritisch hinterfragen, heißt es in den neuen Ethischen Leitlinien der GI. Und weiter: „Das GI-Mitglied trägt Verantwortung für die sozialen und gesellschaftlichen Auswirkungen seiner Arbeit. Er soll durch seinen Einfluss auf die Positionierung, Vermarktung und Weiterentwicklung von IT-Systemen zu deren sozialverträglicher und nachhaltiger Verwendung beitragen." Die Herausbildung einer Professionsethik ist meist krisengetriggert. Es war die Erkenntnis, dass Informatikprodukte im Vietnamkrieg zu Töten helfen, die zur Gründung von Computer Professionals For Social Responsibility 1983 in den USA führte und, mit Joseph Weizenbaum als Brücke zwischen den beiden Welten, 1984 des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung. Im „about" des FIfF heißt es: „Die Gründungsmitglieder leisteten dem NATO-Doppelbeschluss offen Widerstand, sie wollten die Informations- und Kommunikationstechnologie vor allem als Mittel der Völkerverständigung genutzt wissen." Heute geht es weiter um den Missbrauch als Heeresgut, neben vielen weiteren Themen, aber auch um die toxische Kommunikation, die Völkerverständigung gefährdet.

Ich hatte mit globaler Konnektivität angefangen und möchte das zum Schluss noch einmal aufgreifen. Dinge durchzudenken ist Aufgabe der Wissenschaft. Die Koevolution von technischen, psychischen und sozialen Systemen läuft selten wie geplant. Wie

kann da die Informatik ihrer Selbstverpflichtung nachkommen, Handlungsalternativen im Hinblick auf die absehbaren Wirkungen und möglichen Folgen ihrer Systeme aufzuzeigen? Dazu keine Antworten, aber einige Überlegungen:

Erstens: Soziotechnische Systeme werden gebaut, um in die Interaktionen zwischen Menschen und Welt einzugreifen. Wir können nur bauen, was wir uns vorstellen können. Die Einbildungskraft in populären Visionen, Science Fiction usw., spielt dabei eine Rolle, ebenso vorherrschende und alternative Gesellschaftsmodelle, wie ein demokratischer Sozialstaat oder eben der Neoliberalismus. Diese Systeme werden in den seltensten Fällen aus ihrer Eigenlogik heraus gebaut, sondern im Auftrag, und Auftraggeber ist in den seltensten Fällen die Gesellschaft, sondern wirtschaftliche, wenn nicht gar militärische Interessen. Was aus dem Möglichkeitsraum, den eine Technik aufspannt, tatsächlich verwirklicht und ausgerollt wird, entscheiden meist wirtschaftliche und politische Faktoren.

Zweitens: Einmal in der Welt, formen soziotechnische Systeme uns, auf verschiedene Weisen: Sie werden zu Dingen, zu Metaphern, mit denen wir denken, über uns und die Welt. Z. B. Friedrich Hayek, der hier das Preissystem als ein System der Telekommunikation bezeichnet und Wirtschaftssteuerer vergleicht mit Ingenieuren, die ihre Messinstrumente beobachten und dann entsprechende Änderungen vornehmen. Das Beispiel, um zum einen hinzuweisen auf die ungeheure Attraktivität, die darin liegt, Komplexität auf eine einzige Zahl zu reduzieren: Eine Fülle wirtschaftlicher Faktoren auf den Preis, die Komplexität menschlichen Verhaltens auf einen Social Score in China. Und damit auch die Attraktivität, die davon ausgeht, Komplexität sozialer Fragen an technisch-algorithmische Systeme zu delegieren, deren Antwort dann wieder eine Zahl ist, z. B. 42. Aber auch, natürlich, der Hinweis auf einen der Gründerväter des Neoliberalismus, der den Gebrauch, den wir heute von technischen Systemen machen, seit 40 Jahren maßgeblich bestimmt hat. Z. B. Sherry Turkle, die ebenfalls über die letzten 40 Jahre nachgezeichnet hat, wie der Computer als „evokatives Objekt", wie sie das nennt, psychischen Systemen dafür dient, ihr Selbst- und Weltverhältnis zu konstruieren.

Soziotechnische Systeme formen uns natürlich nicht nur als Metaphern, z. B. das Fitness-Armband, das ich mir als Feedback für mein eigenes Training zulege, gibt es nur mit App, die Daten ins Netz schickt. Gamification lockt mich dann in den Wettbewerb mit anderen, meine Krankenkasse lockt mich mit Vergünstigungen, wenn ich ihr Zugang gebe.

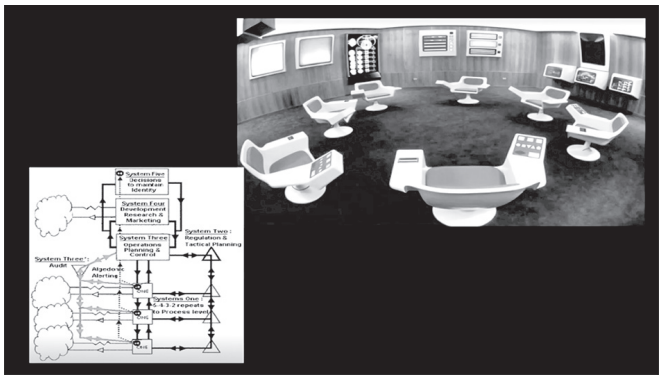
Drittens: Mit einmal Gestalten und dann gestaltet werden ist es natürlich nicht getan, auch eingeführte Technologien werden in ihrem Gebrauch zu etwas anderem, z. B. SMS. Die war für den Notfall gedacht, wenn eine Voice-Verbindung fehlschlägt, und ist zu einem eigenen Medium geworden. Der ursprüngliche Konzeptvorschlag für einen Short Message Service wurde von Friedhelm Hillebrand von der Deutschen Bundespost 1984 erarbeitet und im Februar 1985 in die GS-Standardisierung eingebracht. Er legte u. a. die Länge auf 160 Zeichen fest, weil er festgestellt hatte, dass die meisten Postkarten und Telexe weniger als 160 Zeichen enthielten. Niemand hätte gedacht, dass Menschen, die einen breitbandigen Sprachkanal oder sogar Videotelefonie zur Verfügung haben, die beschränkte Tastaturkombination in nennenswertem Umfang nutzen würden. Hier ein BBC-Beitrag zur „Generation Mute": Ein Anfang-20jähriger, der gefragt wird, wann er das letzte Mal telefoniert habe, und er sagt, hmm, ich kann mich nicht so richtig daran erinnern, wenn ich es genau überlege, habe ich noch nie telefoniert. Und natürlich geht es dabei nicht nur um SMS, sonder vor allem um Messenger, aber die Idee ist natürlich dieselbe, die Nutzungsform, und kennzeichnet eine überraschende Wende von Voice- oder gar Bildtelefonie zu Text, und damit auch die Verkehrung des Smartphones zum kleinen Computer für alles andere, außer zum Telefonieren.

Viertens: Technologie ist also gestaltbar, durch ihr Design mit seinen impliziten Nutzungen, durch seine tatsächlichen Nutzungen, durch Regulierung und Förderung im öffentlichen Interesse, durch Selbstregulierung in Gremien wie IEEE und IETF. Also geht die Frage auf die Ziele der Gestaltung, z. B. zentral vs. dezentral. Das scheinen mir Strukturelemente zu sein, die für soziale wie für technische Systeme relevant sind und damit einen guten Common Ground für interdisziplinäre Verständigung bieten. „Wir wollen keine zentralisierten Infrastrukturen, die von globalen, intransparenten Konzernen betrieben werden, sondern dezentralisierte und selbstverwaltete Systeme", heißt es in der Ankündigung dieser FIfFKon. Klar, lieber Mastodon als Facebook. Lieber Peer-to-Peer als Client-Server. Lieber jeder ihr eigener Server als die Cloud. Auf der EuropeanaTec im April diesen Jahres gab es ein Panel zu der Frage; die Bibliotheksinformatiker bekannten dort: „Unser Herz schlägt für dezentral, aber oft sind zentrale Elemente praktisch." Und schließlich: Das Internet selbst ist dezentral, was die Herausbildung der US-Giganten aber auch nicht verhindert hat. Vielleicht und sehr wahrscheinlich wird es letztlich immer um die Machtfrage gehen. So, wie es kein richtiges Leben im Falschen geben kann, kann es auch keine richtige Technologie geben.

Volker Grassmuck

Volker Grassmuck, Mediensoziologe, freier Autor und Aktivist. Er hat an der Freien Universität Berlin, der Tokyo Universität, der Humboldt-Universität zu Berlin und der Universität São Paulo über die Wissensordnung digitaler Medien, Urheberrecht und Wissensallmende studiert und geforscht. Sein jüngstes Forschungsprojekt, *Grundversorgung 2.0* (2012-2015) am Zentrum Digitale Kulturen (CDC) der Leuphana Universität Lüneburg, fragte nach der Zukunft des öffentlich-rechtlichen Rundfunks. Er hat die Konferenzserie *Wizards-of-OS.org* und das Informationsportal zum Urheberrecht *iRights.info* geleitet, die Initiativen *mikro-berlin.org*, *privatkopie.net* und *CompartilhamentoLegal.org* mit gegründet, ist Vorstandsmitglied des Digitale Gesellschaft e. V., Mitglied von C-Base.org und C3S.cc und bloggt unter *www.vgrass.de.*

Z. B. die Kybernetik. Die passte als Steuerungstheorie und -praxis sowohl in einen wissenschaftlichen Sozialismus wie Kapitalismus. Anfang der 1970er erlebte Chile unter Salvador Allende einen kurzen Sommer der Kybernetik. (Also nicht wörtlich, sondern das waren zwei Jahre.) CyberSyn für Cybernetic Synergy sollte ein Rückkopplungssystem werden, das relevante Informationen liefert und alle in die sozialistisch-demokratische Steuerung einschließt. Die Idee zu einer demokratischen, datengestützten Planwirtschaft stammt vom damaligen Finanzminister Fernando Flores, der den britischen Management-Kybernetiker Stafford Beer hinzuholte. Der Militärputsch von Pinochet setzte dem Experiment ein Ende und der wunderbare Kontrollraum [Folie 5] ist dann ziemlich schnell danach zerstört worden.



Folie 5

Fast 50 Jahre später sehen wir heute ein weiteres, neues kybernetisches Großmodell, den Social Score im „sozialistischen Kapitalismus" – so nennen die sich tatsächlich – Chinas. Nur dass hier nicht Produktions- und andere Gesellschaftsdaten allen zur Entscheidungsfindung zugänglich gemacht werden, sondern Personendaten von allen der Partei. Aber auch den Bürgern untereinander, die in einer gamifizierten Rückkopplung aufeinander achten, um das allgemeine Wohlverhalten zu stärken.

Meine letzte „Was wäre, wenn"-Frage: Können wir uns eine Gesellschaft vorstellen, in der Big Data „for good" verwendet wird? In der Sachfragen faktengestützt, interdisziplinär und mit breiter Beteiligung einer dazu befähigten Bevölkerung behandelt werden? Ob Entscheidungen über die Nutzung des elektromagnetischen Spektrums, Maßnahmen zu Zivilisierung des Online-Gesprächs, Vielfaltsfördernde Meinungstechnologien wie Empfehlungssysteme, die Gefahren und Chancen der KI. In der die reale Macht vom Volke ausgeht und das die so als gemeinwohlfördernd etablierten Entscheidungen auch tatsächlich umsetzen kann. In der die Koevolution von technischen, psychischen und sozialen Systemen tatsächlich zu der Völkerverständigung führt, die IKT inhärent immer versprochen hat.

Mehr Fragen als Antworten. Ich bin sicher, alle Anwesenden haben bereits die Erfahrung gemacht, dass weder Philosophie, Psychologie noch Politologie oder Soziologie der Informatik Handreichungen geben kann, wie sie ihrer Verantwortung für soziotechnische Systeme gerecht werden kann. Diese Antworten können nur im interdisziplinären Gespräch und im Gespräch mit der Gesellschaft gefunden werden und ich freue mich darüber, dass das FIfF genau solche Gespräche führt und Räume wie diese FIfFKon anbietet, wo ein solches Gespräch möglich ist. Wenn ich mir zum Schluss noch etwas wünschen dürfte, dann, dass das FIfF viel häufiger sein Gewicht in die Waagschale der öffentlichen Diskussion wirft. Vielen Dank.

FIfF-Konferenz 2018

Gemeinwohl, Demokratie und gute Arbeit in der digitalen Gesellschaft – Von Macht und Mitgestaltung

Verschriftlichung des Vortrags von Annette Mühlberg

Manche Menschen kaufen sich ganze Städte oder Teile davon, doch der damit verbundenen Gestaltungsmacht ist bislang wenig entgegengesetzt worden. Denn es geht nicht – wie etwa bei Le Corbusier – um das Unterbringen der eigenen ArbeiterInnen, sondern viel wesentlicher um Macht und Kontrolle von Verkehr, Kommunikation, Energie und Arbeit kompletter urbaner Räume. Technische Zentralisierung unterminiert etwa die rechtlich und politisch gebotene Gewaltenteilung und die Mitbestimmung von lokalen Behörden.

Was also ist die demokratische Antwort darauf? Wir müssen neue Regularien finden, insbesondere auch für die Arbeitswelt mit ihren sehr bestimmenden Machtasymmetrien. Dies drückt sich u. a. auch ganz konkret in demokratisch auszuhandelnden Anforderungen an die dort verwendeten IT-Systeme aus. Fachleute aus Informatik, Recht oder Politik müssen dafür ebenfalls einbezogen werden.

Ich rede heute nicht nur zu Smart Cities, sondern allgemein über die Frage von Gemeinwohldemokratie und guter Arbeit in der digitalen Gesellschaft und wurde gebeten, auch dieses ganz speziell nochmal aus dem Blickwinkel von Macht und Mitgestaltungsmöglichkeiten zu beleuchten.

Das trifft sich gut, weil ver.di seit einiger Zeit jährlich einen Kongress veranstaltet, der sich mit den Fragen der Digitalisierung von Arbeitswelt und Gesellschaft auseinandersetzt und gerade in diesem Jahr galt er dem Thema „Gemeinwohl in der digital vernetzten Gesellschaft". Wir arbeiten daran, denn wir begreifen uns als Mitgestalter, sowohl als Arbeitnehmerinnen und Arbeitnehmer, als auch als Bürger. Und als solche stellen wir Anforderungen an die Rahmenbedingungen von Arbeitswelt und Gesellschaft. Besonders wichtig für uns ist, dass wir über eine Vision unseres Gemeinwesens verfügen, die nicht die Interessen von Digitalunternehmen ins Zentrum stellt sondern vielmehr die Bedürfnisse von Menschen als Bürger und Beschäftigte.

Es stellt sich die Frage, welchen technischen und ethischen Kriterien die Gestaltung unserer IT-Infrastrukturen und Arbeits- und Geschäftsprozessen unterliegen muss, damit wir in Freiheit,

selbstbestimmt und demokratisch leben und arbeiten können, in Würde, solidarisch, sozial gerecht und nachhaltig.

Wie also können wir diese fantastische digitale Technik zum Wohle aller nutzen, ohne Freiheits- und Persönlichkeitsrechte aufzugeben, ohne in technische Abhängigkeiten von Herstellern und in Lock-in-Effekte zu geraten, ohne unsere Sicherheit zu gefährden und kritische Infrastrukturen und notwendige Dienstleistungen „hack-bar" zu machen, ohne politische und ökonomische Machtkonzentrationen zu fördern und ohne in einen globalen Strudel von Lohn- und Sozialdumping zu geraten. Wie können wir das Prozesswissen der arbeitenden Menschen für Innovationen nutzen? Welche Kriterien sind relevant für die demokratische Gestaltung unserer IT-Infrastrukturen? Welche rechtlichen Rahmenbedingungen und politischen Initiativen benötigen wir, um das Gemeinwohl wachsen und gedeihen zu lassen? Hierzu hat ver.di bereits von zehn Jahren das Berliner Manifest zu Daseinsvorsorge in der Informationsgesellschaft verabschiedet, das wir in diesem Jahr mit einem Update versehen wollen.

So sahen die Überschriften damals aus:

1. Grundversorgung und offener Zugang!
2. Wissen teilen, Wissen mehren!
3. Keine Privatisierung öffentlicher Güter im virtuellen Raum!
4. Selbstverwaltung und öffentliche Steuerungsfähigkeit stärken!
5. Verlässliche demokratische Verfahren und Standards!
6. E-Government mit offenen Standards!
7. Kritische Infrastrukturen sichern!
8. Daten- und Persönlichkeitsschutz verwirklichen!
9. E-Demokratie für ArbeitnehmerInnen, Mitbestimmung stärken!
10. Öffentliche Daseinsvorsorge nicht IT-Lobbyisten überlassen!

Eine zentrale Herausforderung für Arbeitswelt und Gesellschaft heute ist, dass uns die demokratische Steuerungsfähigkeit und Entscheidungshoheit nicht entgleitet und dass Prozesse überhaupt noch mitgestaltbar und mitbestimmbar sind.

Angesichts der ungeheuren Finanzkraft einzelner Personen und Unternehmen, die in der Lage sind, ganze Stadtteile und Landstriche mit Wohnungen und Betrieben und Agrarland aufzukaufen müssen wir uns vor der Möglichkeit eines solchen Ausverkaufs schützen.

Bill Gates hat sogar angekündigt, gleich eine ganze Stadt, eine Smart City in der Wüste von Arizona zu errichten. Er hat das Geld dafür. Ihm geht es dabei nicht um die Schaffung des so dringend benötigten sozialen Wohnraums, ihm geht es nicht um Initiativen von neuem Wohnen kombiniert mit neuer Technik, wie es mal bei Le Corbusier oder Ernst May oder noch, genau vor 150 Jahren dem Unternehmer Staub am Herzen lag, gute Wohnungen zu schaffen, die auch mit einer guten Infrastruktur ausgestattet sind. Nein, ihm geht es darum, die Dinge des alltäglichen Lebens zentral zu steuern mittels digitaler High-Speed-Netzwerke.

Wir müssen uns auch vor Quasi-Privatisierungen in acht nehmen. Zum Beispiel wurde in Kanada die Gestaltung eines ganzen Stadtviertels von Toronto an die Google-Tochter Sidewalk Labs übertragen. „Stadtluft macht frei", heißt es, doch damit ist es vorbei, wenn Smart Cities nach den Interessen von Technologiekonzernen geformt werden. Und ich habe gestern nochmal in Wikipedia nachgeguckt, und da stand dann drin, ich zitiere: „… hochentwickelte Smart City kann ein Internet of Things and Services sein. Die gesamte städtische Umgebung ist dabei mit Sensoren versehen, die sämtliche erfassten Daten in der Cloud verfügbar machen: So entsteht eine permanente Interaktion zwischen Stadtbewohnern und der sie umgebenden Technologie. Die Stadtbewohner werden so Teil der technischen Infrastruktur einer Stadt." Das nenne ich menschenzentriert, das nenne ich richtig cool. Kein Wunder, dass der BigBrotherAward dieses Jahr an ein solches Konzept von Smart City ging.

Es gibt auch Staaten, die solche totalitären Infrastrukturkonzepte vorantreiben wollen. Und was macht unsere öffentliche Hand? Sie sucht sich zumeist mit Auslagerungen, Privatisierungen und Verkauf öffentlichen Eigentums zu helfen, statt offensiv neue Aufgaben zu Sicherung von Demokratie und Gemeinwohl zu übernehmen. Dabei könnte sie auch ihre Marktmacht nutzen, um mittels kluger Richtlinien zur Vergabe soziale und gemeinwohlorientierte Strategien umzusetzen. Barcelona gibt dafür ein gutes Beispiel.

Berliner Manifest – Update

Es gäbe viel für die öffentliche Hand zu tun und ich steige gleich in ein Update unseres Manifests ein, und die Fortentwicklung der Kriterien, auf die wir bei der Gestaltung von Arbeitswelt und Gesellschaft achten sollten.

Grundversorgung und offener Zugang

Wir brauchen dringend Bezahlsysteme, die nicht bei jedem Online-Einkauf zur Personalisierung beitragen. Ich möchte das noch ergänzen um entsprechende Liefersysteme, denn wir wollen ja online nicht nur das Lesen von Artikeln bezahlen können, sondern auch Produkte, die wir bestellen, empfangen können.

Wissen teilen, Wissen mehren. Innovative Angebote der öffentlichen Hand: Gute Tools für alle

Die öffentliche Hand sollte endlich die Verantwortung zur Gewährleistung datenschutztechnisch sauberer Kommunikati-

onstools übernehmen. Wir brauchen dringend Alternativen zu WhatsApp, GoogleDocs, Skype und natürlich auch vernünftige Verschlüsselungstools.

Keine Privatisierung öffentlicher Güter im virtuellen Raum. Schaffung neuer Gemeingüter

Wir sollten Open-Data-Strategien so anlegen, dass sie sich den Daten öffentlicher Relevanz widmen, seien sie aus dem öffentlichen oder auch privaten Sektor. Dabei muss sichergestellt werden, dass keine personenbeziehbaren Daten verwendet werden und sie auch nicht im Kontext von Big Data deanonymisiert werden können. Ich denke, da haben wir einen heftigen Brocken vor uns und müssen uns alle gemeinsam Gedanken machen.

Selbstverwaltung und öffentliche Steuerungsfähigkeit stärken

Die demokratische Steuerungsfähigkeit ist das A und O und Volker [Grassmuck] hat schon vorhin die Vorteile der Dezentralität erläutert (siehe ab Seite 40 in diesem Heft); wir müssen das wirklich auch als ein Demokratieelement betrachten.

Verlässliche demokratische Verfahren und Standards

Wenn wir Freiheit und Demokratie erhalten wollen, dann dürfen wir unser Leben und unser gesellschaftliches Tun nicht nach Scoring-Punkten ausrichten. Es wurde schon mehrfach auf dieser Konferenz erwähnt, aber man kann es gar nicht oft genug sagen: das ist der Bereich, wo wir wirklich initiativ werden müssen. Wir wollen kein chinesisches Credit-Score-System, das per Punktesystem das Sozialverhalten seiner Bürger einstuft. Punkte, die über das Zustandekommen oder eben Nicht-Zustandekommen von Mietverträgen entscheiden können, von Krediten, Krankenversicherungen und Arbeitsverhältnissen. Dieser Gefahr müssen wir offensiv und strukturell begegnen. Wir müssen konzeptionell unsere IT-Infrastrukturen, Arbeits- und Geschäftsprozesse so ausrichten, dass sie einem Social Scoring entgegenstehen. Und konzeptionell heißt auch langfristig und missbrauchsresistent. Wir haben jetzt gerade den Hack mit Facebook erlebt, missbrauchsresistent war das definitiv nicht. D. h., wir müssen auch beim Aufbau von personalisierten Bürgerkonten Vorsicht walten lassen, damit aus solchen nicht schnell auch noch Bürgerakten werden können. Und eins muss klar sein: Man muss sich im digital vernetzten Raum frei bewegen können, ohne dass man zu einem üblen Kuhhandel gezwungen wird, der da heißt: Grund- und Verbraucherrechte gegen den Zugang zu elementaren Dienstleistungen wie Stromversorgung, Fernsehen, Gesundheits- und Autoversicherungen. Hier muss privacy-by-design gelten. Und wie sich das Private und das Berufliche vermischt, das kann ich genau am Beispiel Autoversicherungen mal darstellen: Wir haben Situationen, wo Betriebsräte vor die Frage gestellt werden, ob sie den Deal eingehen und sagen, sie stimmen einer Totalüberwachung beim Autofahren zu, weil dann die Versicherung billiger wird, und dafür gibt es dann ein paar Goodies und Leckerle im Betrieb selbst, als Ausgleich. Hier werden ganz konkret die Beschäftigtenrechte durch Autoversicherungspraktiken herausgefordert.

Technologische Souveränität, öffentlich relevante Infrastrukturen mit offenen Standards

Des Weiteren müssen wir für technologische Souveränität sorgen, wobei freie Software und offene Standards wichtige Faktoren sind. Der Staat darf nicht in technische Abhängigkeiten geraten – er ist schon drin, aber er sollte nicht drin sein – und muss die Wahrung der Persönlichkeitsrechte bei seinen Angeboten, z. B. Suchfunktionen auf Web-Seiten von staatlichen Krankenhäusern – gewährleisten, und darf diese nicht an Google abtreten.

Kritische Infrastrukturen sichern

Wir müssen prüfen, ob die Plattformökonomie neue, kritische Versorgungsinfrastrukturen erzeugt hat, die wir sichern müssen. Wenn Pflegeleistungen über Plattformen vermittelt werden, dann gehören solche zu kritischen Infrastrukturen, und wenn Wasser- und Getränkelieferungen nur noch über Plattformen funktionieren, dann gehört auch dies zu kritischen Infrastrukturen, und all dieses müssen wir uns vergegenwärtigen.

Wir benötigen, wie es auch in der Smart-City-Erklärung von netzpolitik.org betont wird, bei kritischen Infrastrukturen analoge Backup-Systeme und entsprechend sowohl digital als auch analog geschultes Personal für solche Fälle.

Daten- und Persönlichkeitsschutz verwirklichen

Wir wollen den Datenschutz und die Persönlichkeitsrechte verwirklichen, auch und gerade in der Arbeitswelt. Hier gilt es, die Auswirkung neuer Technik auf die Beschäftigten zu prüfen bevor sie eingeführt wird. Und ich richte dieses nicht nur als Appell, sondern das ist ein elementarer Bestandteil, über den wir mit Informatikerinnen und Informatikern unbedingt reden müssen, denn es geht darum, die Technik schon im Interesse der Beschäftigten zu gestalten.

Ich nenne hier als Beispiele die Armbänder zum Tracken von Bewegungen und Körperfunktionen, die Stimmanalyse zur Bewertung des Emotionszustandes sowie Anforderungen an Beschäftigte, sich Chips implantieren zu lassen. Nicht schön, wäre aber toll, wenn die Messung unserer alleinigen Kontrolle unterliegen würde.

Beschäftigtendatenschutz verwirklichen

Und das hier ist richtig ernst: In Call-Centern soll die Stimmanalyse mittels Künstlicher Intelligenz regeln, dass die Aufträge nur an die Kollegen gehen, deren emotionaler Zustand auf eine hohe Wahrscheinlichkeit eines guten Verkaufsabschlusses schließen lässt. Was bedeutet das? Du sitzt da, hast eine Runde zuviel gegähnt beim ersten Gespräch und – schwupps – bist Du draußen. Du kriegst keinen Auftrag mehr. Wie Du Deine Miete bezahlst, ist der KI egal, die Chance ist vorbei, hier haben wir wirklich ein elementares Problem und ich frage mich, wo bleibt da die Würde das Mitarbeiters, wie steht es um die ethischen Kriterien bei der Entwicklung solcher Totalüberwachungssoftware?

Der Economist hat im März zur KI-Bespitzelung am Arbeitsplatz ein eigenes Heft entwickelt, ich kann nur sagen: Das lohnt sich.

RFID-Chips, Magnete, Sensoren kennen wir als Arbeitstools in Kleidern, Brillen und Geräten, doch nun werden sie nicht mehr nur außerhalb des Körpers eingesetzt, sondern direkt in den menschlichen Körper implantiert. Nicht zur Verbesserung der Gesundheit oder als Selbstexperiment sondern mit dem Motiv der Zurichtung des Menschen auf einen ganz bestimmten Arbeitsplatz. Das gibt es bereits, und zwar nicht irgendwo transatlantisch, sondern im europäischen Schweden, wo im Zentrum für High-Tech-Start-Ups den Mitarbeitern ein Mikrochip unter die Haut ihres Handrückens operiert wird; damit lassen sich Türen öffnen, Kopierer bedienen und perspektivisch Arbeitsunterlagen darauf speichern; die Kollegen sollten damit gelockt werden, dass sie ja ihren Kaffee dann auch ganz easy mit einer Handbewegung bezahlen können.

Mitbestimmung stärken

Mit so einer Praxis gehen nicht nur gesundheitliche Gefährdungen einher, sondern auch Fremdbestimmung und Kontrolle. Auch deshalb ist es wichtig, die Mitbestimmung zu stärken. Und natürlich wird in Zeiten von Künstlicher Intelligenz die Tranparenz und Nachvollziehbarkeit von automatisierten Entscheidungsprozessen immer wichtiger. Sie ist die Voraussetzung für die Mitbestimmbarkeit und Mitgestaltbarkeit, denn eine Black Box kann man weder demokratisch kontrollieren, noch auf sicherheitsrelevante Abläufe prüfen.

Strategie der Bundesregierung zu KI neu ausrichten

Die Bundesregierung hat gerade eine Strategie zu Künstlicher Intelligenz vorgelegt und dazu einen Konsultationsprozess eröffnet. Ich möchte hier ein paar Punkte aus gewerkschaftlicher Sicht darlegen: Dazu gehört, dass wir klare Ethikregelungen mit Grundwertbindungen für systemrelevante Infrastrukturen fordern, Rechenschaftspflichten, die Definition von Verantwortlichkeiten und das Verbot autonomer Waffensysteme, die Kennzeichnungspflicht für Chatbots, die Offenlegung der Verteilung von Rationalisierungsgewinnen – dies ermöglicht wiederum die Re-Investition von KI-Gewinnen zugunsten gesellschaftlicher Bedarfsfelder, sozialer Innovation und Qualifizierung – und wir treten ein für die gründliche Erprobung und somit konzeptionelle Entschleunigung bei der Umsetzung autonomer Entscheidungsprozesse.

Gute Arbeit fördern

Wir wollen gute Arbeit fördern, dazu gehört unter anderem digitale Mündigkeit, Weiterbildung, gesundes Arbeiten verbunden mit einem zeitweiligen Recht auf Telearbeit und einem Recht auf „log off". Ich denke, es ist allen bekannt, der Burn-Out hat dramatisch zugenommen und es besteht ein direkter Zusammenhang in der Entgrenzung der Arbeit und der Arbeitszeit, insofern sind das ganz wichtige Faktoren.

Solidarsysteme erhalten

Wir wollen die Solidarsysteme erhalten und soziale Sicherheit auch unter den Bedingungen der Plattformökologie gewährleisten. Ich nehme an, viele kennen das Statement von Lukas Biewald, der davon schwärmte:

> *„Ohne das Internet wäre es richtig schwer gewesen, jemanden zu finden und zehn Minuten für sich arbeiten zu lassen und dann zu feuern. Aber jetzt mit der Technologie findet man sie, zahlt ihnen winzige Geldbeträge und wird sie los, wenn man sie nicht mehr braucht."*
> *(Lukas Biewald, zitiert nach Marvit in: The Nation, 04.02.2010)*

Sie sehen, das erzeugt Handlungsbedarf. Wir sehen das anders als er und kümmern uns aktiv um faire Standards und gute Entlohnung, um Autonomie ohne Prekarität, um Sozialpartnerschaft statt Willkürherrschaft. Und – Stichwort Willkürherrschaft – möchte ich kurz noch einmal auf das Phänomen Uber eingehen, was hier gottseidank noch nicht ganz so verbreitet ist, aber es gibt ja starke Tendenzen, es doch mehr zuzulassen. Wir haben hier mit der Plattform-Ökonomie eine neue Situation, wo gerade die Akteure, die immer super-viel Transparenz überall fordern, selber total intransparent handeln, wo ein System entsteht, wo de facto Arbeitgeber sagen: „Wir sind nur Plattformbetreiber, wir haben damit gar nichts zu tun, wir übernehmen keinerlei Verantwortung", können aber diejenigen, die ihren Lebensunterhalt als De-Facto-Taxifahrer verdienen, ohne Ankündigung, ohne Information, denn es gibt ja keinen Vertrag, von der Plattform aus-

Annette Mühlberg

Annette Mühlberg leitet bei der Vereinten Dienstleistungsgewerkschaft (ver.di) die Projektgruppe *Digitalisierung* und ist im Bereich Politik und Planung zuständig für digitale Arbeit, Netzpolitik, E-Government. Sie engagiert sich für Demokratie, Gemeinwohl und Gute Arbeit in der digital vernetzten Welt. Bereits 2003 war sie Mitglied der Regierungsdelegation zum Weltgipfel zur Informationsgesellschaft; 2005 wurde sie in die Internetnutzervertretung von ICANN und 2010 als Sachverständige in die Enquête-Kommission des Deutschen Bundestags zu *Internet und digitale Gesellschaft* berufen. Sie vertritt ver.di beim Konsortium für *Online-Plattform-Genossenschaften* sowie beim Steering Committee des deutschen Internet Governance Forums. Sie ist Autorin von Artikeln zu Arbeitswelt, Demokratie und gemeinwohlorientierter Infrastruktur im Kontext von Digitalisierung und entwickelte Bausteine für E-Government-Dienstvereinbarungen.

schließen. Das ist dramatisch, das sind Zustände, das ist Wildwest, das können wir so nicht dulden und nicht tolerieren als demokratische Gesellschaft, deshalb ist es wirklich wichtig, dass wir hier vorangehen und sagen, wir brauchen dafür klare Regelungen.

Gemeinwohl nicht IT-Lobbyisten überlassen

Wir wollen neue und innovative Wege gehen, das sollte auch der Staat im Sinne des Gemeinwohls, mit neuen Bümdnispartnern, wie beispielsweise Onlineplattform-Genossenschaften, weil da ist das dann ganz anders gelagert, da haben die Beschäftigten selbst die Kontrolle über die Gestaltung dieser Plattformen und die Regularien. Der Staat sollte für soziale Standards Sorge tragen und sich auch um die künftige Finanzierung der Daseinsvorsorge kümmern. Auch da möchte ich kurz an das gestrige Referat anknüpfen und sagen ja, das ist sehr wichtig, dass wir uns auch um Steuern kümmern insofern das Modell Tax-by-Design auch im Kopf haben. Die Persönlichkeitsrechte sind elementare Voraussetzungen für die Demokratie, die spezifische Machtasymmetrie zwischen Arbeitgebern und Arbeitnehmern erfordern ein eigenes Beschäftigtendatenschutzgesetz.

FIfF-Konferenz 2018

Protective Optimization Technologies (POT): The revolution will not be optimized?

Verschriftlichung des Vortrags von Seda Gürses[1]

In the 1990s, software engineering shifted from packaged software and PCs to services and clouds, enabling distributed architectures that incorporate real-time feedback from users. In the process, digital systems became layers of technologies metricized under the authority of objective functions.

These functions drive selection of software features, service integration, cloud usage, user interaction and growth, customer service, and environmental capture, among others. Whereas information systems focused on storage, processing and transport of information, and organizing knowledge – with associated risks of surveillance – contemporary systems leverage the knowledge they gather to not only understand the world, but also to optimize it, seeking maximum extraction of economic value through the capture and manipulation of people's activities and environments. The ability of these optimization systems to treat the world not as a static place to be known, but as one to sense and co-create, poses social risks and harms such as social sorting, mass manipulation, asymmetrical concentration of resources, majority dominance, and minority erasure. In the vocabulary of optimization, these harms arise due to choosing inadequate objective functions. During the talk, I will provide an account of what we mean by optimization systems, detail their externalities and make a proposition for Protective Optimization Technologies.

Prolog: Funding matters

Zunächst eine kleine Ankündigung: Wir haben kürzlich eine Kritik an der Auswahl der privaten Sponsoren für Privacy-Konferenzen formuliert, die mittlerweile in vielen Ländern sehr üblich geworden ist. Wir haben mit einem eindeutigen Beispiel angefangen: Palantir ist bekannt dafür, Überwachungssysteme für Polizei- und Geheimdienstbehörden zu entwickeln, und ist einer der Hauptsponsoren der Amsterdam Privacy Conference. Wir haben die Organisatoren gebeten, das zu ändern. Bisher haben wir keine befriedigende Antwort erhalten. Wir wollen die Kritik ausweiten, ausgehend von Palantir, wo das Problem offensichtlich ist. Ebenso gibt es berechtigte Einwände gegen Google, Facebook, Amazon und zahlreiche andere Sponsoren im Kontext von Privacy-Konferenzen. Wir müssen eine breite Diskussion darüber führen. Mittlerweile haben wir über 200 Unterschriften. Sie sind eingeladen, das heute auch zu unterzeichnen oder einfach die Diskussion auch in Deutschland fortzuführen, wo es Konferenzen gibt, die von problematischen Zusammenstellungen von Sponsoren getragen werden.

Zusammenfassung

Es geht wesentlichen um drei Punkte: (1) Ich werde differenzieren, was Künstliche Intelligenz in der Wissenschaft, auf dem

Markt und in der Technologiepolitik ist. Für die letzten beiden möchte ich betonen, dass hier in der Vergangenheit schon viele Investitionen in beliebige Technologien gemacht worden sind. Es gibt also ein großes Angebot an Investitionen und es es wird versucht, durch die Technologiepolitik einen Bedarf zu schaffen. Es ist sozusagen eine umgekehrte Ökonomie. (2) Wir hören seit 60 Jahren, dass Künstliche Intelligenz kommt und die Welt ändert, und ich habe das Gefühl, dass das, was als Künstliche In-

telligenz bezeichnet wird, sich komplett geändert hat. Es wird immer gesagt, Künstliche Intelligenz kommt, aber es ist immer etwas anderes, was kommt. Das führt zu einer Art von moralischer Panik, so dass Städte und Institutionen und Staaten immer mehr Geld investieren, damit diese Investitionen überhaupt erfolgreich werden. Zudem wird in den Künstliche-Intelligenz-Diskussionen, nicht in der Wissenschaft, aber in der Technologiepolitik, immer von abstrakten Technologien gesprochen. (3) Ich werde heute die Perspektive auf diese Technologien mit einem Blick auf den Wandel der Praxis der Softwareentwicklung beleuchten. Ich werde nicht diskutieren was Künstliche Intelligenz und diese abstrakten Technologien sind, aber ich werde fragen: Wie sieht Softwareentwicklung aus, wie hat sie sich verändert und wie hängt das damit zusammen, was jetzt Künstliche Intelligenz genannt wird? Ich werde zeigen, dass wir mittlerweile sehr datenintensive Services haben: Software wird nicht mehr als Produkt, sondern als Service angeboten werden, Services, die dann innerhalb der Logik von Optimierung funktionieren.

Es geht hier um die Optimierung aller Software-Umgebungen und Populationen. Wir müssen ausgiebig darüber diskutieren. Ich werde mich hier auf die externen Kosten der Optimierungen konzentrieren. Jedes optimierte System birgt externe Kosten, Externalitäten, die durch die Optimierung entstehen. Diese sollten einerseits internalisiert werden, das heißt Technologiefirmen sollten diese Kosten tragen, andererseits sollten wir als Nutzer auch von außen Widerstand leisten können. Die Idee von POTs, Protective Optimization Technologies, baut auf die Idee von PETs auf, Privacy Enhancing Technologies. Analog zur Idee, Werkzeuge zu entwickeln, die Nutzer befähigt, ihre Privacy sozusagen selbst schützen zu können, sollen Nutzer sich auch vor den durch Optimierungen verursachten Externalitäten schützen können. Wir wissen, dass solche Schutzmechanismen nicht revolutionär sind, und die strukturellen Probleme von Daten und Optimierungen nicht völlig lösen, aber sie sind ein hilfreicher und wichtiger Zwischenschritt auf dem Weg zu einer Lösung.

Introduction: Artificial Intelligence – waiting for Godot

Waiting for Artificial Intelligence is like waiting for Godot. It is about creating a demand for an investment that is in the process of creating an immense supply. Artificial Intelligence has been coming for 60 years. However, what we referred to Artificial Intelligence 60 years ago is different from its manifestation today. And probably this will hold for whatever is claimed to be the Artificial Intelligence in the future. And we have not only been waiting for Artificial Intelligence. Consortia of tech companies first asked us in the last 20 years to expect things like the Internet of Things. That was in the beginning of the 2000s, for those who are old enough, and it was following the trends in the 90s in research labs like Xerox Parc where people said we will not get the Internet of Things, but we will get Ubiquitous Computing. What we instead got, instead of Ubiquitious Computing, was Social Networks.

First, governments, companies, and journalists alike argued that Social Networks would lead to revolutions and bring to us democracy – and also bring democracy even in the authoritarian world. In the last three years now we hear the Social Networks bring authoritarians to democracies. So there is an underlying logic to the argument that there is a technology that is unstoppable, inevitable, revolutionary and we should prepare ourself for receiving it.

Demand for technological solutions is constructed

First of all, what is expressed as unstoppable technological change is in fact a story about companies already investing in a technology, meaning they are already creating a supply. The objective of waiting for the technology is to create an expectation that its arrival is inevitable, and its reception is welcome – a necessary condition for economic and social progress and therewith creating a demand. In the current case of Artificial Intelligence the argument is that if your health system, your city, your car, your policing are not "smart", i.e. not made "smart" with Artificial Intelligence, you are going to fall behind. Hence cities, health and educational institutions demand it and do so without much regulation.

So the moral panic that is then surrounding this promised technology, Artificial Intelligence, is part of creating a demand. We are told that Artificial Intelligence will deliver an industrial revolution, a market revolution. However, it may also cause some problems. These include for example, according to A.I. Now, that we might lose jobs, experience bias and exclusion, have an infringement upon rights and liberties and may have problems with safeties in critical infrastructures – a short, but very worrying list.

However, this is a list that again creates moral panic. And remarkably this moral panic is cultivated with industry funded think tanks, which have apparent ties with universities who make them look very neutral. Both start from the assumption that these technologies will come, but only with limited side effects. These research centers and think tanks ask us not only to expect these technologies, but to imagine how we will live with them once they arrive, how they should be tweaked to better fit our lifes. But it's only about tweaking, and never about questioning whether we should get these technologies or not.

One of the recent manifestations of this approach is an effort to achieve algorithmic fairness which would take too much time right now to elaborate in detail. But we clearly see in the algorithmic fairness that it is merely about tweaking algorithms, but not actually questioning whether the introduction of some of these systems will cause inequalities which are much grander than what can be corrected by any tools. Well, it is signifcant in all of these framings of artificial intelligence coming, that they allow those engaged in the topic not to name any actual actors who are engaged in the political economy of Artificial Intelligence.

Artificial Intelligence is an abstraction, very much like algorithms, big data and internet of things are all abstractions. Abstraction also suggests nobody is pushing for them, they just come from the sky, they fall upon us. In this notion Artificial Intelligence can be abstractly discussed and criticised as if technologies are neutral and are only colored by the shortcomings of the world around them. This is manifest in statements like "Algorithms are not biased. They do not discriminate, but the data sets represent our bias as a society and the algorithms reflect them back to us." Algorithms in that sense are presented like neutral mirrors. They just present us to ourselves. It is conceived as an accident rather

than the condition enabled by the ways in which we produce knowledge and technology.

As an alternative to this abstraction and as an alternative to this idea that artificial intelligence is inevitable and it's coming, I want to look at the past. I propose that we analyze software engineering practices and systems developments which are made possible through concrete social economic production decisions. I locate some of the origins of the current discussions on Artificial Intelligence in the shifts of software engineering from shrink wrap software and Personal Computers to services and clouds which allow software developers and companies to incorporate real-time feedback from users and their environments in the business and software development processes.

So here are the three shifts that we see at least since the 1990s. If you have been in the computer business since the 1960s you will actually see a pendulum where we used to have mainframes and services, it went to PCs and coming back. What we see now since the 1990s is the starting with shrink wrap software, waterfall models, and personal computers to what I would say is services, agile programming, and the cloud.

Interlude: "Shrink wrap software" and "waterfall model"

Formerly customers went to a shop to buy software in a box. It came with a plastic wrap around it, that was the shrink wrap. And when they opened the shrink wrap they went into a contractual agreement with the software company before even installing it. Then they took the disquettes home and installed it on their Personal Computer, if all went well had the software ready and started using it. The relationship with the company was mostly at this moment where the customer opened the box. And afterwards what they did with the software was mostly their own issue, unless people used illegal copies of the software and the companies came after this illegitimit use.

The waterfall model is a form of developing software. It came about in the 1960s. If you look at the history of sofware engineering, there is always a battle of people who think software engineering is a managing issue, that it is just breaking down tasks and managing them well, and others who think that it is a matter of experts building systems bottom-up. What we have seen in change is the waterfall model which was much more managerial and top-down being questioned in the last 20 years by agile programming. Developers who propose a whole host of different methods which I am calling agile programming that would basically put the developers and the users at the center of software engineering. And finally with a shift of services we moved away from having a lot of processing done on our computers to the cloud – what will be elaborated in more detail below.

We did an exploratory study including interviews and conversations, analysis of industry white papers and legal and policy literature to understand the phenomenon we call the agile turn – the change of the environment that we live in and its great impact on the development of privacy, but also the corresponding kinds of protective technologies we can create. To give you a feeling about the excitement around shrink wrap let me refer to a video of the Windows 95 release party[2], where people are dancing and celebrating the the new release of the Windows OS. Releasing software was something that happened every two or three years. Apparently, in Microsoft literally after the release everybody would get up and change their position in the offices in this very large company. Windows 95 was like such a big party, it was a big thing to release new software versions. But what we have seen today with services is that software developers can release software updates up to 50 times an hour, a day, whatever, depending on the company. So we can not party as much, something has fundamentally changed.

From shrink wrap software to services

I will start with the move from shrink wrap to services and focus on one or two incidents that provide some insight: There is this one statement, some people claim this was a note sent by Jeff Bezos to his employees in 2001 or 2002, where he basically said: "All the teams will henceforth expose their data and functionalities through service interfaces." So he pushed all his Amazon's workforce into creating interfaces for their databases and making their services available internally, but also externally, which could also be seen as the start of the Amazon cloud that we know today.

Another example, if we just go to the extreme – shrink wrap on the one side and services on the other is between Microsoft Word and Office 365 or Google Docs. Think about the difference in the experience: In the beginning you ran installed software on your machine and you were also maintaining your machine. Customers hoped that the software in the box mapped their hardware. This was not a trivial thing and a big headache for developers. Users had a lot of control. This was seen as a problem for many people, but not for geeks. Also, users paid in advance.

With services however, what we have is that we have no installation anymore, unless maybe installing your browser or an app which is much easier in comparison to what users had to do formerly. The update and maintenance of the code remains on the developer side, because the code remains where the developer is. There is no release party where developers have to let go off their "baby". It actually sticks with them, they can continue to make changes to the code, they can always do updates. And with services what we have, also interesting for the users, is that they don't have this much control. Everything they do can now be datified. Develeopers can basically see where the users are clicking, what services they are using, or how they are using the features.

But it also allows things like user collaboration. Formerly users sent Word documents, or Open Documents if using open source alternatives, through e-mails and then there were all sorts of versioning problems. This new environment basically allows collaboration to be much more easy.

What also changes is that you pay as you use. This is where of course the term "you pay with your data" comes in as well. Formerly users didn't pay with their data when they bought Microsoft Word, they paid for the license or got an illegal copy, but now users can basically pay per use or even try software before

moving it to the whole enterprise. So it's a very big shift both for the users and the developers.

So if we look at what this whole shift means is that we have now a server-client model. That means that the transaction that was only at the moment of purchasing shrink wrap software is now throughout the use lifecycle, users are constantly in transaction with the company. We have bundled services, and we have licensing and pricing models that are basically based on use, which means intensified tracking to know who is using what and how. This is especially important, because often we talk about tracking as a problem of the advertisement world but we do not talk about it also as part of the service and licensing architectures. These are important little details.

So basically there were two different phases: production and use. What happened with the services is that developers start producing the software, and do not produce everything themselves. They integrate a bunch of services that have already existed somewhere. Then the users using the service, for instance with a pay-per-use model on-going. While users are paying for the use of the software, the production is still going on. The production and the consumption phases are collapsed, there is no separate production from use. Everything they use is integrated into how this software gets produced.

If you think for example of a website to create pictures, this website might have some specific application features for uploading photos and filters. But the developers do not want to develop things like advertisement, authentication or payment themselves. So they integrate a third party service that allows payments for instance. The same with functionalities to locate pictures or use a social network for discussion, etc. Basically the service provider will integrate numbers of third services into the website. For the users it looks like they are interacting with one party, but in fact behind the surface they are interacting with a couple and hundreds of service providers, which they mostly not not know all.

What's also interesting is that this service model also applies to the developement process. The developers themselves use a number of services to develop software. Anywhere from team integration tools, to data brokers to get data about your users or analytics like Google Analytics to test your features, or for A/B-testing. You basically use a bunch of other services to even develop the service itself. So also these are hardly visible to the users. For example FullStory was a service that a website could integrate it to give the developers a complete replay of the users' interactions in a video form. So this did not not just reveal clicks, but basically showed completely how users moved around the website, which services they used, what things they typed into the boxes that were in the forms, etc. We found that in the top one million sites we already had quite a few of the websites using this service. Colleagues at Princeton even wrote out about how they could actually see people's logging credentials and private information using FullStory.

The background why developers probably are integrating FullStory is to see if the users have problems with their services and where did they struggle with certain kind of interface elements. But it actually ends up being like a privacy nightmare. And it becomes very difficult to make these things visible to the users.

The agile turn

Another main change we see is the move from waterfall to agile programming.[3] The waterfall model was basically a model of software engineering with discrete development-phases that come one after the other and finally lead to the final software programme. The company starts with a requirement analysis and specification. Software engineers go into the company to understand what the requirements of the system were or go to the environment where a system is going to be introduced. Then the requirements are turned into a specification. Afterwards they do architectural design and start implementing and integrating the software. Two or three years later the software is ready, and the engineers go back to the company who ordered the software and start doing verification and testing to see that what was produced in the last years has anything to do with what the company originally wanted. Then engineers go into the mode of operation and maintenance.

Then it turned out that with this model roughly about two thirds of the projects failed. Failed meant that they either failed completely or they failed in terms of costs, they cost much, much more than it was estimated or it took much, much longer to develop. So this model was not really working, especially from an economic perspective which is really important in my line of argument here. It also turned out that 60 % of software costs is due to maintenance and of that 60 % is adding new functionality to legacy software. So you can imagine that when service architectures came and the code could remain on the side of developers, the companies that were losing so much money and basically bleeding with these waterfall models were very happy. And so were the developers who claimed the Agile Manifesto.

Here are basically, in a very quick and unfair manner, the main principles of agile programming:

- Individuals and interactions over processes and tools: It is very interesting what gets left out here and how that actually impacts the practice of development: The process itself is gone.
- Working software over comprehensive documentation: If you think about the European General Data Protection Regulation you see the conflict with its obligations on documentation.
- Customer collaboration over contract negotiation: It is very much about reducing costs, and there goes the requirements document.
- Responding to change rather than following a plan.

Of course, there are many different approaches of Agile Programming. Another approach is called Extreme Programming which says a lot about getting things even faster and which is very focused on exhaustive testing.

What happens with the move to agile development methods is that testing becomes very central. So does user centricity or client centricity most of the times. Because we have services and we can constantly collect data about how features are being used,

we can also do all sorts of testing using that data. Accordingly, it is no longer about testing the correctness of software but testing the interactions. Development is supposed to be in short iterations. So in order to develop a photo album service, developers start with the uploading and then go feature by feature what and every step they iterate and test to see how the users are reacting. Another goal is simplicity, a main goal is re-use and modularity which means to break things down as much as possible.

Optimization

What we start getting as a result of all these developments is a feature based optimiziation. What we start seeing is that if software development was a cost issue with services and with the kind of data we can collect, it comes completely out under the logic of optimization. So when Annette Mühlberg in this issue is talking about workers being put under the logic of optimization or municipalities or health systems, we see also software developers are put under the logic of optimization and all the resources they use as well. That becomes possible because we have services and because we have agile methods.

With services you can capture the behavior of the users, in order to constantly adjust the features, to know which are the features that lead to maximizing profit. We can economically optimize while we are optimizing for example for clicks. But the tracking included in services is not limited to tracking the users. For example, when integrating a service into a website, there is a need to also track those services themselves. Developers need to know that the services are all functioning the way they should be, because their products are dependent on external parties for the services to run. There is a lot of tracking going on to make sure that the service ecosystem is functioning. Finally there are literally layers and layers of tracking to see how many resources are used, which services are working, user tracking and license tracking – we are seeing a whole sort of ecosystem of tracking and optimization that is going on.

Implications and externalities – optimization in practice

Finally I want to give an example in location-based services, Waze. Many people use Waze to reroute around traffic. It is similar to Google Maps, also owned by Google, but does not just give directions, but it tells you how to get there in the fastest way possible. Waze is symbolic of how location-based services have changed with the move to services. Location services no longer just track and profile individuals to generate spatial intelligence, but they now leverage this information to manipulate users' behavior and create ideal geographies that optimize space and time to their investors' interest. So part of this development are population experiments using techniques like A/B testing that drive iterative design in order to ensure sufficient gain for most users while maximizing profits. Waze reroutes users even when there is congestion on a given path allowing these users to act with perfect selfishness. In some happy universe if everybody could get as fast as possible from A to B, you would think this is a good thing. But it turns out, researches from Berkeley showed, that traffic apps might work for the indivdual, but they do so at the cost of making congestion worse over all. Waze also often redirects users off the highways through suburban neighbourhoods that cannot sustain heavy traffic. So while it's useful for drivers, it affects neighbourhoods by making streets busy, noisy and less safe.

Consequently, towns may need to fix and police roads more often. With such systems even when some users benefit, non-users and the environments they inhabit may bear the ill effects of optimization. So this underlines the point that actually the traffic engineers that looked at it show that if only a few users are using Waze they do get from A to B faster, but if everybody starts using Waze there is just chaos.

What are we proposing? Optimization systems have these externalities and we have many, many reports that the companies do not react when people say: Look, my neighbourhood is destroyed, because Waze is rerouting this traffic. Annette Mühlberg had a lot of examples of workers getting weird messaging from their bosses, because they took pauses, etc. There are all these externalities and the companies will not take them seriously. So could we maybe do something else? And we decided to be inspired by the users of these systems for exploring new ways to deal with these things. Namely we found out that people who live in these suburban areas that do not want the Waze traffic will start reporting road blocks on their streets so that Waze would reroute to another road.

So here are some examples: In one of them somebody did a virtual road block. Apparently even the police has a problem, because people can log for example whether there is a police control and speed limit, etc. So they started over-populating Waze so that people do not have the correct information. There were some researchers in Israel that created a bunch of ghost accounts and managed to make it look like there is a lot of traffic on the freeway, got all the cars rerouted and then had the freeway to themselves. Our idea is that we want to be inspired by how these users have been looking at manipulating optimization systems, re-optimize themselves and the environments that they live in. We want to design tools that actually are effective and allow them to do so in a much more successful way. Basically, in computer science terms what we are saying is optimization systems are machine learning systems at this point. What we can do is use adverserial machine learning to re-optimize the conditions of the users and their environments when they are hit hard by optimization systems.

We published a paper on what we mean by POT and how to develop them, but basically we propose that you think of a benefit function.[4] Let's say Waze has a benefit function for all the people including non-users and the environment. The people who benefit the most are on the top-hill, they are happy users and then the ones who are messed up when cars start spying into their yards, because it is a road that shouldn't have that much traffic. They are the ones that are not getting a very big benefit. We think about what kind of inputs we can do to change this curve, the outcome of this optimization system. The question is what should it be changed to? There we have different strategies.

And really Waze is not the only place this happens. For example Pokémon Go, if you are into collecting Pokémons it turns out

that if you are in a very poor neighbourhood, if you are in rural areas, you are not gonna get a lot of Pokémons. So what the users have been doing is spoofing their GPS so they go to main cities. They even changed the map indicators in Open Street Map to make it look like there are things like water sources, which apparently will lead to spawning more Pokémons. Uber drivers have been known to turn off their apps when a big event is happening so that they can induce search prices so that can be paid well. We have been looking at credit scoring outcomes and asked if you could change for example the amount of money you ask for – in order to more likely to get a credit from the bank. You can read more about our empirical work in the referenced paper.

Conclusion: The cost of optimization

What is at stake with all this? Agile software engineering seems like an efficient way to create software. But what is at stake is that all of a sudden all of our lifes are put under the logic of optimization. All of the social activities that are touched with services are put under the logic of optimization. Think about what it means to put all sorts of social things into a logic of logistics and control. Also politically, often what we get is based on the idea that the outcome is is in some way "optimal" and therefore we are supposed to desire these systems.

There is a lot happening there with this switch from information systems to optimization systems. Trying to summarize what has changed we can say: Not only we went from shrink wrap to services and software engineering has changed, but the quality of the systems has changed. Whereas information systems are focused on storage, processing, transport of information and organize knowledge and are thus about knowing, knowledge and reasoning, optimization systems are not about knowing at all. They basically leverage the data that they gather, to not only understand the world, but optimizing it.

Optimization systems seek to extract economic value through the capture and manipulation of people's activities and environments. All of these services constantly capture your activities, they capture information about our environments. They don't care to know, they care to manipulate in order for improving the economic income. Consequently optimization systems in comparison to information systems treat the world not as a static place to be known, but one to sense and co-create. This is very, very different kind of systems. The kind of problems that we can see with optimization systems have been on the headlines, they have been spoken about by academics and activists for a long time:

- Social sorting – we hear a lot about algorithmic discrimination, but originally academics started talking about this problem in the 1990s;
- mass manipulation – we hear about Cambridge Analytics and the elections;
- asymmetrical concentration of powers – we have the GAFAM: Google, Apple, Facebook, Amazon, and Microsoft;
- absolute majority dominance – where minority users get hunted down almost and there's very little done to protect the minorities.

So these are the ways we talk about these things in general, but if we look at software engineering we can talk about the phenomenons in terms of optimization.

Software engineering has become data-centric and it functions under the logic of optimization. What can we say about these things in terms of optimization systems? We argue that optimization systems come with externalities. There is no optimization system without these problems. There is no "good" optimization goal without those problems. Optimization systems always come with externalities. This is not a complete list, but here is a start: They disregard non-users for sure, see the examples given above. They disregard environments that they function in. They make use of them.

There is an optimization curve and some people are optimal and some people are not. Developers have to explore the world, they sometimes have to try new things out which might lead to exploit users to explore things. The costs and risks associated with that exploration mostly falls on the shoulders of the users.

Anmerkungen

1 *Der vorliegende Vortrag basiert auf zwei Papieren, in denen sich weiterführende Referenzen finden: Gürses S und Van Hoboken J (2017) Privacy after the agile turn. In The Cambridge Handbook of Consumer Privacy, 1–29. Cambridge Univ. Press und Overdorf R, Kulynych B, Balsa E, Troncoso C und Gürses S. POTs (2018) Protective Optimization Technologies. arXiv:1806.02711 [cs], 7. Juni 2018. http://arxiv.org/abs/1806.02711.*

2 *https://www.youtube.com/watch?v=84c7mRP7PLw*

3 *If you believe in one of these things I am going to do a bad job in explaining your color of agile development. I am very, very sorry. I am just giving a very broad overview.*

4 *https://arxiv.org/abs/1806.02711*

Seda Gürses

Seda Gürses ist Informatikerin, Post-Doc am COSIC/ESAT im Department of Electrical Engineering der KU Leuven, Belgien, und forscht am Center for Information Technology and Policy, Princeton University. Sie arbeitet u. a. zu den Themen Privatsphäre in sozialen Online-Netzwerken und der Rolle von subjektiven Vorstellungen im IT-Design.

Virtueller Einbruch – Update des Staatstrojaners

Verschriftlichung des Vortrags von Constanze Kurz

Das erste höchstrichterliche Urteil zum Staatstrojaner stammt schon aus dem Jahr 2008. Seither konnten keine Bundesregierung und kein Innenminister von dem Vorhaben lassen, zu versuchen, das staatliche Hacking in das Arsenal der Ermittlungswerkzeuge aufzunehmen.

In der letzten Legislaturperiode nun wurde der Staatstrojaner als normales Ermittlungsinstrument für Dutzende Straftaten erlaubt. Die technisch ziemlich komplexe Aufgabe, einen Staatstrojaner zur Anwendung zu bringen, bereitet den Behörden bis heute Probleme. Und viele ungelöste Fragen bestehen vor und beim Einsatz der Schadsoftware noch immer. Der Vortrag gibt einen Überblick über den Stand der Dinge bei deutschen Staatstrojanern und spart natürlich auch nicht mit Forderungen, was zu tun wäre.

Im Folgenden möchte ich tatsächlich ein Update geben. Dabei habe ich mir ein lustiges Wortspiel erlaubt, denn „Update des Staatstrojaners" kann man natürlich auch im technischen Sinne verstehen und der Kampf um diese Schadsoftware dauert inzwischen zehn Jahre. Ich will aber nicht die gesamte Geschichte abreißen, sondern mir geht es um folgende Fragen: Wo stehen wir zur Zeit in Bezug auf den Staatstrojaner und welche Entwicklungen haben sich in jüngster Zeit ergeben? Wie sind die politischen Entscheidungen und die des Gesetzgebers gefallen?

Vorgeschichte: Bundesverfassungsgerichtsurteil von 2008

Ich möchte nicht verhehlen, dass ich selbst Teil dieser Entwicklung war. Mehrmals war ich Sachverständige bei Staatstrojanern, bin erklärter Gegner von Staatstrojanern, habe aber auch gute Argumente, die ich im Rahmen dieses Updates darstellen werde. Der Begriff des „virtuellen Einbruchs" im Titel ist natürlich eine etwa so blöde Metapher wie der der „Online-Durchsuchung". Denn ein Einbruch zeichnet sich in der Regel nicht dadurch aus, dass man eine dauerhafte Schadsoftware auf einem System hinterlässt oder dass man die Tür für einen Dritten offen lässt. Ich bitte daher, den etwas unkorrekten Titel zu entschuldigen.

Über die folgenden Dinge werde ich nicht reden: Ich werde nicht nochmal zum 27. Februar 2008 zurückgehen, an dem das erste Urteil zum Staatstrojaner gefallen ist. Ein sehr wichtiges Urteil, das ich auf gar keinen Fall geringschätzen möchte. Denn in diesem über zehn Jahre alten Urteil haben wir ein neues Grundrecht geschenkt bekommen: das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Auf dieses Grundrecht werde ich mehrfach zu sprechen kommen.

Ausgangspunkt: Staatstrojaner-Hack von 2011

Mein Ausgangspunkt wird aber – damit ein paar Jahre der Entwicklung des Staatstrojaners gekürzt werden können – der Staatstrojaner-Hack vom Oktober 2011 sein. Auf den Hack selbst brauche ich nicht im Detail einzugehen. Wer das möchte, kann zwei technische Berichte von uns dazu lesen, die sehr genau sind. Wie sich herausstellte war die damals relativ weit verbreitete Software der hessischen Firma Digitask nicht nur handwerklich unterirdisch schlecht, sie eröffnete auch Dritten die Möglichkeit, die Schadsoftware mit zu nutzen. Ihr Hauptproblem aber war, dass die rechtlichen Grenzen, die damals gesetzt waren, mit dieser Software nicht eingehalten werden konnten. Dies hatte neben der politischen Diskussion – wir hatten ja die Binaries eines dieser Staatstrojaner veröffentlicht – auch einige konkrete Folgen, auf die ich kurz zu sprechen kommen möchte, um zu vergleichen, was tatsächlich in der Folge umgesetzt wurde.

Zum einen wurde eine standardisierende Leistungsbeschreibung erdacht. Eine interessante Sache, die es davor offenbar nicht gegeben hatte. Digitask war zwar bereits seit 2001 als technischer Dienstleister zertifiziert, man hatte aber offenbar keine Form von Pflichtenheft oder anderer standardisierender Leistungsbeschreibung erstellt. Nun wurde also versucht, technisch zu spezifizieren, was dieser Staatstrojaner eigentlich können soll und wie er technisch umzusetzen sei, damit die gesetzlichen Grenzen nicht überschritten werden.

Zum anderen entschied man sich für eine BKA-Eigenentwicklung. Anders als heute ging es damals immer nur um das BKA und um Fälle schwerer Verbrechen, insbesondere Terrorismus. Tatsächlich ist bis heute der internationale Terrorismus im BKA-Gesetz die Klammer für den Einsatz des Staatstrojaners. Das betrifft nicht einmal den NSU, sondern nur internationalen Terrorismus. Diese Beschränkung hat sich in der letzten Zeit, besonders in den letzten zwei Jahren, komplett aufgelöst. Tatsache ist etwa, dass der Einsatz des Staatstrojaners in einigen geplanten oder schon verabschiedeten Landespolizeigesetzen vorgesehen ist. Darauf komme ich später zurück.

Ich habe also diesen Ausgangspunkt gewählt, weil er ein politisch entscheidender Punkt war. Damals kamen relativ viele Informationen über den tatsächlichen praktischen Einsatz von

Staatstrojanern heraus. Dies auch, weil die Opposition in vielen Landtagen kritisch nachfragte und es in Bezug auf die politische Kommunikation noch eine andere Zeit war. Heute ist es wesentlich so, dass die Bundesregierung gar nichts mehr sagt. Alles ist nunmehr *national security* und die Herausgabe zu vieler Informationen an die Öffentlichkeit würde vorgeblich dem Projekt des Staatstrojaners zuwiderlaufen.

Kommerzielle Anbieter

Neben der BKA-Eigenentwicklung gab es aber auch noch einen anderen Strang, der besonders für die technische Weiterentwicklung des Staatstrojaners wichtig wird. Man hatte sich nämlich entschlossen, trotz der Eigenentwicklung auch bei kommerziellen Anbietern einzukaufen und über Firmen haben wir im Laufe der Zeit (immerhin von 2011 bis heute, also 2018) viel mehr Informationen sammeln können. Dies zum einen, da Gruppen – und hier ist insbesondere das Citizen Lab aus Kanada zu nennen – sehr detaillierte Berichte über staatliche Hacking-Software erstellt haben. Zum anderen hat die Presse mehr über die Überwachungsindustrie recherchiert.

Wir wissen also mehr über diese Anbieter und ihre Produkte. In Deutschland ist das insbesondere *FinSpy* der Firma FinFisher. Sehr schön passend zum zehnjährigen Jubiläum des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität kommunikationstechnischer Systeme wurde im Februar dieses Jahres dieser kommerzielle Trojaner freigegeben. Ob er tatsächlich eingesetzt wird, ist unbekannt. Wer also über ein Exemplar davon verfügt, wird um Übergabe gebeten. Seitdem ist es auf jeden Fall möglich, dass das BKA diesen Trojaner einsetzt. Offenbar erfüllt er die Anforderungen. Überprüfbar ist das nicht, von keiner Behörde, denn nach wie vor ist es auch nicht vorgesehen, dass diese kommerziellen Partner den Quellcode der Software herausrücken.

Auch den Aufsichtsbehörden – namentlich der für das BKA zuständigen Bundesbeauftragten für den Datenschutz – ist der Einblick verwehrt. Falls jemand Lust hat, sich etwas über die Firma FinFisher zu informieren: die haben ganz sicher Blut an ihren Händen. Die haben wenig Hemmungen mit den Diktaturen dieser Welt zusammenzuarbeiten und mittlerweile ist über die eine Menge bekannt. Die Bundesregierung hat dies bisher in keinster Weise dabei gestört, FinFisher als Geschäftspartner überhaupt in Erwägung zu ziehen und letzlich mit ihnen ins Geschäft zu kommen.

In den Landtagen verhält es sich etwas anders. Ich war auch in einigen Polizeigesetzgebungsprozessen Sachverständige und mein Eindruck war, dass in den Landtagen einige (auch regierende) Parteien sehr wohl Bedenken haben, mit solchen Firmen ins Geschäft zu kommen. Eine konkrete Regelung, die das untersagen würde, hat allerdings keines der bereits beschlossenen oder im Entwurf befindlichen Landespolizeigesetze enthalten.

Das bedeutet, dass dieser zweite Strang weiterhin existiert, der hinsichtlich der technischen Potenz in einer anderen Liga spielt. Das ist eine in vielen Beispielen getestete Software, die in Videos, wo sie beworben wird, wie in Verkaufsveranstaltungen lamadeckenartig vertickt wird. Ich glaube es gibt ein anderes Geschäftsfeld, wo man in diesen Hacking- und Überwachungsfirmenmarkt auch staatliche Gelder investiert.

Das Urteil zum BKA-Gesetz …

Ich möchte zum zweiten Urteil kommen. Die meisten werden wissen, dass es ein weiteres Urteil zum Staatstrojaner gab, allerdings in einer in verschiedener Hinsicht anderen Konstellation als zehn Jahre zuvor. Es gab auch hier eine lange Anhörung und man hat auch wieder technische Sachverständige angehört, was nicht selbstverständlich für ein Gerichtsverfahren ist, bei dem natürlich zuvörderst die juristische Perspektive interessiert. Die Anhörung dauerte sechseinhalb Stunden. Das BKA-Gesetz, das im Mittelpunkt des Rechtsstreits stand, war hochkomplex und wies neben dem Staatstrojaner sehr viele weitere Elemente auf, die enorm umstritten waren. Darunter auch andere technische Überwachungsmaßnahmen, die Übermittlung von Überwachungsdaten ins Ausland, aber auch die Frage des internationalen Terrorismus, der sich wie eine Klammer um dieses BKA-Gesetz herum befindet, und seine Definition.

Ich würde sagen, dass sich ungefähr ein Drittel der Anhörungen nur mit dem Staatstrojaner beschäftigt hat und zwar in beiden Varianten. Diese beiden Varianten, die Quellen-TKÜ (Quellen-Telekommunikationsüberwachung) und die Online-Durchsuchung, gibt es nach wie vor. Sie unterscheiden sich darin, dass die Onlinedurchsuchung uneingeschränkt das gesamte informationstechnische System durchleuchtet und daraus Daten ausleiten kann, während die Quellen-TKÜ ihre Grenze in der laufenden Kommunikation hat, zumindest annähernd. Das Urteil ist in Bezug auf den Staatstrojaner in beiden Varianten enttäuschend, weil es keine weiteren Sicherungen enthält, die an das Urteil von 2008 anschlössen und weil es letztlich die Festlegung manifestiert, dass es angeblich zwei verschiedene Arten von Staatstrojanern gäbe – nämlich einen für das Gesamtsystem und einen weiteren für die laufende Kommunikation.

Mir ist, generell gesagt, schon damals sehr aufgefallen, dass dieses Urteil einen gewissen Zeitgeist ausdrückt. Der Minister Thomas de Maizière ist, was nicht häufig vorkommt, selbst vor Gericht erschienen und hat eine sehr emotionale Rede für technische Überwachungsmaßnahmen im Fall des internationalen Terrorismus gehalten, die das Verfahren aus meiner Sicht stark beeinflusst hat. Dies nicht nur, weil er selbst Jurist ist, sondern auch weil er die Gefahren und den ganzen Zeitgeist, der sich mit der Terrorismusabwehr verbunden hat, sehr dezidiert vorgetragen hat. Man hat sehr deutlich gemerkt, dass der verhandelnde Senat nicht mehr derselbe war wie zehn Jahre zuvor unter Hans-Jürgen Papier und dem Berichterstatter Hoffmann-Riem. Das drückt sich auch im Urteil klar aus. Zwischen den Zeilen ist zu lesen, dass man im Falle von Terrorismus eigentlich Verständnis für Staatstrojaner habe. Das hat sich sehr gewandelt und war hier sehr greifbar. Der Wandel deutete sich vorher schon an. In der Verhandlung zum Anti-Terror-Gesetz, an der ich ebenfalls teilnahm, etwa zum Thema der Datenbank, die sich mit der Terror-Datei verbindet, hatte man das auch schon gemerkt, aber hier viel deutlicher.

Ein weiteres Problem war, dass es sich um ein fünf Jahre währendes, sehr komplexes Verfahren handelte. In der Verfassungsbeschwerde wurden sehr viele verschiedene Punkte angeführt und da eine neue Regierung an der Macht war, die das Gesetz gar nicht gemacht hatte, wurde die Politisierung sehr schwer. Die politische Diskussion war aus meiner Sicht auch schwieriger als beim Urteil zuvor.

Ein Vorteil war allerdings, dass die Öffentlichkeit viel besser als 2007/2008 darüber informiert war, was so ein Trojaner eigentlich bedeutet und was er kann. Damals hatten ich und die anderen Sachverständigen vor allem erklärbärt. Nun war die Öffentlichkeit schon aufgrund der Tatsache, dass man in jeder Zeitung über Schad- und Spionagesoftware lesen kann, viel besser informiert.

Das Verfahren bekam große Aufmerksamkeit, aber im Ergebnis ist zumindest für die Varianten des Staatstrojaners wenig gewonnen. Zwar sind Teile des BKA-Gesetzes verfassungswidrig und der Gesetzgeber musste Änderungen vornehmen, aber er hat sicherlich ein schwächeres Signal als 2008 erhalten.

… und seine politischen Folgen

Ich möchte damit zu den politischen Folgen kommen. Das ist mir sehr wichtig. Der damalige Innenminister de Maizière hat sich noch am selben Tag vor die Presse gestellt und mehrfach betont, dass er dieses Urteil vollumfänglich ausnutzen wolle, im Sinne einer Kopiervorlage. Er wolle die von Karlsruhe gesetzten Grenzen unmittelbar in ein neues Gesetz gießen, was dann an sich auch geschehen ist. Es ist heute noch umstritten, ob das dann erarbeitete BKA-Gesetz verfassungsgemäß ist. Vor allem aber umstritten ist die Übernahme dieser Grenzen in die Landespolizeigesetze und die Strafprozessordnung.

Ich möchte das noch einmal hervorheben: im BKA-Gesetz ging es um die Abwehr des internationalen Terrorismus, das ist die Klammer um dieses Gesetz. Was die Staatstrojanerregelung in der StPO aber auch in den Landespolizeigesetzen betrifft, haben wir uns von Terrorismus längst weit entfernt. Besonders hervorheben möchte ich das PAG in Bayern. Das ist bereits beschlossen und es hat eine gewisse Relevanz für uns alle, denn unser Heimatminister ist ja Bayer. Der mag als politische *Lame Duck* und als nicht mehr ernst zu nehmen gelten. Aber er plant mit seinen Kollegen zusammen dieses PAG als Mustervorlage für ein Musterpolizeigesetz aufzunehmen. So hat er dies gesagt.

Glücklicherweise äußert sich Seehofer derzeit nicht zu diesem Feld. Er ist ja eigentlich ein sehr monothematischer Minister. Dies kann durchaus von Vorteil sein, denn zum Südkreuz oder zu anderen Fragen, die technisierte Überwachung angehen, sagt er wenig. Mal sehen, wie dies nach der Bayernwahl aussehen wird.

Die Justizministerkonferenz hat über dieses Muster-PAG schon gesprochen, das dann natürlich auch bedeuten würde, dass alle Bundesländer eine vergleichbare Version bekommen würden, die jeweils beide Varianten des Staatstrojaners enthielte. Seehofer hat seine diesbezügliche Drohung wahr gemacht.

Was aus meiner Sicht auch ein Teil des Zeitgeistes ist: Die Grenzen, die Karlsruhe setzt, werden tatsächlich wortwörtlich als Kopiervorlagen für Gesetze genutzt. Man geht also genau bis an die Grenze, was ich gerade im Überwachungsgesetzgebungsumfeld als ausgesprochen beunruhigend empfinde.

Die Strafprozessordnung hebe ich besonders hervor, weil sie in einem in vielerlei Hinsicht interessanten Prozess zustande gekommen ist. Selten habe ich für eine so weitreichende und seit Jahren umstrittene Regelung so eine Art der beschleunigten Gesetzgebung gesehen. Die Regelung für den Staatstrojaner kam hinten herum und in einer ganz anderen Regelung, nämlich dem „Gesetz zur effektiveren und praxistauglichen Ausgestaltung des Strafverfahrens". Es gab heftige Kritik, aber die beiden Regierungsparteien haben sich in der Sache dazu kaum geäußert. Von der Bundesbeauftragten für den Datenschutz, die ja sonst kein Wort sagt, sich aber wenigstens hier dezidiert geäußert hat, gab es einen harschen Brief. In der Anhörung gab es keinen einzigen Sachverständigen, der nicht massive Kritik übte. Dennoch wurde diese enorme Erweiterung des Einsatzes des Staatstrojaners ohne viel Federlesen durchgewunken.

Die Erweiterung betrifft Dutzende Arten von Verbrechen bis hinunter zu Urkundenfälschung oder Verstößen gegen das Betäubungsmittelgesetz. Vergehen also, die sich weit unterhalb jener Schwelle befinden, über die wir eigentlich immer geredet hatten: schwerste Verbrechen, die die Bundesrepublik in ihrem Bestand gefährden, die Terrorismusbezug haben oder zumindest das Leben oder die Gesundheit der Menschen ernsthaft gefährden.

Ich habe ehrlich gesagt noch nie einen parlamentarischen Prozess erlebt, in dem mit solcher Rigorosität solche weitreichenden Befugnisse durchgesetzt wurden. Ich habe noch nie wie in diesem Prozess erlebt, wie die Stellungnahmen und Sachverständigen, die sich der Bundestag herbeigezogen hatte, mit Ignoranz behandelt wurden.

Im Detail und um den Kern herauszuheben lässt sich sagen: Das eine ist die Quellen-TKÜ. Sie wird im Wesentlichen wie eine allgemeine Telekommunikationsüberwachung behandelt. Ich will kurz den Unterschied klarmachen. Eine normale TKÜ, in der Regel eine Telefonüberwachung, wird mit Hilfe des Anbieters durchgeführt, durch standardisierte Abhörschnittstellen, die in Deutschland und Europa verbreitet sind. Man nimmt also sozusagen die Kommunikation beim Anbieter ab. Das ist natürlich ein großer Unterschied zu der Situation, in der ich das Gerät, auf dem die Kommunikation stattfindet, hacke. Diese Gleichstellung ist in vielerlei Hinsicht kritisiert worden und auch technisch dämlich.

Risiken

Über die Jahre hat sich eine Risikodiskussion entfaltet. Da geht es um ganz verschiedene Bereiche und Fragen wie: sollte der Staat mit unseren Steuergeldern überhaupt für so eine Form von Sicherheitslücken bezahlen? Für kommerzielle Trojanerpartner? Oder generell für die Unterstützung einer ganzen Industrie, die darauf basiert, Sicherheitslücken möglichst lang geheim zu halten, um daraus ein Geschäft zu machen? Sollten wir das unterstützen? Ist das, in einer etwas weiteren Perspektive betrachtet, nicht eigentlich ein Nachteil für die Innere Sicherheit? Kann man in einer Zeit, in der viel über Milliardenschäden durch Trojaner, namentlich NotPetya und WannaCry, bekannt wird und man in Betracht zieht, welche Risiken man in Kauf nimmt, wenn man in diesen Markt investiert, diesen politischen Weg überhaupt noch weitergehen?

Wieso glauben Polizeien, seien es Landespolizeien oder BKA, dass sie besser seien als die NSA und die CIA, deren kompletter Trojanerschrank abhanden gekommen und ins Netz gewandert ist? Wieso glauben die eigentlich, sie könnten das besser? Wer kann eigentlich überprüfen, welche Versprechungen die kommerziellen Partner machen?

Vom Kernbereich der privaten Lebensgestaltung zur IT-Sicherheitsdiskussion

An diesen Risiken hängen eine Menge verschiedener Probleme, die sich aus meiner Sicht über die Jahre verändert haben. Die Diskussion hat sich mehr auf die Risiken fokussiert, was aus meiner Sicht ein Nachteil ist. Natürlich bin ich ein Hacker und sehe das alles stärker aus der Angreifer-Perspektive, aber die ursprüngliche Diskussion drehte sich um etwas anderes, nämlich um den Kernbereich der privaten Lebensgestaltung, unsere Intimsphäre. Ich möchte betonen, dass es einen Unterschied zwischen Privatsphäre und dem Konzept des Kernbereichs der privaten Lebensgestaltung, also dem innersten hochpersönlichen Kern einer Persönlichkeit, in die hier eingegriffen wird, gibt. Darum drehte sich die Diskussion eigentlich einmal. Da redete man über das ausgelagerte Gehirn und darüber, wie der Alltag und auch die Geschichte der Menschen in technische Artefakte eingehen und wer unter welchen Umständen darauf zugreifen darf.

Die IT-Sicherheitsdiskussion, die aus meiner Sicht sehr wichtig ist, hat das auf gewisse Art und Weise überlagert. Ebenso die Frage, wie weit eigentlich diese Geräte Extension unserer Körper sind und wie viel wir denen eigentlich anvertrauen. Was sagt eigentlich das Grundrecht, wenn es über eine Gewährleistung der Integrität und Vertraulichkeit redet, wenn wir immer nur darüber reden, auf welchem Wege sie hintenrum reinkommen? Und wie totalitär ist diese Ansicht, dass es keine Form der Kommunikation geben darf, die geschützt ist?

Letztere Ansicht stammt aus der Debatte um das „Going Dark", die ja noch parallel dazu lief und die ursprünglich im US-amerikanischen Raum debattiert wurde, sich aber auch bei uns sehr verbreitet hat.

Ich finde, das ist eine schwierige Diskussion, die man unbedingt hätte führen müssen, als die StPO im Gesetzgebungsprozess war, die aber einfach abgewürgt wurde. Das heißt nicht, dass es nicht auch einen gewissen juristischen und akademischen Streit gibt und eine Menge Papiere und Techniker, die darüber geschrieben haben. Aus meiner Sicht ist das aber im politischen Prozess in keiner Weise so reflektiert besprochen worden, wie es nötig gewesen wäre.

Ich möchte eine kleine Ausnahme machen, die auf das BKA-Gesetzurteil zurückgeht. Bei der Online-Durchsuchung, also jenem Trojaner, der alle Aspekte der Festplatte betrachten darf und auch ausleiten dürfte, hat man als Hürde den Verdacht auf eine besonders schwere Straftat und wesentlich die Schranken des großen Lauschangriffs gesetzt. Das bedeutet ganz praktisch, dass es zu diesen Online-Durchsuchungen in der StPO nur im äußersten Ausnahmefall kommen kann. Zur Erinnerung: der Streit um den großen Lauschangriff, war der um die Wanze im Schlafzimmer. Da ging es also auch um den Kernbereich der privaten Lebensgestaltung. Man hat hier sehr hohe juristische Grenzen gesetzt und die werden auch tatsächlich beachtet. Das kann man in Statistiken gut nachvollziehen, die dokumentieren, wie selten große Lauschangriffe durchgeführt oder Wanzen in Wohnungen angebracht werden. Man darf also zumindest im Rahmen der StPO die Hoffnung haben, dass die Online-Durchsuchung nicht sehr häufig sein wird, was sich aber letztendlich erst mit der Zeit zeigen wird.

Verfassungsbeschwerden

Mittlerweile weiß man von vier anhängigen Verfassungsbeschwerden. Es könnte natürlich noch weitere geben, aber die vier sind die, die relativ viel Aufmerksamkeit erreicht haben. Sie fokussieren sich sehr stark auf die Quellen-TKÜ, die Online-Durchsuchung und ein paar nebensächliche Themen. Ein Teil davon ist im Netz nachlesbar und auch für Nicht-Juristen durchaus interessant.

Wir werden vor allem warten müssen, wie lange das Gericht braucht, um die Verfassungsbeschwerden zu behandeln. Ich habe aber eigentlich keine Zweifel, dass sie zumindest diese Fragen wieder aufrollen, weil im Gesetz einige Dinge erlaubt wurden, die sich mit früheren Urteilen nicht vertragen und gegen die Juristen eine sehr gute Argumentation vorgebracht haben. Ich glaube, die technischen Argumente sind nicht unwichtig. Sie finden sich auch in allen vier Verfassungsbeschwerden. Erfahrungsgemäß werden wir aber noch eine Weile warten müssen bis wir Ergebnisse bekommen. Zumindest ein Zurückstutzen würde mich allerdings nicht überraschen.

Technisches Wettrüsten

Für den allgemeinen Zeitgeist heißt das aber nicht viel. Es gibt noch eine andere Form der Entwicklung, die ich von der juristischen trennen will. Ich habe sie mal „Technisches Wettrüsten" genannt, wegen der Entscheidungen, die parallel dazu in Bezug auf Behörden oder Institutionen fielen, welche gegründet wurden, um eine Form der technischen Unterstützung zu leisten.

Hier ist insbesondere ZITIS zu nennen. Das ist eine Behörde, die ziemlich nah an der Bundeswehr-Uni angesiedelt ist und sozusagen als technischer Dienstleister fungiert. Sie soll nicht nur im Bereich „Angriff auf Verschlüsselungssysteme" oder „offensive Angriffsmethoden", sondern auch in anderen Bereichen wie etwa Forensik liefern. Man hat da tatsächlich – die haben da gar keine Scham – einen BND-Mann an die Spitze gesetzt, als sei das normal. ZITIS ist bisher faktisch noch im Aufbau. Sie haben mit dem Strukturaufbau begonnen und bisher wenig Inhalte geliefert, aber da wird sicherlich viel kommen, das dann natürlich geheim sein wird. Es wird wenig gesagt, obwohl sich der Chef von ZITIS einigen Diskussionen gestellt hat.

Eine andere Sache ist die Agentur für disruptive Innovation in der Cybersicherheit (AdIC). Mittlerweile nutzen Innen- und Verteidigungsministerium das Wort „disruptiv" nicht mehr. Diese Agentur ist sozusagen noch einen Zacken dreister, da eine Kooperation zwischen dem Verteidigungs- und dem Innenministerium in Deutschland nicht der Normalfall ist. Da geht es in diese Richtung „Hack-Back", die auch politisch etwas debattiert wird: in wieweit darf man gegen wen und unter welchen Bedingungen zurück hacken? Inwieweit betrifft dies Völkerrecht? Dazu gibt es auch eine interessante Studie der wissenschaftlichen Dienste des Bundestages: welche Entitäten in Deutschland dürfen das? Armee? Geheimdienste? Polizei? Das ist noch etwas im Fluss. Gesetzgebung gibt es bisher noch nicht. Die Agentur steht aber natürlich in diesem Zusammenhang. Die Darstellung, die von der Leyen und Seehofer dazu machten, war natürlich eine andere. In jedem zweiten Satz dieser Pressekonferenz haben die DARPA erwähnt, um eine Anleihe an die amerikanische

Agentur zu machen. Aber ehrlich gesagt konnte bei dieser Pressekonferenz eigentlich gar nicht so viel zu dem Thema rausgeholt werden, weil das direkt nach Chemnitz war. Wenn man sich allerdings ansieht, wie sich die Bundeswehr in der letztens Zeit zu CNO (ComputerNetworkOperation) positioniert, wenn man die Frage von Hack-Back und wer das eigentlich machen kann überlegt und dass die Agentur von beiden, vom Innen- und vom Verteidigungsministerium gegründet wurde, dann ist das schon ein relativ klares Zeichen der strukturellen Positionierung.

Die Rolle der Geheimdienste

Nun zu einem anderen Bereich: Wir haben da auch noch ein Geheimdienstproblem. Natürlich haben wir verschiedene Geheimdienstprobleme, aber wir haben auch eines, das mit dem Staatstrojaner verbunden ist. Aus meiner Sicht war diesbezüglich die Diskussion in Hessen am deutlichsten: In Hessen gab es das erste Landespolizeigesetz und gleichzeitig auch ein Update des Landesamts für Verfassungsschutz, in dem geheimdienstliche Trojaner enthalten waren.

Auch in Hessen gab es einen interessanten Streit. Sie hatten hier mehr als 20, sehr verschiedene Sachverständige geladen, die auch alle Stellungnahmen abgegeben hatten. Auch im hessischen Gesetzentwurf war sehr viel mehr als nur der Trojaner enthalten, aber es war der erste, in dem sie einen Staatstrojaner für Geheimdienste wollten. In Hessen haben sie ein ziemlich kleines Landesamt für Verfassungsschutz – und plötzlich sollten die hacken dürfen. Die fanden das völlig normal.

Zu meiner Überraschung hat sich der hessische Landtag im Ergebnis dagegen entschieden. Zwar darf die hessische Polizei jetzt hacken, aber für das Landesamt für Verfassungsschutz haben sie es nicht zugelassen. Da waren wir doch überrascht. Wahrscheinlich ist man als Sachverständiger schon gewohnt, dass die eigenen Stellungnahmen geschreddert werden, so dass man gar nicht mehr erwartet, dass sie dem tatsächlich folgen. Aber es gab auch eine relativ breite Kritik, die auch in die Zeitungen getragen wurde und eine Demo im Februar.

Im hessischen Gesetzentwurf ist aber darüberhinaus eine interessante Sache drin, die ich so noch nicht gesehen hatte: sie wollten in Hessen auch noch die Computer Dritter hacken. Man hat also eine Fortsetzungsregel für den Staatstrojaner drinnen gehabt, dergestalt, dass wenn die überwachte Person auch informationstechnische Systeme Dritter verwendet, die Online-Durchsuchungen auch auf diesen Computern Dritter durchgeführt werden können. Das war neu. Es gab natürlich auch eine Menge Kritik juristischer Art, aber tatsächlich ist diese Regelung drinnen geblieben, zwar nicht für die Geheimdienste, aber für die hessische Polizei.

Die Diskussion war insgesamt in Hessen etwas anders, denn Landtag ist nicht Bundestag. Das kann ich für alle Anhörungen sagen, bei denen ich bei Landespolizeigesetzen dabei war. Die Landtagsdiskussionen sind aus meiner Sicht sehr viel sachlicher als im Bundestag. Man merkt, dass die Abgeordneten der Regierungs- und Oppositionsseite oft wirkliches technisches Erkenntnisinteresse haben. Das kann ich im Bundestag selten feststellen. Dennoch bleiben diese Regierungs-/Oppositionsgräben, die man auch in Hessen gesehen hat.

Ich will aber beim Geheimdienst etwas anderes nicht verschweigen. Unser Heimatministerium, genauer ein Staatssekretär, tingelt jetzt durch die Lande. Durchs Informationsfreiheitsgesetz habe ich mal eine seiner Reden frei bekommen und darin wird auch Hacken für den Verfassungsschutz gefordert. Nun muss ich sagen, dass diese Rede von Staatssekretär Wittwer noch vor der Maaßen-Anomalie stattgefunden hatte. Möglicherweise würde man heute nicht mehr ganz so offensiv an das Bundesamt für Verfassungsschutz gehen, aber die Argumentation läuft etwa so: Die dürfen das doch jetzt alle, warum sollen wir das nicht auch dürfen? Es ist ja jetzt sozusagen breit in der Strafprozessordnung und in mehrere Landespolizeigesetze übergegangen, warum soll da der Verfassungsschutz jetzt nicht auch hacken?

So entsteht natürlich ein großes Problem. Schon bei der Polizei teilt die Regierung in der Regel nichts mit und es gibt nur wenige Möglichkeiten der Kontrolle. Wenn der Geheimdienst hacken wird, werden wir genau gar nichts darüber erfahren. Weder ob es eine Eigenentwicklung ist, noch ob es ein kommerzieller Partner ist oder wie oft gehackt wurde. Wir werden gar nichts erfahren. Das sind alles Bereichsausnahmen, wo wir davon ausgehen können, dass es überhaupt keine Form von öffentlicher Kontrolle gibt. Daher müssen wir sehr, sehr wachsam sein, ob sie diese Idee tatsächlich umsetzen. Wie sich das weiter entwickelt, das werden wir dann vielleicht nach der Bayernwahl sehen, wenn wir einen ernsthaften Innenminister haben. Die Selbstverständlichkeit, mit welcher die Geheimdienste in die Trojaner integriert werden, finde ich sehr beunruhigend.

Gesamtüberwachungsrechnung

Ich will natürlich die Gesamtüberwachungsrechnung aufmachen und habe schon angesprochen, dass sich die Diskussion verändert hat. Trojaner werden mittlerweile selbstverständlich für ganz andere Geräte entwickelt, mit einem sehr starken Fokus auf Mobilgeräte. Während sich die Diskussion am Anfang zum Beispiel um Skype auf Desktop-Computern gedreht hat, geht es heute längst um Tablet und Mobiltelefone. Sie haben auch schon angekündigt, dass sie Staatstrojaner auch für mobile Geräte haben. Das hat sich sehr verändert. Aber ich glaube, die gesamte Gesamtüberwachungsrechnung müssen wir neu aufmachen und auch stärker fordern. Das wird wenig getan. Das ist mir auch in den Landespolizeigesetzen sehr aufgefallen, dass man, wenn jemand – vielleicht auch zurecht – überwacht wird, nicht mehr die Gesamtheit der Überwachungsmöglichkeiten und verschiedenen Datensätze betrachtet, sondern alles nur noch einzeln. Und dieser Zeitgeist, dass es keine Art von Kommunikation geben dürfe, in die man nicht hineinschauen kann, ist aus meiner Sicht stärker geworden. Wir müssen das noch stärker betonen, dass wir technisierte Überwachung in ihrer Gesamtheit betrachten müssen und nicht immer nur vereinzelt.

Dazu möchte ich einen zweiten Punkt nehmen, der vielen bewusst ist, die sich damit beschäftigen, dass diese Überwachungsausweitung-Hackingindustrie ein richtig signifikanter Industriezweig geworden ist. Insbesondere durch die enormen Gelder, die aus dem Geheimdienstbereich dort hineinfließen und wo sich Deutschland anschickt, selber zu investieren. Das ist eine große Änderung, weil dadurch natürlich auch dieser Markt professionalisiert wird und letztlich die Schwachstellen in Software,

mit denen wir jeden Tag zu kämpfen haben, auf eine Weise ausgebaut werden, wie wir das vor ein paar Jahren noch nicht gesehen haben. Seit der Zeit des ersten Urteils zum Staatstrojaner, wo es diesen Markt noch gar nicht gab, hat er sich zu einem großen Gebilde ausdifferenziert.

Ich kann nur empfehlen, die Studie zu lesen, die Privacy International einmal im Jahr herausgibt, um sich klarzumachen, wie groß dieser Markt ist.

Ein Punkt, zu dem ich nicht allzuviel sagen möchte: Transaktionen werden Kommunikation. Dinge, die wir automatisieren in all den Geräten, die eher Handlungen sind, die kommen in eine solche Auswertung mit rein. Und die betreffen natürlich auch den Staatstrojaner. Niemand von euch würde mir sein Mobiltelefon geben. Und ich kann das verstehen. Aber dazu brauche ich nicht so viel sagen.

Gefährdung von Menschenleben

Ich möchte noch einen letzten Punkt machen, den ich vor allem in den Landtagen immer mit in die Sachverständigen-Gutachten hineingeschrieben habe. Es geht um den Punkt, dass sie dort keine Grenzen setzen. Der Begriff des informationstechnischen Geräts ist sehr breit und sie nehmen keine Rücksicht darauf, ob es sich dabei vielleicht um ein Gerät handelt, das die Gesundheit oder das Leben von Menschen gefährden kann. Das ist nicht erst ein Problem, seit wir diese Hacks wie z. B. beim Jeep gesehen haben, sondern ich glaube das muss man noch holistischer betrachten, wenn man die Art der informationstechnischen Geräte, die gehackt werden dürfen, staatlicherseits beschränkt.

Ich möchte dazu eine kurze Geschichte aus dem Landtag in Niedersachsen, also in Hannover, erzählen, wo es auch um diesen Trojaner ging. Ich hatte dort den Punkt angesprochen, als es um das Gutachten, das der CCC abgegeben hatte, ging. Und da entstand eine interessante Diskussion mit Doris Schröder-Köpf, die für die SPD dort drin sitzt. Ich hatte also erläutert, dass ich es für eine gute Idee hielte, wenn der Gesetzgeber hier eine Beschränkung einbauen würde und sozusagen sowas wie Medizinalgeräte oder Fahrzeuge, in denen Menschen sitzen, ausnimmt. Da sagte Doris Schröder-Köpf zu mir: „Ja, Frau Kurz, aber wenn wir das machen, dann steht es ja so im Gesetz und dann wissen ja die Verbrecher, dass sie darüber kommunizieren können." Ich musste erst kurz parsen, was sie eigentlich sagt und sagte dann: „Ahhhh, ich muss ihnen da was sagen: Falls sie angenommen haben, das staatliche Hacken ist so wie in US-Vorabendserien; das ist nicht der Fall. Es gibt ganz viele Geräte und Betriebssysteme, die sie nicht hacken können. Wenn sie also eine Ausnahme für Medizinalgeräte oder vielleicht für Fahrzeuge reinschreiben, heißt das noch lange nicht, dass es die einzige Ausnahme wäre, die irgendwelche Verbrecher ausnutzen können." Der Einwurf sagte mir etwas über diese Denke, die dahinter steckt. Er machte klar, dass sie nach wie vor nicht wissen, wovon sie reden, wenn sie von Staatstrojanern reden, sondern so eine Vorstellung haben wie im Fernsehen. Jedes Gerät sei zack-zack-zack zu hacken. Sie können sich auch nicht vorstellen, dass es sehr viele Betriebssysteme oder Geräte gibt, wo man nicht schnell reinhacken kann. Sie wollen keinen Bereich, und sei er sogar verbunden mit dem Leben und der Gesundheit von Menschen, auch nur potenziell ausschließen. Ich musste mich erstmal wieder fangen, als mir klar wurde, was sie da eigentlich fragte. Und das ist nur ein Beispiel. Mir geht es hier nicht um diese Person; mir geht es um die Denke. Das fand ich sehr gruselig.

Wir müssen wieder die richtige Debatte führen

Aber weil ich nicht so negativ enden will, habe ich ein kleines Zitat aus dem allerersten Urteil, das zehn Jahre alt ist. Ich möchte an etwas erinnern. Nämlich daran, dass schon vor zehn Jahren jene Verfassungsrichter, die uns das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geschenkt haben, etwas anderes im Blick hatten:

Ich möchte endlich zu der Situation zurück, in der wir wieder über die beträchtliche Ausforschung reden und nicht nur über die Sicherheit und die Probleme, die sie damit haben. Ich möchte, dass wir auch darüber reden, was bereits in diesem Urteil in Bezug auf Beschlagnahmen steht, über die schon gar nicht mehr gesprochen wird. Und in Bezug auf die Mächtigkeit dieser Tools wünsche ich mir generell, dass wieder mehr die Perspektive der Potenz so einer staatlichen Hacking-Software in den Fokus rückt und auch die Tatsachen, die in den Urteilen stehen. Zum Beispiel jene Tatsachen, dass es nicht nur darum geht,

Constanze Kurz

Constanze Kurz ist promovierte Informatikerin, Autorin und Herausgeberin mehrerer Bücher, aktuell zum Cyberwar. Ihre Kolumne *Aus dem Maschinenraum* erscheint im Feuilleton der FAZ. Sie ist Aktivistin und ehrenamtlich Sprecherin des Chaos Computer Clubs. Sie forschte an der Humboldt-Universität zu Berlin am Lehrstuhl *Informatik in Bildung und Gesellschaft* und war Sachverständige der Enquête-Kommission *Internet und digitale Gesellschaft* des Bundestags und im Beirat des FIfF.

Dinge zu hacken, sondern dass durchaus auch dann der Kernbereich betroffen sein kann, wenn man einfach nur unsere Smartphones oder Festplatten beschlagnahmt. Ich wünsche mir, dass wir darüber wieder stärker reden, um eine Agenda zu haben, etwas, um dagegen zu halten und nicht immer nur zu reagieren, wenn sie schon wieder irgendeinen Gesetzentwurf in Landespolizeigesetzen oder im Bundestag haben.

Dies war ein wirklich ziemlich krampfhafter Versuch, aus der Entwicklung des Staatstrojanerproblems etwas Positives heraus zu extrahieren. Im Gesamtbild ist sicher klar geworden, dass wir beim Staatstrojaner einen relativ schlechten Stand haben. Aber falls jemand einen hat, nehmen wir den immer noch mit Freuden entgegen und werden die Binaries auch veröffentlichen. Ich bedanke mich für die Aufmerksamkeit.

Benjamin Kees, Rainer Rehak, Stefan Hügel

Jahresrückblick des FIfF

Eine freudige Panoramafahrt durch das FIfF-Jahr

In unserem Jahresrückblick stellten wir die wichtigsten Aktivitäten des FIfF seit der FIfF-Konferenz 2017 im Oktober 2017 in Jena dar. Mit Auszügen aus unseren Stellungnahmen, Pressemitteilungen und Beiträgen zur FIfF-Kommunikation illustrieren wir die Aktivitäten.

Oktober 2017

Startpunkt des FIfF-Jahres, über das hier berichtet werden soll, ist die **FIfF-Konferenz 2017**[1], die von Eberhard Zehendner und seinem Team organisiert wurde und am 20.-22. Oktober 2017 an der Universität Jena stattfand: *TRUST – wem kann ich trauen im Netz und warum?* In der Eröffnungsrede hieß es:

> *„TRUST – Vertrauen – ist die Basis, auf der unsere Gesellschaft aufgebaut ist. Wenn wir einander nicht mehr vertrauen können, funktioniert unser Zusammenleben nicht – das gilt selbstverständlich auch im Netz. […] Doch das Vertrauen wird heute im Netz täglich verletzt, sowohl illegal als auch legal. Wir müssen uns vor kriminellen Menschen schützen, die unser Vertrauen missbrauchen. Seit den Veröffentlichungen des Whistleblowers Edward Snowden wissen wir aber auch, dass Behörden unsere Kommunikation umfassend ausspähen. […] Dazu kommt der Datenhunger der Diensteanbieter, die ihre Geschäftsmodelle auf der Nutzung der Daten aufbauen und dies zum Beispiel durch für den Laien unverständliche Nutzungsbedingungen formaljuristisch legalisieren. Dem soll mit dem neuen europäischen Datenschutzrecht gegengesteuert werden – doch inzwischen wissen wir, dass gerade die deutsche Bundesregierung massiv versucht, dieses Recht aufzuweichen und zu bremsen. Auch damit wird Vertrauen zerstört."*

Im Rahmen der FIfFKon17 wurde der **FIfF-Studienpreis 2017** an Tobias Krafft verliehen: *Qualitätsmaße binärer Klassifikatoren im Bereich kriminalprognostischer Instrumente der vierten Generation*, so der Titel seiner Arbeit.

Bekanntlich fanden im September 2017 Wahlen zum Deutschen Bundestag statt. Die daran anschließenden Koalitionsverhandlungen zogen sich hin; lange sah es so aus, dass es zu einer christlich-ökologisch-liberalen Koalition kommen könnte (*Jamaika*-Koalition, so die etwas alberne Bezeichnung, die auf den Landesfarben Jamaikas basiert). Aus der Erwartung heraus, dass sich vor allem Bündnis90/Die Grünen und die FDP wieder stärker für Bürgerrechte einsetzen würden, wandten sich 23 Nichtregierungsorganisationen – unter ihnen das FIfF – mit einem **Offenen Brief zur Vorratsdatenspeicherung** an deren Vorsitzende. Wir forderten sie darin auf, sich für eine Abschaffung der Vorratsdatenspeicherung von Telekommunikationsdaten einzusetzen. Heute wissen wir, dass es nicht zu einer solchen Koalition kam. Doch auch die Hoffnung auf eine bürgerrechtsfreundliche Politik von Bündnis90/Die Grünen und der FDP hat seither so manchen Dämpfer erhalten.

Stefan Hügel, Rainer Rehak und Ben Kees beim Jahresrückblick

November 2017

Im Jahr 2016 hatten wir uns ausführlich mit dem Thema Transhumanismus beschäftigt – unter anderem mit zwei Schwerpunktausgaben der FIfF-Kommunikation. Der Beziehung des Transhumanismus zum Miltär widmeten wir uns in einem **Dossier für die Zeitschrift Wissenschaft & Frieden 4/2017**: *Transhumanismus und Militär*[2], das von Hans-Jörg Kreowski herausgegeben wurde.

Unsere Kontakte zur Tübinger Informationsstelle Militarisierung (IMI) konnte ebenfalls Hans-Jörg Kreowski durch einen eingeladenen **Vortrag beim IMI-Kongress**[3] *Der Informationsraum aus militärischer Sicht* vertiefen. Dem folgte eine Veröffentlichung in der IMI-Studie 2018/04 *Krieg im Informationsraum*[4].

Dezember 2017

Beim Friedensratschlag in Kassel waren wir 2017 leider nicht vertreten. Doch in der **Konferenzdokumentation zum Friedens-**

ratschlag 2016[5] erschien im Dezember der Beitrag zu unserem damaligen Workshop[6].

Schlechte Nachrichten aus München: Die Umstellung der Stadtverwaltung auf offene Software (LiMuX) soll rückgängig gemacht werden[7]. Dagegen hatte sich das **Aktionsbündnis *München bleibt frei*** gebildet – das FIfF gehörte zu den Unterstützern. in der Erklärung des Bündnisses[8] hieß es:

> *„Da Freie Software die Autonomie der Nutzer stärkt, freie Standards unterstützt und damit die digitale Teilhabe und Nachhaltigkeit fördert und gleichzeitig eine notwendige Voraussetzung für Sicherheit und Datenschutz ist, wäre es gerade jetzt, wo national wie international die Weichen für Freie Software gestellt sind, widersinnig, einen Weg zu unfreier Software einzuschlagen."*

Auch beim **Chaos Communication Congress 2017** (34c3), erstmals in den Messehallen Leipzig, waren wir mit unserer Assembly dabei. Dazu gab es einen Talk von Rainer Rehak *Die göttliche Informatik*[9]. „Die Informatik löst formale (mathematisch modellierte) Probleme ganz vorzüglich – doch nun soll sie alle anderen Probleme auch noch lösen", hieß es in der Ankündigung.

Januar 2018

Bei der **Sitzung des Vorstands** der Herausgeber der Zeitschrift **Wissenschaft & Frieden** übergab Dietrich Meyer-Ebrecht die Vertretung des FIfF an Hans-Jörg Kreowski, der auch am Vorabend das FIfF bei der **Podiumsdiskussion** *Angriff und Verteidigung in der ‚Ära des Cyberkriegs' – Theorie und Praxis der digitalen Strategie der Bundeswehr* vertrat.

Die Regionalgruppe München organisierte im Lauf des Jahres mehrere **Cryptoparties**, bei denen Grundlagen der Verschlüsselung und der sicheren Kommunikation vermittelt wurden.

Februar 2018

Bei der **Anhörung im Hessischen Landtag** zum Gesetzentwurf von Bündnis90/Die Grünen und der CDU für die **Neuausrichtung des Verfassungsschutzes in Hessen** nahmen wir zur darin geplanten Quellen-Telekommunikationsüberwachung und Online-Durchsuchung Stellung. In unserer Pressemitteilung[10] hieß es dazu:

> *„Geheimdienste, also staatliche Behörden, die wesentlich auf verdeckte Maßnahmen, Tarnoperationen, ‚Vertrauensleute' oder verdeckte MitarbeiterInnen setzen, sind inhärent auf Intransparenz angelegt und angewiesen, da Heimlichkeit das primäre Mittel ist, die ihnen übertragenen Aufgaben auszufüllen. Ermächtigungen derartiger Dienste müssen folglich besonders kritisch analysiert werden, da einmal freigegebene Maßnahmen und ermöglichte Methoden meist nur nach Skandalen erneut zur breiten Diskussion gestellt werden (können).*
>
> *Auch wenn sich die Aufgabenbereiche von Polizeien und Geheimdiensten mittlerweile gefährlich überlappen, sind dennoch die Berichts- und Transparenzpflichten von polizeilichen Behörden – im Gegensatz zu verdeckt tätigen Organisationen – zumindest grundsätzlich auf Offenheit angelegt. Wegen dieses gewichtigen Unterschieds gehen die rechtfertigenden Referenzen des Gesetzentwurfs bezüglich der Entscheidung des Bundesverfassungsgerichts zum BKA-Gesetz natürlich prinzipiell fehl. Ein Geheimdienst ist keine Polizei und eine Polizei ist kein Geheimdienst."*

März 2018

Im **Kinderkanal** erschien in der Reihe Timster *Zeig mir Dein Gesicht!*[11] ein **Erklärfilm zur Gesichtserkennung** und dem Bahnhof Berlin Südkreuz, mit Benjamin Kees als Experten.

April 2018

In Bremen sollte das Polizeigesetz verschärft werden, wobei u. a. der Ausbau der Videoüberwachung, elektronische Fußfesseln und Staatstrojaner vorgesehen waren. Das FIfF beteiligte sich am **Bündnis Brementrojaner**, das sich dagegen bildete. In der Pressemitteilung des Bündnisses hieß es:

> *„In Bremen treibt die rot-grüne Landesregierung im Eiltempo und ohne gesellschaftliche Debatte eine folgenschwere Änderung des Bremischen Polizeigesetzes voran. Der Senator für Inneres hat einen entsprechenden Gesetzentwurf […] vorgelegt. Er sieht gravierende rechtsstaatliche, grund- und datenschutzrechtliche Eingriffe vor. […] Auch nach möglichen Änderungen durch die rot-grüne Koalition wird unsere grundsätzliche Kritik an der Verschärfung des Bremischen Polizeigesetzes bestehen bleiben."*

Auch an der **Berliner Allianz für Freiheitsrechte** ist das FIfF als Erstunterzeichner beteiligt. Die Allianz wendet sich gegen Videoüberwachung, wie sie am Bahnhof Berlin Südkreuz eingeführt werden soll und dabei insbesondere gegen ein Volksbegehren, das den Ausbau der Videoüberwachung forderte.

Am 26. April 2018 stellten Hans-Jörg Kreowski, Benjamin Kees und Rainer Rehak das FIfF im **Chaosradio** vor. Sie sprachen über die Gesichtserkennungsversuche am Südkreuz, den Hessentrojaner, die FIfFKon18 und die Cyperpeace-Kampagne. Die zweistündige Sendung ist als Podcast[12] verfügbar.

Mai 2018

Im Mai war das FIfF auf mehreren Veranstaltungen vertreten: bei der **re:publica 18**[13] in Berlin – mit Informationen und der Beteiligung an den Diskussionen über einen höchst befremdlichen und äußerst unsensiblen Auftritt der Bundeswehr[14], an der **Konferenz der Informatikfachschaften**[15] in Bremen – mit FIfF-Vorstellung und Workshop – und am **Corso Leopold**[16] in München mit einem Informationsstand.

Als Mitglied des Bündnisses **#noPAG – Nein zum neuen Bayerischen Polizeiaufgabengesetz**[17] waren wir an der Großdemonstration in München beteiligt:

„Die CSU und die Staatsregierung rüsten die Bayerische Polizei auf. Nicht nur mit Waffen und Granaten, wie in der Vergangenheit, sondern vor allem mit Gesetzen. Im August 2017 wurden durch das sogenannte Gefährdergesetz die Befugnisse der Polizei bereits extrem ausgeweitet. Mit der Neuordnung des Polizeiaufgabengesetzes will die CSU jetzt noch viel weiter gehen. […]

Das Bündnis ‚noPAG – NEIN! zum Polizeiaufgabengesetz Bayern' fordert den Bayerischen Landtag auf, die geplanten Änderungen am Polizeiaufgabengesetz nicht zu beschließen und die im August 2017 beschlossene Einführung der „drohenden Gefahr" und der theoretisch möglichen unendlichen Haft zurückzunehmen."

Bei der Vorstellung des **Grundrechte-Reports**[18] 2018 und der anschließenden Redaktionssitzung war das FIfF als neuer Mitherausgeber beteiligt. Bereits im Grundrechte-Report 2018 gab es einen Beitrag von Stefan Hügel zum Ransomware-Trojaner **WannaCry**: *Öffentliche Sicherheit durch unsichere IT?*

Als Beilage zur Zeitschrift **Wissenschaft und Frieden** 2/2018 erschien das vom FIfF mitherausgegebene **Dossier Nr. 86**: *Wachsendes Ungleichgewicht – Cyberrüstung und zivile IT-Sicherheit*[19]:

„Cyber-Angriffe auf Behörden, Wirtschaft und Zivilgesellschaft sind mittlerweile auch in Deutschland an der Tagesordnung. […] Die Daten zeigen […] dass die Angreiferseite sehr viel stärker ausgerüstet wird als die IT-Sicherheitsverantwortlichen. Abzulesen ist eine massive Rüstungsspirale, die eine erhebliche Bedrohung der zivilen IT-Nutzung darstellt."

August 2018

TDRM – Tihange Doel Radiation Monitoring wird weiter ausgebaut: Durch den Launch einer neuen **Website** und der **Kooperation mit der Abteilung für Katastrophenschutz der Städteregion Aachen** mit einer Diskussion über das weitere Vorgehen für die Nutzung der Messergebnisse aus der Umgebung der belgischen AKWs für frühzeitige Alerts.

Neu in den **FIfF-Beirat** haben wir Prof. Dr. **Wolfgang Hofkirchner** und Prof. Dr. **Jochen Koubek** berufen.

September 2018

Das Thema der diesjährigen **FIfF-Konferenz** – FIfFKon18[20] – in Berlin lautete *Brave New World – Gestaltungsfreiheiten und Machtmuster soziotechnischer Systeme*. In der Einladung hieß es:

„Bei der stetigen Digitalisierung und Vernetzung der Gesellschaft müssen die Freiheit des Individuums und das Wohl der Gesellschaft im Vordergrund stehen, Kommunikationsmittel sollten integre und vertrauliche Systeme sein, die die Menschen und ihre Grundrechte respektieren, ohne von Geheimdiensten und Militär durchdrungen zu werden.

Die Informatik ist immer auch Gestaltungsdisziplin – weit über die reine Technik hinaus. Daher will die diesjährige Konferenz Sichtweisen und konkrete Wege erarbeiten, auf welche Weise in technischen Systemen und politischen Entscheidungen Aspekte wie demokratische Teilhabe, Freiheit, Selbstbestimmung, Pluralismus von Lebensentwürfen und Nachvollziehbarkeit Eingang finden können."

Erstmals verliehen wir die neu geschaffene **Weizenbaum-Medaille** an Wolfgang Coy[21]:

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung verleiht die Weizenbaum-Medaille 2018 für seine außerordentlichen Verdienste um das Lehr- und Forschungsgebiet Informatik und Gesellschaft an Wolfgang Coy. Als Professor für Informatik in Bildung und Gesellschaft an der Humboldt-Universität zu Berlin hat er das Fach Informatik und Gesellschaft in Forschung und Lehre einzigartig, beispielhaft und maßgeblich ausgestaltet unter Einbeziehung medientheoretischer, sozial- und kulturgeschichtlicher, fachdidaktischer und ethischer Gesichtspunkte.

Den bisherigen FIfF-Studienpreis verliehen wir erstmals als **Weizenbaum-Studienpreis**[22], ihn erhielten in diesem Jahr:

- Leon Kaiser für seine Arbeit *Vulnerable Systems: The Quantification of Affect in an Experimental Blockchain Pilot-Project for Financial Transaction Management for Refugees*,
- Severin Engelmann für seine Arbeit *The Digital Dimensions of Personal Identity*,
- Nico Lück für seine Arbeit *Künstliche Intelligenz und Rüstungskontrolle. Der Einsatz maschinellen Lernens in Waffensystemen und Verifikationsmaßnahmen* und
- Jörg Pohle für seine Arbeit *Datenschutz und Technikgestaltung.*

Oktober 2018

Das FIfF unterstützte die Großdemonstration **#unteilbar – Solidarität statt Ausgrenzung**[23] in Berlin, an der rund 2.500.000 Menschen teilnahmen. Im Aufruf hieß es unter Anderem:

„Es findet eine dramatische politische Verschiebung statt: Rassismus und Menschenverachtung werden gesellschaftsfähig. Was gestern noch undenkbar war und als unsagbar galt, ist kurz darauf Realität. Humanität und Menschenrechte, Religionsfreiheit und Rechtsstaat werden offen angegriffen. Es ist ein Angriff, der uns allen gilt.

Wir lassen nicht zu, dass Sozialstaat, Flucht und Migration gegeneinander ausgespielt werden. Wir halten dagegen, wenn Grund- und Freiheitsrechte weiter eingeschränkt werden sollen. […]

Während der Staat sogenannte Sicherheitsgesetze verschärft, die Überwachung ausbaut und so Stärke markiert, ist das Sozialsystem von Schwäche gekennzeichnet: Millionen leiden darunter, dass viel zu wenig investiert wird, etwa in Pflege, Gesundheit, Kinderbetreuung und Bildung."

Das FIfF war an einem **Offenen Brief**[24] an ausgewählte Mitglieder der Bundesregierung beteiligt mit der Aufforderung, die **ePrivacy-Verordnung** nicht weiter zu torpedieren und auf EU-Ebene endlich für einen wirksamen Schutz unserer Online-Aktivitäten einzutreten. 16 Organisationen fordern darin:

1. Stärken Sie den Rechtsrahmen für elektronische Kommunikation.
2. Schützen Sie Privatsphäre und Wettbewerb.
3. Sichern Sie die Privatsphäre durch Technikgestaltung und Voreinstellung.
4. Schützen Sie vor Tracking Walls.
5. Verhindern Sie Massenüberwachung und Vorratsdatenspeicherung.

Anmerkungen

1 *https://2017.fiffkon.de*
2 *https://wissenschaft-und-frieden.de/index.php?pid=12&dvar=85#n85*
3 *http://www.imi-online.de/2017/11/29/krieg-im-informationsraum-3/*
4 *http://www.imi-online.de/2018/03/23/broschuere-krieg-im-informationsraum/*
5 *Henken L Hg. (2017) Spannungen, Aufrüstung, Krieg – und kein Ende? Konfliktanalysen und Lösungsansätze aus der Friedensbewegung. Kassel: Verlag Winfried Jenior*
6 *Hügel S, Meyer-Ebrecht D (2017) Cyberwar – Cyberpeace: Wir brauchen einen Gegenentwurf. in: Henken L Hg. (2017) a.a.O., S. 92-106*
7 *Krempl S (2017) Endgültiges Aus für LiMux: Münchener Stadtrat setzt den Pinguin vor die Tür, heise.de, https://www.heise.de/newsticker/meldung/Endgueltiges-Aus-fuer-LiMux-Muenchener-Stadtrat-setzt-den-Pinguin-vor-die-Tuer-3900439.html*
8 *https://muenchen-bleibt-frei.de*
9 *Rehak R (2017) Die göttliche Informatik. Talk auf dem 34c3, https://media.ccc.de/v/34c3-8998-die_gottliche_informatik_the_divine_computer_science*
10 *https://www.fiff.de/presse/pressemitteilungen/fiff-stellungnahme-zum-trojanereinsatz-durch-den-hessischen-verfassungsschutz-fiff-lehnt-hessentrojaner-ab*
11 *https://www.kika.de/timster/sendungen/sendung105710.html*
12 *https://chaosradio.de/cr245-fiff*
13 *https://18.re-publica.com/*
14 *Ein Bericht der Veranstalter über den Auftritt und das kommunikative Nachspiel gibt es unter https://18.re-publica.com/de/page/bundeswehr-bei-rp18-chronologie-paar-fragen.*
15 *https://wiki.kif.rocks/wiki/KIF460:Hauptseite*
16 *https://corso-leopold.de*
17 *https://no-pag.de*
18 *http://grundrechte-report.de*
19 *https://wissenschaft-und-frieden.de/index.php?pid=12&dvar=86#n86*
20 *https://2018.fiffkon.de*
21 *https://www.fiff.de/studienpreis/Laudatio-Coy-2018*
22 *https://www.fiff.de/studienpreis*
23 *https://www.unteilbar.org*
24 *https://www.fiff.de/presse/pressemitteilungen/offenerbriefeprivacy2018*

FIfF-Konferenz 2019

Künstliche Intelligenz als Wunderland

22.–24. November 2019 in Bremen

In der berühmten Erzählung *Alice im Wunderland* von Lewis Carroll begegnet die Protagonistin im Wunderland den merkwürdigsten Gestalten und erlebt kuriose Abenteuer. Ein neues Wunderland eröffnet sich heute durch Künstliche Intelligenz. Es ist von Robotern bevölkert, die Fußball spielen, tanzen, jonglieren, kochen, Dienstleistungen aller Art erbringen, Alte und Kranke pflegen und Orte erkunden, die für Menschen gefährlich oder unerreichbar sind. Es gibt dort selbstfahrende Autos und unbemannte Flugobjekte. Lernende neuronale Netze beeindrucken, weil sie fast alle Spiele gegen fast alle Spielerinnen und Spieler gewinnen. Man trifft allenthalben auf Systeme, die sehen, lesen, sprechen und lernen können. Und es wird gemunkelt, dass sich demnächst eine neue Spezies mit Superintelligenz dazu gesellen wird, die besser denken kann als alle Menschen zusammen.

Wir möchten alle Interessierten zur FIfF-Konferenz 2019 vom 22. bis 24. November 2019 nach Bremen einladen, um mit uns dieses Wunderland zu erkunden und genauer unter die Lupe zu nehmen. Was ist dran an den hochfliegenden Plänen und Versprechungen? Welche Erwartungen und Hoffnungen sind realistisch, welche sind übertrieben, welche sind unerfüllbar? Welche gesellschaftlichen Auswirkungen sind zu erwarten und wie soll man mit ihnen umgehen? Welche Risiken und Gefahren sind mit den aktuellen und zukünftigen Entwicklungen der Künstlichen Intelligenz verbunden und wie ist ihnen zu begegnen?

Veranstaltungsort: Universität Bremen, MZH, Bibliothekstraße 5, 28359 Bremen

Kontakt: Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V., Goetheplatz 4, 28203 Bremen; Pressekontakt *presse@fiffkon.de*, Twitter *@fiffkon*

NETZPOLITIK.ORG

Anna Biselli, netzpolitik.org

Urheberrechtsreform: Was in den letzten drei Jahren geschah

Wann haben die Diskussionen über die EU-Urheberrechtsreform begonnen? Seit wann ist bekannt, dass der Entwurf uns Upload-Filter und ein neues Leistungsschutzrecht bringen könnte? Und ist jetzt noch irgendetwas zu retten? Ein Überblick.

Jeden Tag gibt es neue Meldungen über die EU-Urheberrechtsreform, am meisten Aufmerksamkeit bekommen dabei die befürchteten Upload-Filter und die enthaltene Neuauflage des Leistungsschutzrechts. Auch wenn das leicht in Vergessenheit gerät: Eigentlich wird schon seit fast drei Jahren über die geplanten Änderungen diskutiert. Da kann man schon mal den Überblick verlieren, vor allem beim EU-Gesetzgebungsprozess[1].

Wir haben die Ereignisse der letzten drei Jahre sortiert und geben einen Ausblick, was jetzt noch bevorsteht.

16. Juni 2015: Der Rechtsausschuss des EU-Parlaments beschließt einen Bericht zum Urheberrecht von Julia Reda[2]. Damit fordert das Parlament die EU-Kommission auf, die bestehenden Urheberrechtsregeln zu prüfen und zu reformieren.

14. September 2016: Die EU-Kommission legt den ersten Entwurf[3] für eine Richtlinie „über das Urheberrecht im digitalen Binnenmarkt" vor. Der damalige Digital-Kommissar Günther Oettinger präsentiert[4] zusammen mit Vize-Kommissionschef Andrus Ansip die Pläne, die Kritik[5] an der ersten Version der Urheberrechtsreform ist massiv.

Der Kommissionsentwurf geht ins Parlament

20. Februar 2017: In einem Berichtsentwurf lehnt die für den Verbraucherausschuss des EU-Parlaments zuständige Berichterstatterin Catherine Stihler den Vorschlag der Kommission ab[6].

10. März 2017: Der für die Urheberrechtsreform federführende Rechtsausschuss des EU-Parlaments veröffentlicht den Berichtsentwurf[7] der EU-Parlamentarierin Therese Comodini Cachia. Sie ist zu diesem Zeitpunkt die Berichterstatterin und somit verantwortliche Abgeordnete für das Gesetz.

22. März 2017: Der Rechtsausschuss[8] diskutiert über den Entwurf. Die Verhandlungsführerin Comodini Cachia spricht sich gegen den Entwurf von Oettinger[9] aus.

11. Mai 2017: Der Parlamentsausschuss für den Binnenmarkt und Verbraucherschutz (IMCO) diskutiert über seine Position[10] zum Kommissionsentwurf.

8. Juni 2017: IMCO stimmt über die Stellungnahme des Ausschusses ab, auf eine gemeinsame Position einigen konnten sich die Ausschussmitglieder nicht[11]. Zwar lehnt ein Großteil der Parlamentarier Upload-Filter ab, eine Mehrheit für eine Ablehnung des Leistungsschutzrechts bildet sich jedoch nicht.

Ab jetzt ist Axel Voss zuständig

15. Juni 2017: Der CDU-Politiker Axel Voss löst die maltesische Parlamentarierin Comodini Cachia als Berichterstatter für die Urheberrechtsreform ab, da sie das EU-Parlament verlässt[12].

11. Juli 2017: Sowohl der Industrie- als auch der Kulturausschuss stimmen über ihre Stellungnahmen[13] zur Urheberrechtsreform ab. Der Industrieausschuss macht einen halbgaren Vorschlag, um Upload-Filter zu entschärfen, der Kulturausschuss würde mit seiner Stellungnahme die Situation noch verschlimmern und sogar Uploads zu Cloud-Diensten filtern.

20. November 2017: Der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) beschließt seine Position[14] und spricht sich gegen Upload-Filter aus. Plattformen sollen bei ihnen eingestellte Inhalte nicht generell überwachen müssen. Zum Leistungsschutz äußert sich der Ausschuss nicht.

25. Mai 2018: Der Rat der EU beschließt seine Position[15], Upload-Filter und Leistungsschutzrecht inklusive, und erteilt mehrheitlich das Verhandlungsmandat. Deutschland stimmt dagegen.

Der Entwurf wackelt im EU-Parlament

20. Juni 2018: Der federführende Rechtsausschuss im EU-Parlament beschließt seine Änderungsanträge[16] – pro Upload-Filter und Leistungsschutzrecht. Nun geht es ins Plenum des Parlaments, das üblicherweise den Vorschlag des federführenden Ausschusses absegnet. Eine reine Formsache.

5. Juli 2018: Paukenschlag: Das EU-Parlament winkt den Textvorschlag des Rechtsausschusses nicht durch[17].

12. September 2018: Das Parlament stimmt erneut ab. Die Mehrheit der Abgeordneten winkt den Vorschlag in dieser zweiten Abstimmung durch[18]. Damit ist der Weg für den Trilog[19] geebnet, in dem EU-Parlament, Kommission und Rat einen Kompromiss zwischen ihren jeweiligen Positionen verhandeln.

Verhandlungen hinter verschlossenen Türen

Oktober 2018 bis Februar 2019: Im Trilog ringen Parlament, Kommission und Rat hinter geschlossenen Türen um den endgültigen Gesetzestext.

18. Januar 2019: Die Verhandlungen geraten ins Stocken[20], da elf Länder im Rat den erarbeiteten Kompromissvorschlag blockieren – darunter auch Deutschland. Die größten Streitpunkte sind weiterhin Artikel 11 und 13, die ein neues Leistungsschutzrecht festsetzen und Betreiber von größeren Internetplattformen dazu zwingen würden, Inhalte vor der Veröffentlichung nach Urheberrechtsverletzungen zu filtern.

13. Februar 2019: Die Trilog-Verhandler geben bekannt, dass sie sich auf einen gemeinsamen Text zur Urheberrechtsreform geeinigt haben[21]. Der finale Text enthält, aller öffentlichen Kritik zum Trotz, Upload-Filter und ein neuerliches Leistungsschutzrecht.

19. Februar 2019: Der Rechtsausschuss des Parlaments diskutiert[22] über das Ergebnis des Trilogs. Berichterstatter Axel Voss dementiert, dass der Text überhaupt Upload-Filter enthalte und zieht damit Spott und Kritik[23] auf sich.

20. Februar 2019: Im Rat der EU wird der Kompromiss aus den Trilog-Verhandlungen abgesegnet. Deutschland stimmt dem finalen Text zu[24]. Das steht im Widerspruch zum Koalitionsvertrag zwischen SPD und Union, in dem Upload-Filter als unverhältnismäßig bezeichnet[25] werden.

Alles zu spät?

26. Februar 2019: Der Rechtsausschuss des EU-Parlaments stimmt dem Verhandlungsergebnis zu[26]. 16 von 25 Ausschussmitgliedern befürworten die Richtlinie.

Irgendwann zwischen Ende März und Anfang April stimmt das EU-Parlament final über das Gesetz ab. Am Text der Einigung zwischen Rat, Kommission und Parlament lässt sich nicht mehr rütteln. Das EU-Parlament könnte die Reform als Ganzes ablehnen, das ist in der Vergangenheit jedoch nur selten vorgekommen. Doch der öffentliche Druck ist groß[27], an vielen Orten in ganz Europa organisieren breite Bündnisse Demonstrationen gegen die Richtlinie.

Anmerkungen

1 *http://www.europarl.europa.eu/germany/de/europa-und-europawahlen/ordentliches-gesetzgebungsverfahren*
2 *https://juliareda.eu/2015/06/reda-bericht-angenommen-ein-wendepunkt-in-der-urheberrechtsdebatte/*
3 *https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52016PC0593&from=DE*
4 *https://netzpolitik.org/2016/reaktionen-auf-reformvorschlaege-der-eu-kommission-es-haette-nicht-schlimmer-kommen-koennen/*
5 *https://netzpolitik.org/2016/geleakter-entwurf-der-eu-urheberrechtsrichtlinie-viele-versaeumnisse-dafuer-20-jahre-leistungsschutzrecht/*
6 *https://www.golem.de/news/google-steuer-eu-verbraucherausschuss-lehnt-leistungsschutzrecht-ab-1702-126378.html*
7 *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-601.094+01+DOC+PDF+V0//EN&language=EN*
8 *http://www.europarl.europa.eu/news/en/press-room/20170316IPR67318/committee-on-legal-affairs-meeting-22-03-2017-am*
9 *https://www.heise.de/newsticker/meldung/Copyright-Reform-Verhandlungsfuehrerin-im-EU-Parlament-spricht-sich-gegen-Leistungsschutzrecht-aus-3647186.html*
10 *http://www.europarl.europa.eu/news/en/news-room/20170504IPR73427/committee-on-the-internal-market-and-consumer-protection-11052017-(am)*
11 *https://netzpolitik.org/2017/eu-urheberrechts-richtlinie-erste-abstimmung-gegen-uploadfilter-aber-fuer-leistungsschutzrecht/*
12 *https://www.eppgroup.eu/newsroom/news/axel-voss-appointed-new-rapporteur-for-copyright-directive*
13 *https://netzpolitik.org/2017/filtern-sperren-halbgare-kompromisse-erste-eu-ausschuesse-haben-ueber-urheberrecht-abgestimmt/*
14 *https://netzpolitik.org/2017/urheberrechts-richtlinie-wenig-libe-fuer-uploadfilter-im-eu-parlament/*
15 *https://netzpolitik.org/2018/eu-staaten-sprechen-sich-fuer-upload-filter-und-leistungsschutzrecht-aus/*
16 *https://netzpolitik.org/2018/jetzt-uploadfilter-in-der-eu-urheber rechtsreform-verhindern-sag-dem-eu-parlament-deine-meinung/*
17 *https://netzpolitik.org/2018/chance-fuer-aenderung-eu-parlament-verhindert-durchwinken-von-uploadfiltern-und-leistungsschutzrecht/*
18 *https://netzpolitik.org/2018/das-eu-parlament-legt-einen-schleier-ueber-das-internet-votum-fuer-upload-filter-und-leistungsschutzrecht/*
19 *https://de.wikipedia.org/wiki/Trilog*
20 *https://netzpolitik.org/2019/eu-urheberrechtsreform-elf-laender-auf-letztem-meter-gegen-uploadfilter/*
21 *https://netzpolitik.org/2019/eu-urheberrecht-verhandler-meisselten-uploadfilter-in-stein/*
22 *http://www.europarl.europa.eu/ep-live/en/committees/video?event=20190219-0900-COMMITTEE-JURI*
23 *https://www.golem.de/news/eu-urheberrechtsreform-das-absolute-unverstaendnis-des-axel-voss-1902-139511.html*
24 *https://www.golem.de/news/uploadfilter-regierung-bricht-koalitionsvertrag-in-eu-abstimmung-1902-139520.html*
25 *https://netzpolitik.org/2018/urheberrecht-im-koalitionsvertrag-zwischen-modernen-nutzungsformen-und-einem-eu-leistungsschutzrecht/*
26 *https://twitter.com/Senficon/status/1100403956449083397*
27 *https://netzpolitik.org/2019/immer-mehr-demonstrationen-gegen-uploadfilter-schon-vor-dem-grossen-aktionstag/*
28 *https://pgp.mit.edu/pks/lookup?op=get&search=0x18735033A249AE26*

Anna Biselli

Auf einem Zettel steht, dass sie eigentlich Informatikerin ist. **Anna Biselli** war ab 2013 bei netzpolitik.org und ist nach einer Pause wieder als freie Autorin dabei. Sie interessiert sich vor allem für staatliche Überwachung und Dinge rund ums BAMF. Du erreichst sie unter anna@netzpolitik.org – am besten verschlüsselt[28] [325C 6992 DCD3 1167 D9FA 9A57 1873 5033 A249 AE26]

Hans-Jörg Kreowski

Bericht über das zweite Cyberpeace-Forum

Nach dem ersten Cyperpeace-Forum im November 2016 hat nun – endlich – am 15. und 16. März 2019 das zweite Cyberpeace-Forum in Bremen stattgefunden. Mit einer kleinen Nachlese möchte ich über die Veranstaltung berichten. Ich hoffe, damit zur Nachahmung anzuregen. Mögen sich FIfF-Mitglieder andernorts finden, die Ähnliches organisieren. Es ist der Mühe wert.

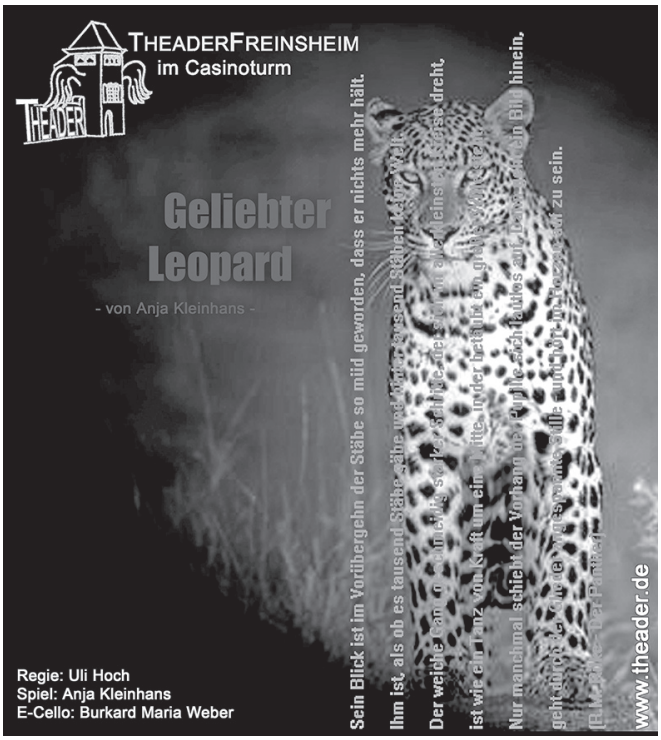
Am Freitagabend bildete ein Gastspiel des *TheaderFreinsheim* im Gemeindezentrum Zion in der Bremer Neustadt den Auftakt. Es wurde das Stück *Geliebter Leopard – Ein Stück Aufrüstung für den Frieden* von Anja Kleinhans aufgeführt. Es handelt sich um ein Einpersonenstück – von der Autorin unter der Regie von Uli Hoch selbst gespielt und begleitet von Burkhard Maria Weber am E-Cello. Zu dem Stück heißt es auf der Webseite des Theaters *(http://www.theader.de/04Repertoire34.html)*:

> *„Iris ist die Urenkelin einer Rüstungsfirmendynastie und Kuratorin der firmeneigenen Stiftung zur Hilfe traumatisierter Kinder. Sie führt intensive Briefgespräche mit Navid, einem jungen Mann aus Afghanistan, der als Kind, nachdem seine Familie von den Taliban ermordet worden war, nach Deutschland gebracht wurde, wo er durch die Stiftung eine Pflegefamilie und einen neuen Lebensstart ermöglicht bekam. Beide verbindet eine intensive Liebe zu dem Leoparden, wobei stets fraglich bleibt, ob diese gefährliche Kraftkreatur als grausamste Zerstörung oder eigentlicher Heilsbringer erscheint. Ist Krieg notwendig? Hat die bedeutungsvolle Rolle der Rüstungsindustrie im Weltgeschehen ihre tiefmenschliche, sinnmachende Berechtigung? Unbequeme Fragen … eingebettet in eine feine, musikalisch hochwertig begleitete Liebesgeschichte – letztendlich zu sich selbst."*

Die etwa 70 Besucherinnen und Besucher waren tief beeindruckt von dem fesselnden Stück. Nach der Aufführung entspann sich noch eine interessante Diskussion, in der sich die Unterschiede zwischen einer künstlerischen und einer politischen Auseinandersetzung mit dem Thema Krieg und Frieden offenbarte. Das TheaderFreinsheim verdiente noch viele weitere Gastspieleinladungen mit diesem Stück.

Das Cyberpeace-Forum wurde am Samstagnachmittag im Haus der Wissenschaft in der Bremer Innenstadt fortgesetzt, mit Vorträgen und Diskussionen unter dem Motto: *Gegen wachsende Rüstungsanstrengungen in Deutschland, Europa und anderswo.* In der Einladung heißt es dazu:

> *„Die Bundeswehr hat seit knapp einem Jahr ein Kommando Cyber- und Informationsraum. Neben Land, Luft, Wasser und Weltraum ist damit ein fünftes Schlachtfeld nun auch offiziell eröffnet. Darüber hinaus wird der Rüstungsetat Schritt für Schritt erhöht, um die Bundeswehr aus der Sicht der Regierung auf zukünftige Aufgaben in der Europäischen Verteidigungsunion und der NATO vorzubereiten. Diese Maßnahmen reihen sich ein in die weltweite Aufrüstung bei konventionellen und nuklearen Waffen. Insbesondere kann eine gigantische Aufrüstung für den Cyber- und Drohnenkrieg beobachtet werden, was völkerrechtswidrig gerade auch Zivilpersonen und zivile Infrastrukturen wie Strom- und Wasserversorgung, Verkehr, Gesundheitswesen und die Netzwerke von Staat und Wirtschaft in den Industriestaaten bedroht. In vielen Teilen der Welt ist Krieg mit schrecklichen Folgen für die Betroffenen. Die wachsenden Rüstungsanstrengungen weltweit bergen die Gefahr weiterer Kriege. Dass sich die Völker der Welt mit der Unterschrift unter die UN-Charta verpflichtet haben, ihre Konflikte friedlich zu lösen, scheint völlig vergessen. Das Cyberpeace-Forum dient der Diskussion über Kriegsgefahren und Friedenschancen, wobei moderne Rüstungstechnologie einen besonderen Fokus bilden."*



Die Veranstaltung bestand aus drei einstündigen Vortrags- und Diskussionsblöcken mit kurzen Pausen dazwischen, in denen Wasser, Saft, Kuchen, Kekse und Obst gereicht wurden. Die Vorträge können unter *https://mlecture.uni-bremen.de/ml/* angesehen werden.

Als Erstes habe ich selbst zu *Cyberpeace statt Cyberwar* vorgetragen. Ich habe das gleichnamige Video gezeigt (bei *vimeo* und *youtube* zu sehen), noch ein paar ergänzende Anmerkungen zu Cyberkrieg gemacht, um dann auf die Idee von Cyberpeace überzuleiten. Ich kann bestätigen, dass sich dieses vom FIfF in Auftrag gegeben fünfminütige Video bestens eignet, eine Diskussion über den Irrsinn des Cyberkriegs zu initiieren.

Andrea Kolling aus Bremen, die im *European Network Against Arms Trade* und in der *Fachgruppe Rüstungsexport der Gemeinsamen Konferenz Kirche und Entwicklung* mitarbeitet, hat zum

Thema *Von der Verdoppelung des Wehretats zu neuen Rekorden bei deutschen Rüstungsexporten* gesprochen. Es ist ein Skandal, dass die Bundesregierung trotz gegenteiliger Lippenbekenntnisse Waffenexporte in Krisengebiete erlaubt und bestehende Exportbeschränkungen immer mehr aufweicht. Es ist ein Skandal, dass das ominöse Zwei-Prozent-Ziel, also ein Wehretat von zwei Prozent des Bruttoinlandsprodukts, nicht mehr Diskussion und Widerstand herausfordert. Mit den Milliarden, die das Kriegswesen verschlingt, ließe sich wahrlich Besseres anstellen.

Und schließlich hat Franz Wanner, ein bildender Künstler aus München, einen videografischen Vortrag über *Battle Management Language – Sprachlose Mythen militärischer Strukturen* gehalten. Im Zentrum standen einige seiner Videosequenzen, die zu seinen Installationen gehören. Er hat u. a. Szenen aus seiner *5-Kanal-Videoinstallation DUAL-USE I – V* vorgeführt, die 2016 in der Städtischen Galerie im Lenbachhaus und Kunstbau München gezeigt wurde. Darin geht es zum Beispiel um die Firma *Sitec Aerospace* in Bad Tölz, deren Geschäftsführer Wert darauf legt, dass das Unternehmen trotz einschlägiger Produkte und Kunden nicht als Rüstungsbetrieb bezeichnet wird. Vorgestellt wird auch eine Drohnenpilotin, die zusätzlich als Model arbeitet. Und erwähnt sei noch die Vorstellung des *Ludwig Bölkow Campus* bei München, benannt nach dem Entwickler der Nazi-Düsenjäger, auf dem eine äußerst enge Zusammenarbeit von Wirtschaft und Wissenschaft auf dem Gebiet von Luft- und Raumfahrt in enger Verflechtung mit der Rüstung – als Verteidigung und Sicherheit verbrämt – betrieben wird.

Die Veranstaltung wurde organisiert vom Cyberpeace-Team Bremen, einer Kooperation des Bremer Friedensforums, der Bremerhavener Initiative Mut zum Frieden, der DFG-VK-Gruppe Bremen, der FIfF-Regionalgruppe Bremen, der GEW Bremen und der Rosa-Luxemburg-Initiative – Rosa-Luxemburg-Stiftung Bremen.

Weitere Informationen unter *cyberpeace.fiff.de.*

Lesen & Sehen

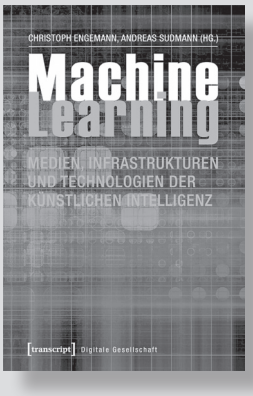
Neues für Bücherwürmer & Cineasten

Britta Schinzel

Christoph Engemann, Andreas Sudmann (Hg.): „Machine Learning“

Die beiden Medienwissenschaftler haben eine 17-teilige Textsammlung zum *Machine Learning* (ML) herausgegeben. Sie möchten einen Überblick über die angesprochenen informationstechnischen Entwicklungen aus historischer, epistemologischer, medienkultureller, technischer und philosophischer Sicht geben. Mit dem Begriff Machine Learning werden eine Reihe von Verfahren zusammengefasst, bei denen Programme anhand von Daten „lernen“, Aufgaben auszuführen. Machine Learning benutzt in einer ersten „Lern“-Phase eine Menge von eingegebenen Daten dazu, sie zu klassifizieren, Muster zu finden oder aus ihnen Regeln abzuleiten, um diese dann in der Anwendungsphase auf neue Daten anzuwenden oder automatisierte Reaktionen auszulösen. Hier werden also nicht wie bei sonstiger Software Konzepte und Relationen einprogrammiert sondern durch Lernprogramme auf einer Metaebene anhand von Daten zu einem Programm auf Gebrauchsebene „erlernt“. (Hieraus ergibt sich auch der Zusammenhang mit *Big Data*.) Techniken des Machine Learning werden jedoch erst im Interviewanhang, und nur am Beispiel von *Deep Learning* (DL) etwas klarer gemacht. Andere Techniken, wie *Support Vector Machines*, die auf geometrisch-topologischen Ansätzen beruhen und gern beim Versuch der Nachbildung von menschlichen Erkennungsleistungen in Verbindung mit fMRT-Bildern verwendet werden, oder die viel einfacheren Entscheidungsbäume, die immerhin den Vorteil von Reproduzierbarkeit und Nachvollziehbarkeit haben, werden nicht behandelt. Eher gewinnt die LeserIn Einsichten über die medienpolitischen Veränderungen durch Künstliche Neuronale Netze (KNNs), zu denen auch Deep Learning gehört; und diese im Wesentlichen mit Anwendungen im kommerziellen Bereich, zu denen auch soziale Netzwerke zählen.

Historisches dazu wird zwar angemessen dargestellt, aber diese Aufarbeitung ist bereits vielfach, etwa in den Bereichen Geschichte der Informatik und der KI, erfolgt. Ebenso sind die philosophischen Überlegungen wohlbekannt.



Engemann C., Sudmann A. (Hg.):
Machine Learning. Medien, Infrastrukturen und Technologien der Künstlichen Intelligenz;
Transcript Verlag (2018), Reihe Digitale Gesellschaft, Bd. 14
392 Seiten,
Preis € 32,99,
ISBN 978-3-8376-3530-0

Es ist sicher ein Verdienst von Hermann **Rotermund**, Charles Babbage‘s *Difference Engine* und seine *Analytical Engine* nochmals eingehender zu beschreiben, sowie Ada Lovelace‘s zukunftsweisende Gedanken über die potenziellen Fähigkeiten der Analytical Engine zu erwähnen. Letztere rechtfertigen die Aufnahme in ein Buch über ML.

Einige Texte befassen sich mit dem Lernen von ML an der Schule, es wird dadurch ein sukzessives Höherschrauben der Ansprüche an die SchülerInnen befürchtet, ja ein Kontrollverlust im Bildungssystem (Jeremias **Herberg**). Einige Texte befassen sich Robotern und Robotik (Jutta **Weber**).

Ich greife hier einige der mir interessant erscheinenden Texte heraus:

Eindrucksvoll ist Jutta **Weber**s Darstellung der *Disposition Matrix*, auf der mittels Big Data Tötungslisten und Ziele für Drohneneinsätze für den *War on Terror* zusammengeführt sind. Sie beschreibt die soziotechnische Verflechtung von Artefakten und menschlichen Entscheidungsprozessen im Kontext datenzentrierter Kriegsführung und diskutiert ausführlich die Probleme mit Big-Data-gespeistem ML.

Zunächst eine beispielhafte Definition der automatisierten Kriegsführung durch das *US Department of Defense* von 2012:

> *"A weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-super-vised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation."*

Künstliche Intelligenz (KI) wird zur Navigation, Zielerkennung und -identifikation sowie Angriffsplanung und -ausführung genutzt. Als Assistenzsystem für Kampfpiloten werden ML-Systeme darauf trainiert, Ziele anhand des Radars zu erkennen, um aus größerer Entfernung Abschussentscheidungen zu treffen. Weiter entwickelte Systeme können navigieren, entwerfen eigenständig eine Route und suchen nach Zielen, bis das Missionsziel erreicht ist. Noch avanciertere Systeme können simultan Geschossen ausweichen, auf mehrere Ziele feuern, sich an koordinierten Manövern beteiligen, feindliche Taktiken registrieren und davon lernen. Diese KI lief sogar auf einem nur 35 USD teuren Computer (Raspberry Pi) und wurde vom *US-Air-Force*-Colonel Gene Lee 2016 als „the most aggressive, responsive, dynamic and credible AI I've seen to date" bezeichnet.

Die Zielerfassung und -identifikation kann durch ML präzisiert werden, indem die typischen Fähigkeiten des DL – Wahrnehmung und Klassifikation von Objekten – eingesetzt werden. Die spezifischen Probleme solcher Software jedoch sind: systematische Lernfehler, mangelnde Nachvollziehbarkeit und die Anfälligkeit für Manipulationen.

Doch zu Webers Text: Die *Disposition Matrix* soll die Tötungslisten, die aus unterschiedlichen Quellen, CIA, NSA, aber auch den sozialen Medien, Journalistenkommunikation, NGOs etc. gespeist sind, „harmonisieren". Darin werden die Methoden, u. a. Social-Network-Analysen, Geodaten- und Sentiment-Analysen, integriert. Doch das Wissen darüber, wie und warum eine Relation in die Matrix gestellt wurde, geht während diesem vielschichtigen Prozess der Zusammenführung und Filterung der riesigen Mengen an Metadaten verloren und ignoriert jeglichen sozialen, politischen und kulturellen Kontext, aus dem die Daten stammen. Dazu bleibt auch geheim, wer aufgrund welcher Indikatoren in die Liste aufgenommen wird. Und, so meint Weber, auch eine genauere Definition von Terrorismus oder eine Verfeinerung der Kriterien für die Aufnahme in die Listen oder eine Verbesserung der Software behebe das eigentliche Problem nicht: den Mangel an Erklärung an kausalen Zusammenhängen, an Kohärenz, Konsistenz und Transparenz. Denn der Mangel an all dem, was etwa Rationalität und Verlässlichkeit produzieren könnte, ist integraler Bestandteil des Verfahrens. Sie fasst es zusammen als „das Verkennen von Form als Inhalt", eine Verkürzung, die m. E. vieles vermischt. Ich würde es lieber nennen „das Verkennen von Resultaten chaotisch mit Big Data verschränkter KI-Formalismen, denen jede Möglichkeit der Herleitung oder Verifikation fehlt, als Bedeutung". Doch die beim Lernen erzeugten Modelle können, mit einer unwahrscheinlichen Datenverteilung konfrontiert, Fehler erzeugen. Zudem stellt die Möglichkeit, maschinelles Lernen mit Eingabedaten so zu manipulieren, dass die folgenden Daten falsch interpretiert werden, ein großes Sicherheitsrisiko dar.

Das automatisierte Targeting produziert immer mehr Verdächtige, da mittels Metadaten die Beziehungen auf immer größere Umfelder ausgeweitet werden. Die „Entscheidung" über einen gefährlichen Terroristen als Tötungsziel beruht also auf vagen Kategorisierungen, was als Terrorismus und als zentraler Knoten in dessen kartiertem Netzwerk betrachtet wird. Durch die präsidentielle Letztentscheidung wird die nicht menschliche Vorentscheidung verschleiert und der Souverän vorgeschoben.

Denn John Brennan 2012:

> *„we conduct targeted strikes because they are necessary to mitigate an actual ongoing threat. What do we mean when we say significant threat? Significant threat might be posed by an individual who is an operational leader of Al Qaeda or one of its associated forces. Or the individual is himself an operative, in the midst of actually training for all planning to carry out attacks against US persons and interests. The individual processes unique opera skills that are being leveraged in planned attack."*

Im Folgenden befasst sich Weber mit den KI-, Big Data- und ML-Methoden im Allgemeinen: Mit moderneren No-SQL-Datenbanken, die auf Kosten von Kausalität, Reproduzierbarkeit, oder Konsistenz flexibel und schnell mit Big Data umgehen können, werden Probleme behandelt, „gelöst", die nicht voll verstanden sind, und deren Lösungsweg im Dunkeln bleibt. Nach Haraway und Manovich sind die wichtigsten Merkmale dieser epistemologischen Logik formalisiertes und systematisiertes *Tinkering*. Man denke an evolutionäre, probabilistische oder genetische Algorithmen, an Trial-and-Error-Verfahren, Suchheuristiken und Verfahren des Post-Processing. Die Methoden, Unberechenbares zu erschließen, seien Adaption, Imitation und Imagination. Im Gegensatz zur naturwissenschaftlichen Rationalität ist diese nicht an intrinsischen Eigenschaften von Objekten interessiert, sondern konzentriert sich auf deren Verhalten und ihre Relationen. Und sie ist auf mögliche Rekombinationen von Modulen, Codefragmenten, sowie das Erstellen von Systemblöcken hin orientiert. Techniken wie *Risk Profiling*, *Algorithmic Modeling*, *Information Integration* und *Data Analytics* ersetzen zunehmend die Prinzipien der Repräsentation und des Verstehens mit den Prinzipien der Investigation und der Intervention. *Data Mining* rekonfiguriert die Welt als flexibel, offen und unvorhersehbar, als einen Ort der Kombination, der Rekombination und des Redesigns (Haraway 1985/91), wo Daten klassifiziert, gruppiert, kombiniert und neu gruppiert werden, um Vorhersagen zu machen, Hypothesen zu testen und Suchen zu optimieren. Heuristiken, stochastische Prozesse, statistische

Methoden können kontingente Ergebnisse, zufällige Relationen und Rekombinationen produzieren.

Auch die Tötungslisten sind flexibel und dynamisch, da sich nicht nur die Datenlagen sondern auch die Regeln für ihre Auswahl ständig ändern. Das riesige Daten-Universum wird nach Schlüsselwörtern, Mustern, Assoziationen, Anomalien und Abweichungen untersucht. Gelöst werden soll nicht ein genau definiertes Problem, sondern es wird gemäß einem breit beschriebenen Ziel emergentes Verhalten in einem veränderlichen Problemraum unter gegebenen Randbedingungen beobachtet. Die offene Suchheuristik kennzeichnet die postmoderne präemptive Technosecurity um Ungewissheiten und unberechenbare Risiken, die mit vagen Kriterien wie Worst-Case-Szenarien die Imagination über Fakten stellen und so alle möglichen Bedrohungen vorweg nehmen und abwehren möchte.

Obgleich der Text relevante Informationen bietet und interessante gender- und medientheoretische Schlüsse zitiert, leidet er an einer gewissen Unschärfe und an Wiederholungen.

Christoph **Engemann**s Text *Rekursion über Körper. Machine-Learning-Trainingsdatensätze als Arbeit am Index* bezeichnet die Erstellung von Lerndatensätzen als „eine zeitlich und prozessual gespreizte Form der Verschränkung von Menschen und Computern", wobei Menschen als indexikalische Zeichengeber eingebunden werden.

Engemann interessiert sich v. a. für die Trainingsdatensätze für ML, denn insbesondere die kommerziell eingesetzten DL-Verfahren beim überwachten und halbüberwachten Lernen sind auf die Interaktion mit Menschen angewiesen. Dieses sei nicht nur als Voraussetzung für die spätere Autonomie-Anmutung, sondern auch medienwissenschaftlich bedeutungsvoll, jedoch bisher wenig erforscht. Beim überwachten Lernen werden während des Trainings (schichtweise) Korrelationen zwischen den Eingabedaten und Zielwerten gebildet. Die trainierten Modelle, welche die Zielwerte am besten treffen, werden am Ende genutzt. Beim Matching von Daten und Begriffen müssen für jedes lernrelevante Datum im Trainingsdatensatz – bisher händisch – Annotationen und Labels vergeben werden. Da ML umso besser funktioniert, je mehr und „qualitätvollere" Daten dem System zu Verfügung gestellt werden – für die Bilderkennung etwa Millionen von Bildern – ist dies eine aufwändige Arbeit. Bislang sind automatisierte Verfahren noch recht fehleranfällig, weisen *noise* auf. Zur Erkennung von Bildern werden auch *boundary boxes* eingefügt, welche gesuchte Features im Bild einrahmen. Für das Labeling von ML-Ergebnissen werden von Firmen wie Facebook und Google die Kunden oft als Klick-Worker gebraucht, auch für Objekte im Straßenverkehr, wie Verkehrsschilder, Hauseingänge oder Autobusse. Um der Ambiguität bei der Interpretation und Annotation von Bildern beizukommen, wird zur Qualitätskontrolle „ein statistisch organisiertes Misstrauen", d. h. die statistische Mittelung der Klicks vieler Nutzer, angefügt.

Engemann beschreibt die dreiteiligen ML-Verfahren als maschinisierte statistische Inferenz von Relationswahrscheinlichkeiten, hier für die Spracherkennungs- und Sprachausgabesoftware an Assistenzsystemen wie Siri oder Alexa und die Nachverwertung ihrer so gewonnenen Daten, nicht nur zur Optimierung der Systeme, sondern auch zur Individualisierung, Profilbildung und weiteren verschränkten Nutzungen. Während die Verfahren selbst von den Firmen derzeit sehr offen mit dem Ziel der Rekrutierung der besten MitarbeiterInnen publiziert werden, bleiben die Verfahren der Datenerschließung und des Labeling proprietär, von der Verwendung der Nutzenden als Klick-Worker abgesehen. Hier ziehen Google oder Facebook auch Relationen zwischen Bildern und Text, z. B. der *Google-reCaptcha-Service*, der unter anderem zur Annotation von Bildern aus Streetview, etwa Verkehrsschildern, auffordert, oder Facebook mit der Aufforderung an die Nutzenden, Personen auf Fotos mit Namen zu versehen, wodurch Labels entstehen, an denen Gesichtserkennungsnetzwerke trainiert werden können. So entstehen Trainingsdatensätze, die Dinge, Daten und Wörter einander zuordnen. Dies verweist schon auf die semiotische Frage, ob solchen Annotaten Indexikalität, d. h. eine Verbindung zwischen Wort und Ding, innewohnt. Zwar ist die Bindung von Daten, die als Adressen für Objekte, Prozesse oder Personen gelten sollen, aufgrund von Verfahren wie Metadaten-, relationalen Analysen etc. notwendigerweise unsicher. Doch wenn in die Lücke zwischen Wörtern, Daten und Dingen wie beim überwachten ML der etikettierende Mensch als verknüpfendes Relais gezogen wird, bleibt diese Zuordnung als Indexeffekt aufgezeichnet und sie garantiert durch die gewesene körperliche Anwesenheit die Passung von Datum, Label und Wirklichkeit. Engemann sieht dies als Verbindung von Körper zu Körpern, als verteiltes *Embodiment*, das auf eine genuin soziale Ressource zurückgreift, da es auf die Akquise und Konzentration anhand von Populationen kalibrierten Wissens angewiesen ist. Überwachtes ML also fragt nach Körpern, um eine großindustriell organisierte Indexikalisierung zu zeitigen, bei der durch massenhaftes Klick-Working und statistische Kopplung Zeichen auf Referenten verwiesen wurden, wobei die körperlichen Interaktionen die Referenten sind. Diese Human-Computer-Relation ist weder Anpassung zu menschengerechter Benutzung wie bei Human-Computer-Interfaces, noch Immersion, bei der virtuelle Körper auf reale Körper verweisen, sondern es ist eine rekursive Relation zwischen Körpern und lernenden Computern, von der vielfach iteriert auf menschliche schriftliche Aktionen rekurriert wird. Der politische Akt, der in den Verfahren zur Rekrutierung und den Prüfverfahren der zum Etikettieren akquirierten Menschen besteht, woraus die Trainingsdatensätze gebildet werden, ist bisher weder von staatlicher noch von zivilgesellschaftlicher Seite kontrolliert worden, und das, obgleich diskriminierende Effekte Legion sind.

Im gleichen Buch übersetzt Engemann auch einen Text von Lev **Manovich**, *Media Analytics und Gegenwartskultur*, in dem dieser, nach Kreation, Publikation und Distribution die neue Stufe der Entwicklung technologischer Medien, die Computerisierte Analyse sämtlicher online verfügbaren Inhalte diskutiert. Am Beispiel von Spotify wird beschrieben, welche Features dort aus dem Streaming von Songs extrahiert werden, um Nutzenden neue Playlisten anzubieten. Die Internet-Dienste für alle möglichen Spezialisierungen analysieren und wälzen minütlich Terabytes von Daten, für die die Informatik Methoden wie Information Retrieval, Data Mining, KI, Text-, Ton-, Sprach- und Geo-Analysemethoden entwickelt hat, die inzwischen unter dem Begriff *Data Science* zusammengefasst werden. In Echtzeit ablaufende Media Analytics sind heute Bestandteil aller großen Unternehmen, die soziale Netzwerke anbieten oder Medien-

güter online verkaufen, sowie Social Media Dashboards – i. e. Web-Tools für die Überwachung und Analyse von Benutzungsaktivitäten und Posting-Inhalten – verfügbar machen. Die Diskussion über politische und soziale Fragen bei Erfassung und Analyse von Benutzerinteraktionsdaten haben zu Unrecht bisher mehr Aufmerksamkeit erregt als die gleichermaßen folgenreichen politischen Praxen der automatisierten Analyse aller Arten von Online-Medieninhalten. Zusammengenommen haben sie nämlich durch den Einbau in Web-Services und Apps zu großen Verschiebungen der gesamten Medienkultur und Kulturindustrie geführt, die Millionen Personen nicht nur als Konsumenten, sondern auch als Content- und Meinungsbildner beteiligen. In diesem „Prosumer-Kapitalismus" etwa nutzen Konsumer-Produzenten die Services Google Analytics für Websites und Blogs oder Analytics Dashboards von Facebook und Twitter zur Feinabstimmung ihrer Posting-Strategien und Inhalte.

Solche interpersonale und Gruppen-Interaktionen sind seiner Meinung nach historisch neu, denn sie zeigen eine Industrialisierung der Kultur-Produktion in zweierlei Hinsicht: automatisiertes Aufzeigen von Inhalten, Updates und Informationen in Netzwerken einerseits und das optimierende Durchtesten von User Interfaces an großen Nutzerpopulationen andererseits.

Manovich untersucht dann die Werkzeuge der „Big Media"-Datenverarbeitung in der Kulturindustrie, Media Analytics, die online verfügbare Medieninhalte verarbeiten, und die der Cultural Analytics, die sich um Interaktionen zwischen Benutzenden, Softwarediensten und Apps kümmern, so dass individualisiert Inhalte angezeigt werden können. Erstere erlauben die Präsentation und das Abrufen relevanter Inhalte bezogen auf die Gesamtheit der Webinhalte. Komplexität und kontextuelle Vielfalt der angebotenen Tools sind unermesslich, und so sieht er mit ihnen eine neue Logik erreicht, wie Medien im Internet arbeiten und wie sie in der Gesellschaft funktionieren.

Media-Analytics-Werkzeuge wurden demokratisiert, so dass jede z. B. ihren Blog damit ausstatten kann, deren Ergebnisse dann aber auch für die Firmen verfügbar sind. Google hat das Verfahren, jede Nutzende zum Beta-Testen zu gebrauchen, popularisiert, so dass sämtliche Systeme durchgehend auf Grundlage der Interaktionen der Nutzenden lernen. Die neueren Akteure im Bereich der Kulturindustrie fungieren als Schnittstellen zwischen Menschen, professionellen Inhalten und *User generated Content*. In der Tat haben Durchdringung und Produktion mittels dieser Werkzeuge in einigen Branchen, etwa dem Journalismus, der Verlagsproduktion etc. bereits den Status von Totalität erreicht, wird doch inzwischen jedes kulturelle Artefakt automatisch verarbeitet. Automatisiert optimiert werden gleichzeitig auch Vertrieb, Marketing, Werbung, Entdecken und Empfehlen.

Die heutige Medien-Materialität umfasst Big-Data-Speicher- und Verarbeitungstechnologien sowie überwachtes ML, DL und andere maschinelle Lernparadigmen, wie Entscheidungsbäume, *Support Vector Machines* und *Convolutional Neural Networks*, aber auch tageszeitbasiert prädiktive Modelle für das Verhalten aller Personen.

Am Ende wendet er sich der auf Auswertung und Echtzeitanalysen beruhenden Automation von Medienaktivitäten zu. Solche können durch Benutzereingaben gesteuert werden oder auch nicht, und sie können in deterministischer oder – wenn Zufallsparameter integriert sind – in nicht-deterministischer Weise zustandekommen. In jedem Fall sind die Ergebnisse verschiedener Medienaktivitäten kontingent.

Manovich hält die Bezeichnung von Konzepten der automatisierten Analyse und Entscheidungsfindung als „Algorithmen" für irreführend, da sie zumeist auf ML beruhen. Solche Anwendungen sind, anders als Algorithmen, selten interpretierbar, womit er meint, dass die Schritte die bei ML zu Ergebnissen geführt haben, die nicht nachvollziehbar sind, sie wirken als Black Box. Besser sollten sie mit dem allgemeineren Begriff *Software* gefasst werden.

Schließlich kritisiert er die von kommerziellen Interessen geleiteten Metaanalysen und die Form derer Veröffentlichung durch die Kulturindustrie, welche dadurch der Öffentlichkeit und der Wissenschaft nicht in wünschenswerter Weise zur Verfügung stehen.

Der Text *Ein Meer von Daten* der Künstlerin Hito **Steyerl** bringt die Metapher der *Apophänie* ins Spiel, einer Art *Clustering Illusion*, aus der Psychiatrie bekannt, um die menschliche ebenso wie die maschinelle Wahrnehmung von verschlüsselten oder verrauschten Bildern zu fassen. Denn auch für die NSA, für Google und andere Datenabsauger ist die Extraktion von Informationen aus den ungeheuren und inkompatiblen Massen von Big Data ein enormes Problem. Sie zitiert Benjamin Bratton, dass es darum gehe „Verbindungen und Schlussfolgerungen aus Quellen zu ziehen, die keine direkte Verbindung, außer der zu ihrer eigenen unaufhebbaren Wahrnehmungsgleichzeitigkeit haben", die Analyse also oft der Apophänie gleichkommt. Google-Forscher bezeichnen das Erstellen eines Musters aus Rauschen als Inceptionism oder *Deep Dreaming*. Mag es als digitale Wahnvorstellung erscheinen, bringt diese Bildwahrsagerei durch schrittweise Aufversionierung doch oft das Unterbewußte eines Prosumer-Netzwerks ins Bild, etwa unzählige Augen, die einen durchlöchern, oder in Produkte eingebettete Bilder von Katzenbabys, die die Produktions-mittel entlarven. Sie fördert so einen unternehmerischen Animismus zutage, der nicht nur Waren fetischisiert, sondern seine Chimären in Franchises verwandelt. Geschieht diese Apophänie jedoch nicht, so landen die Lernresultate als schmutzige Daten.

Leider resultiert aber ein Vorgehen, das aus an wohlhabenden weißen Männern trainierter Sprache und Mustern – etwa die Unterscheidung von Lärm und Sprache – trifft, zu Ungleichheit, ja Diskriminierung von Bevölkerungsgruppen und wirkt als politischer „Spamfilter".

Als „schmutzig" erkannte und gesammelte Daten bilden andererseits auch einen Speicher heimlicher Ablehnung: Sie drücken die Verweigerung aus, gezählt oder gemessen zu werden.

Steyerl erkennt auch im Ansturm der Online-Formulare eine „Maschine" zur Akkumulation schmutziger Daten, da in der bürokratischen Verengung der Antwortmöglichkeiten notwendigerweise gelogen werden muss. Das Ausfüllen sinnloser Formulare hat auch eine Form „freiwilliger" Reproduktionsarbeit erzeugt, von unterbezahlten Daten-HausmeisterInnen verwaltet. Kein Wunder, dass im Gesundheitswesen der schmutzigste

Sektor des Datensammelns identifiziert wird. „Schmutzige Daten sind echte Daten, die den Kampf echter Menschen mit Bürokratien bezeugen."

Und noch mehr: Die omnipräsente Überwachung durch versklavte Objekte, Autos, Uhren, …, sagt uns: „Du denkst vielleicht, dass du uns besitzt, aber wir werden über dich informieren. Warte ab, welches Wesen wir in dir erkennen werden!"

Und Menschen, die keine Daten produzieren, werden als Abweichungen wahrgenommen, vielleicht als potenzielle Terroristen. Mit Scoring könnte man ihnen beikommen, einem Bedrohungsscore oder einem sozialen Bonitätsscore, wie es in China bereits geschieht. Die aus diesen Technologien emergierenden Regierungsformen erscheinen der Autorin sowohl veraltet als auch abergläubisch und sie fragt: Wie verbindet sich die Welt der Big-Data-Wahrsagerei mit den aktuellen Oligokratien, den Trollfarmen, Hackersöldnern, Botregierungen? Wie radikalisieren sie bestehende soziale Hierarchien? Ist der Staat in Zeiten von Deep Mind, Deep Lernen und Deep Dreaming ein Deep State? Einer in dem es keinen Einspruch oder angemessene Verfahren gegen maschinisierte Erlasse und Wahrsagerei gibt? Dabei sind es in Wahrheit doch nur Ergebnisse probabilistischer Projektionen.

Das Buch endet mit zwei Interviews, die Andreas **Sudmann** führte, das erste mit Yoshua **Bengio**, dem Direktor des *Montreal Institute for Learning Algorithms* (MILA), das zweite mit dem dortigen Assistenzprofessor Roland **Memisewic**.

Zuerst wird die Geschichte des ML beschrieben, der wichtigen Etappen, wie Backpropagation, tiefere Neuronale Netzwerke aus stückweise linearen gleichgerichteten Neuronen (ReLU), überwachtes, halb- und unüberwachtes Lernen, und die Zeitlichkeit berücksichtigende rekurrente Netzwerke. Medientheoretisch interessant ist, dass er als seine wichtigsten Werkzeuge immer noch Kugelschreiber, Bleistift und eine Tafel sieht, und dass er die Kommunikation mit Kollegen, die freie akademische Umgebung ohne vordefinierte Perspektiven als wichtigste Bedingungen für seine Kreativität erachtet. Zentral ist für ihn auch ein nicht hierarchisch organisiertes Labor, in dem den Studierenden viel Freiraum geboten wird: „Sie sind wie Katzen, sie haben ihren eigenen Kopf und lassen sich nicht einhegen. Die Belohnung für ein solches Vorgehen ist jedoch immens."

Das zweite Interview, *Wunderwerke der Parallelisierung*, beschreibt das Funktionieren von künstlichen neuronalen Netzwerken (KNNs) als sehr grobe Abstraktionen der Informationsverarbeitung in Gehirn. Eine genauere Orientierung an den Neurowissenschaften hat einerseits das Problem, dass mit dem vielen Detailwissen eine genauere Nachbildung extrem komplex würde, während andererseits bereits mit der groben Annäherung gute Lern-Ergebnisse erzielt werden können.

Bei der Frage, wie sich ML von menschlichem Lernen unterscheidet, kann die Adaption von Verbindungsstärken und deren Proportionalität zu neuronalen Größen (Hebb'sche Regel) als ähnlich angenommen werden. ML benötigt jedoch beim überwachten Lernen eine große Zahl gelabelter Beispiele, die auf eine bestimmte Lernaufgabe fokussiert sind, wohingegen Menschen sehr verschiedene Aufgaben quasi gleichzeitig erlernen, mit komplexeren Vorgängen als dem Zählen von Klassifikationserfolgen. Verkörperte Erfahrung ist wahrscheinlich der einzige Weg, zu irgendeiner menschenähnlichen Intelligenz zu gelangen, was sich im Wort be-greifen äußert.

Die für ML relevanten Medien – Hardware, GPUs, Netzwerktopologie – sind unverzichtbarer Bestandteil von Deep Learning. Erst sehr spät allerdings hat man die Hardware an KNNs adaptiert, denn der von- Neumann-Rechner verliert im Flaschenhals viel Zeit bei der Simulation. 2012 beschrieben Krizhevsky, Sutskever und Hinton Neuronale Netze auf GPU-Hardware, was seither eingesetzt wird und u. a. den enormen Fortschritt auf dem Gebiet erzeugt hat.

Von enormer Wichtigkeit sind die Datenmengen, oft auf Online-Marktplätzen wie Amazon's *Mechanical Turk* gelabelt, und natürlich die die Software, etwa für Backpropagation.

Dass DL heute auf digitalem Substrat funktioniert, ist nicht essenziell, es könnte ebenso auf analoger Hardware laufen. Im Prinzip kommen auch analoge Repräsentationen statt Zahlen infrage, in gewisser Weise zeigt die subsymbolische Repräsentation schon einen Weg dorthin. Ein Aspekt von KNNs ist der *Population Code*, eine Repräsentation, die durch gemeinsame Aktivität mehrerer Neuronen entstanden ist. Diese ist gewissermaßen analog, kann als Punkt in einem hochdimensionalen Raum verstanden werden, als reelle Zahl, aber in Fließkomma kodiert.

Die Umgebung, die Situierung, die beim Menschen so wichtig ist, spielt auch hier eine Rolle. Zwar benötigt ML nicht den Umweg über Kommunikation oder Belohnungsmechanismen. Dennoch spielt Situiertheit eine wichtige Rolle, weil viele Konzepte, die für Menschen relevant sind, in Alltagssituationen durch körperliche Erfahrung erworben werden.

Lernen in Netzen ist nicht lokalisierbar, aber Zeitaspekte spielen sehr wohl eine Rolle, etwa bei der gradientenbasierten Optimierung von grob zu fein, wo zunächst die grobe Struktur des

Britta Schinzel

Britta Schinzel promovierte in Mathematik, arbeitete in der Computerindustrie und habilitierte sich in der Informatik. Im Rahmen ihrer Professur für Theoretische Informatik an der RWTH Aachen arbeitete sie zunehmend interdisziplinär. Sie war von 1991 bis 2008 Professorin für Informatik und Gesellschaft und Gender Studies in Informatik und Naturwissenschaft an der Universität Freiburg.

Problems verstanden wird und im Laufe der Zeit feinere Unterscheidungen gelernt werden. Auch ist *Sparsity* ein zeitlicher Aspekt: Die Zahl der von null verschiedenen Werte in einer Schicht von Neuronen kann im Laufe des Trainings zunehmen. Im Extremfall, wenn für jedes Input-Datum nur ein Neuron in einer Schicht aktiv ist, kollabiert das System zu einer symbolischen Repräsentation, da jedem einzelnen Neuron hier die Rolle eines Symbols zukommt, das den Input eindeutig repräsentieren muss. Die Tendenz zur Sparsity kann man also als Tendenz zum Symbolischen im Laufe des Lernprozesses auffassen, vermutlich ähnlich wie bei menschlichen Lernvorgängen. Auch gibt es wie bei Menschen Schwankungen im Lernfortschritt. Menschliches Lernen ist von Analogiebildungen geprägt, da wir gezwungen sind, Brücken zwischen verschiedenen Aufgabenbereichen zu schlagen. Eine Denkmaschine, die auf Analogiebildung beruhen würde, hätte einfach mehr Daten zum Lernen.

Wissenschaft & Frieden 1/2019 „70 Jahre NATO“

Die NATO will sich zum 70. Jahrestag ihrer Gründung als „obersten Garanten von Freiheit und Sicherheit“ präsentieren und bei einem Gipfeltreffen im Dezember entsprechend selbst feiern. Ob Osterweiterung, die zunehmende Informationskriegsführung gegen Russland, die Aktivitäten im Hohen Norden, die Gründung von 25 Exzellenzzentren, der Ausbau der Raketenabwehr, die Anpassung der europäischen Verkehrsinfrastruktur an NATO-Bedürfnisse oder das Zwei-Prozent-Aufrüstungsziel – die NATO weitet ihren Aktionsbereich immer weiter aus. Mit Nord-Mazedonien wächst das Bündnis auf 30 Mitglieder an, und die Ukraine hat die NATO-Mitgliedschaft jüngst als Ziel in ihre Verfassung geschrieben. In Summe verdichtet sich der Eindruck: Die NATO bewirkt nicht Frieden, sondern mehr Konfrontation.

Die AutorInnen von W&F 1/2019 gehen in ihren Artikeln auf diese und weitere Aspekte ein:

- *August Pradetto*: Das hybride Bündnis – NATO-Osterweiterung zwischen Integration und Konfrontation
- *Nadja Douglas*: NATO-Russland-Beziehungen – Wege aus der Konfrontation?
- *Agneta Norberg*: Die NATO im Norden – Militarisierung des Nordens und des Ostseeraums
- *Christoph Jehle*: Militärische Mobilität in der EU
- *Katarzyna Kubiak*: NATO-Raketenabwehr – Stand und Herausforderungen
- *Christopher Schwitanski*: NATO-Exzellenzzentren – Motor der militärischen Transformation
- *Lühr Henken*: Das Zwei-Prozent-Ziel der NATO – Deutsche Aufrüstung und kein Ende?
- *Jürgen Wagner*: Die neue Normalität? NATO und Bundeswehr im (Informations-) Krieg mit Russland
- *Axel Gehring*: NATO-Austritt der Türkei?
- *Alexander Neu* und *Katja Keul*: Ist die NATO alternativlos?

Die Texte außerhalb des Schwerpunkts beschreiben die US-Pläne für Raketenabwehr (Regina Hagen), die illegale Rüstungsfinanzierung über den Europäischen Verteidigungsfonds (Björn Aust), die Vorbeugung gegen Dual-Use schon in der Softwareentwicklung (Thea Riebe und Christian Reuter) sowie die Rolle von Transdisziplinarität in der Friedens- und Konfliktforschung (Cordula Dittmer, Christine Fröhlich, Ulrike Krause). Im »Forum« wird u. a. an 80 Jahre nukleare Kernspaltung erinnert und die Kommentierte Presseschau befasst sich mit dem Aachener Vertrag zwischen Frankreich und Deutschland.

Wissenschaft & Frieden, 4/2018: „Kriegsgefahr 4.0“, 9,00 € Inland, EU plus 3,00 € Porto (Bitte um Vorkasse: Sparkasse KölnBonn, DE86 3705 0198 0048 0007 72, SWIFT-BIC COLSDE33XXX)

W&F erscheint vierteljährlich. Jahresabo 35 €, ermäßigt 25 €, Ausland 45 €, ermäßigt 35 €, Förderabo 60 €. W&F erscheint auch in digitaler Form – als PDF und ePub. Das Abo kostet für Bezieher der Printausgabe zusätzlich 5 € jährlich – als elektronisches Abo ohne Printausgabe 20 € jährlich.

Bezug: W&F c/o BdWi-Service, Gisselberger Str. 7, 35037 Marburg, E-Mail: *service@wissenschaft-und-frieden.de*, *www.wissenschaft-und-frieden.de*

Wissenschaft und Frieden ist Trägerin des Göttinger Friedenspreises 2018

FIfF e.V.

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

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

FIfF-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*

Cyberpeace
cyberpeace.fiff.de
Twitter Cyberpeace – *@FIfF_AK_RUIN*

Faire Computer
blog.faire-computer.de
Twitter Faire Computer – *@FaireComputer*

Mitglieder-Wiki
https://wiki.fiff.de

FIfF-Beirat

Ute Bernhardt (Berlin); **Peter Bittner** (Kaiserslautern); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Wolfgang Coy** (Berlin); Prof. Dr. **Wolfgang Däubler** (Bremen); 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. **Wolfgang Hofkirchner** (Wien); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (Konstanz); **Ulrich Klotz** (Frankfurt); Prof. Dr. **Klaus Köhler** (Mannheim); Prof. Dr. **Jochen Koubek** (Bayreuth); 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); **Ingo Ruhmann** (Berlin); Prof. Dr. **Gerhard Sagerer** (Bielefeld); Prof. Dr. **Gabriele Schade** (Erfurt); **Ralf E. Streibl** (Bremen); Prof. Dr. **Marie-Theres Tinnefeld** (München); Dr. **Gerhard Wohland** (Waldorfhäslach)

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Rainer Rehak (stellv. Vorsitzender) – Berlin
Michael Ahlmann – Kiel / Blumenthal
Sylvia Johnigk – München
Benjamin Kees – Berlin
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Prof. Dr. **Dietrich Meyer-Ebrecht** – Aachen
Kai Nothdurft – München
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
Frank Barnick – Bremen

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 200 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck
Schwerpunktredaktion	Rainer Rehak, Benjamin Kees, Stefan Hügel
V.i.S.d.P.	Stefan Hügel
FIfF-Überall	Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert.biskup@gmx.de*. Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *https://www.fiff.de/regionalgruppen*
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder, München
Cover	Motiv des Tagungsplakats der FIfFKon 2018
Druck	Meiners Druck, Bremen

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

Die FIfF-Kommunikation ist das Organ des FIfF und den politischen Zielen und Werten des FIfF verpflichtet. Die Redaktion behält sich vor, in Ausnahmefällen Beiträge abzulehnen.

Nachdruckgenehmigung wird nach Rücksprache mit der Redaktion in der Regel gern erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Wichtiger Hinweis: Wir bitten alle Mitglieder und Abonnenten, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

(mehr Termine unter *www.fiff.de*)

FIfFKon19 „Künstliche Intelligenz als Wunderland"
22.–24. November in Bremen

FIfF-Kommunikation

2/2019 „Brave New World Teil 2"
Rainer Rehak, Benjamin Kees, Stefan Hügel u. a.
Redaktionsschluss: 3. Mai 2019

3/2019 „IT-Security und Cyberpeace"
M. Ahlmann, S. Johnigk, H.-J. Kreowski, K. Nothdurft
Redaktionsschluss: 2. August 2019

4/2019 „Überwachungsgesamtrechnung"
Dagmar Boedicker u. a.
Redaktionsschluss: 1. November 2019

1/2020 „Künstliche Intelligenz als Wunderland"
Michael Ahlmann, Hans-Jörg Kreowski u. a.
Redaktionsschluss: 7. Februar 2020

W&F – Wissenschaft & Frieden

2/18 Wissenschaft im Dienste des Militärs?
(mit Dossier 86: Cyberrüstung und zivile IT-Sicherheit)
3/18 Gender im Visier
4/18 Kriegsführung 4.0
(mit Dossier 87: AfD, PEGIDA & Co.)
1/19 70 Jahre NATO

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

#223 Bürgerrechte im Sport
#224 Der Osten als Vorreiter? Rechtspopulismus im Gefolge wirtschaftlicher und politischer Umbrüche
#225 Wandel der Kommunikationsfreiheit durch Digitalisierung und Internet
#226 Polizei und Technikeinsatz

DANA – Datenschutz-Nachrichten

3/18 Big Data und KI
4/18 Technischer Datenschutz
1/19 Social Media
2/19 Ein Jahr DS-GVO – ein Résumé

Das FIfF-Büro

Geschäftsstelle FIfF e. V.
Ingrid Schlagheck (Geschäftsführung)
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
E-Mail: fiff@fiff.de
Die Bürozeiten finden Sie unter *www.fiff.de*

Bankverbindung
Bank für Sozialwirtschaft (BFS) Köln
Spendenkonto:
IBAN: DE79 3702 0500 0001 3828 03
BIC: BFSWDE33XXX

Kontakt zur Redaktion der FIfF-Kommunikation:
redaktion@fiff.de

Bits & Bäume 2018

Die Konferenz für Digitalisierung und Nachhaltigkeit

Forderungen des Trägerkreises (siehe Seite 7): Von links: Maria Bossmann (DNR), Hendrik Zimmermann (Germanwatch), Teresa Hoffmann (Brot für die Welt), Vivian Frick (IÖW), Nicolas Guenot (Konzeptwerk Neue Ökonomie), Juliane Krüger (OKF), Sven Hilbig (Brot für die Welt), Anja Höfner (IÖW), Rolf Buschmann (BUND), Leon Kaiser (Netzpolitik.org), Rainer Rehak (FIfF), Constanze Kurz (CCC), Tilman Santarius (TU Berlin) Fotos: Santiago Engelhardt, CC BY

Geeignete Texte für den SchlussFIfF bitte mit Quellenangabe an *redaktion@fiff.de* senden.