

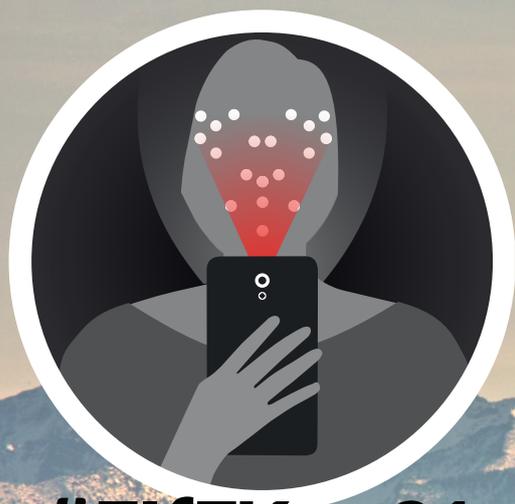
# E..I..f..F..Kommunikation

Zeitschrift für Informatik und Gesellschaft

39. Jahrgang 2022

Einzelpreis: 7 EUR

1/2022 – März 2022



**#FifFKon21**

## Selbstbestimmung in digitalen Räumen

*„Denn man sieht nur die im Lichte,  
die im Dunkeln sieht man nicht.“*

ISSN 0938-3476

• Weizenbaum-Studienpreis • Betrifft: Faire Computer • Cyberpeace •

## Inhalt

Ausgabe 1/2022

inhalt

- 03 Editorial  
- *Stefan Hügel*

### Forum

- 04 Der Brief: Deutsche Sicherheitspolitik am Scheideweg?  
- *Stefan Hügel*
- 06 NATO-Manöver im Cyberraum:  
Cyber Coalition, Locked Shields und Crossed Swords  
- *Aaron Lye*
- 10 Betrifft: Faire Computer – *Fair wie in Fairer Honig*  
- *Sebastian Jekutsch*
- 11 Schwerpunkt Digitalisierung in Staat, Politik & Verwaltung der FIfF-Kommunikation 3/2022  
- Call for Contributions
- 12 Kein Krieg in Europa und anderswo!  
- *FIfF e. V.*

### #FIfFKon21

- 18 Selbstbestimmung in digitalen Räumen  
Editorial zum Schwerpunkt  
- *Dagmar Boedicker*
- 19 Selbstbestimmung in digitalen Räumen  
Begrüßung  
- *Stefan Hügel*
- 20 Digitale Risikokompetenz  
- *Gerd Gigerenzer*
- 25 Potenziale und Grenzen automatisierter Fehlerreduktion  
- *Frauke Kreuter*
- 26 Digitale Gesellschaft zwischen Herrschaft und Innovation  
- *Philipp Staab*
- 29 Voreingenommenheit im Gehirn und im Algorithmus  
- *Abigail Morrison*
- 31 Kontrollierte Selbstbestimmung  
- *Silja Samerski*
- 35 Die soziale Konstruktion von Algorithmen  
- *Heiner Heiland*

### Rubriken

- 67 Impressum/Aktuelle Ankündigungen
- 68 SchlussFIfF

### Joseph Weizenbaum

- 14 Das Verschwinden des Computers  
- *Joseph Weizenbaum*
- 17 Joseph Weizenbaum: Das Verschwinden des Computers  
- *Andrea Knaut und Stefan Ullrich*

### Weizenbaum-Studienpreis 2021

- 38 Weizenbaum-Studienpreis 2021 – Einleitung  
- *Stefan Hügel*
- 39 Hendrik Heuer: Users & Machine-Learning-Based Curation Systems  
- *Laudatio für den ersten Preis*
- 40 Warum YouTubes KI gefährlich ist und was wir dagegen tun können  
- *Hendrik Heuer*
- 44 Helene Hahn: Digital identification systems and the right to privacy in the asylum context: An analysis of implementations in Germany  
- *Laudatio für den zweiten Preis*
- 45 Digitale Identifikationssysteme und das Recht auf Privatsphäre im Asyl-Kontext  
- *Helene Hahn*
- 50 Silke Meiser: Trust me! Vorschlag zum Umgang mit der Vertrauensfrage im digitalen Zeitalter  
- *Laudatio für den dritten Preis*
- 52 Zur (Mit-)Gestaltung der digitalen Gesellschaft durch rationales Vertrauen  
- *Silke Meiser*
- 56 Martin Schmitt: Die Digitalisierung der Kreditwirtschaft Computereinsatz in den Sparkassen der Bundesrepublik und der DDR, 1957-1991  
- *Laudatio für den dritten Preis*
- 57 Die Digitalisierung der Kreditwirtschaft  
- *Martin Schmitt*

### FIfF e. V.

- 62 Neumitglieder-Onboarding & intergalaktischer FIfF-Stammtisch
- 62 Protokoll der Mitgliederversammlung des FIfF
- 63 Jahresrückblick 2020/2021  
- *Stefan Hügel und Rainer Rehak*

## Editorial

Mit *Selbstbestimmung in digitalen Räumen* setzten wir uns bei unserer FIF-Konferenz 2021 auseinander: *Denn man sieht nur die im Lichte, die im Dunkeln sieht man nicht*. Traditionell bildet die Konferenz den Schwerpunkt der ersten Ausgabe der FIF-Kommunikation im neuen Jahr. Im Programm dazu heißt es:

*Unsere elektronischen Geräte sehen wir öfter und länger als Freunde oder Familie. Sie sind wichtige Arbeitsmittel und bequeme, allzeit bereite Helfer im Alltag, ohne sie ginge gar nichts mehr. Das wirft Fragen auf: Nach der Technik – wie funktioniert das? Nach gesellschaftlichen Folgen – welche sind das? Geht es auch anders?*

*Informationstechnik verändert rasant, wie wir kommunizieren, denken, uns bewegen und handeln. Sie dringt in persönliche und zwischenmenschliche Bereiche vor und beeinflusst unser Verhalten, ohne dass wir uns dessen immer bewusst sind. Wo wir uns als handelnde Subjekte sehen, werden wir oft als Objekte vermessen, bewertet und behandelt. Auf Plattformen und in sozialen Netzen, in smarten Infrastrukturen und in Scoring-Systemen wirken höchst profitable Geschäftsmodelle, die wir kaum durchschauen, geschweige denn (selbst) bestimmen können.*

Der Schwerpunkt, der auf den Konferenzbeiträgen basiert, wurde federführend von Dagmar Boedicker zusammengestellt, die auch das Schwerpunkteditorial besorgt hat.

Im Rahmen der Konferenz haben wir die Weizenbaum-Medaille an Christiane Floyd verliehen – die zugehörigen Beiträge müssen wir aus redaktionellen Gründen leider auf die nächste Ausgabe verschieben. Die Autorinnen und Autoren von vier Abschlussarbeiten – zwei Dissertationen und zwei Masterarbeiten – haben wir mit dem Weizenbaum-Studienpreis ausgezeichnet. Die Laudationes und eigene Beiträge der Ausgezeichneten bilden den zweiten Schwerpunkt dieser Ausgabe.

Den Namensgeber der Preise – Joseph Weizenbaum –, der im kommenden Januar 2023 100 Jahre alt geworden wäre, ehren wir auch diesmal mit dem Abdruck eines Beitrags: *Das Verschwinden des Computers, in dem er thematisiert, dass Computer immer unsichtbarer und allgegenwärtiger werden, 20 Jahre später fast eine Selbstverständlichkeit*:

*Der Computer wird in den nächsten fünf oder zehn Jahren aus unserem Bewusstsein verschwinden. Wir werden einfach nicht mehr über ihn reden, wir werden nicht über ihn lesen, außer natürlich Fachleute. ... nehmen wir einen Piloten in einem modernen Flugzeug mit zehn oder sechs Computern. Frage: Was muss der Pilot wissen über Computer? Antwort: Nichts. Er muss wissen, wie ein Flugzeug zu fliegen ist auch ohne Computer.*

In der Ausgabe 4/2022 wird es dann, wie bereits angekündigt, einen umfassenden Schwerpunkt zu Joseph Weizenbaum geben.

Auch unsere gewohnten Kolumnen sind in diesem Heft enthalten, die Kolumne *Cyberpeace*, in der Aaron Lye über *NATO-Manöver im Cyberraum: Cyber Coalition, Locked Shields und Crossed Swords* schreibt:

*Auf dem Warschauer Gipfel im Jahr 2016 hat die NATO den Cyberraum/Cyberspace zum Operationsgebiet erklärt und sich die Verbesserung ihrer operativen Reaktionen und die Entwicklung der Kriegsführung durch Übungen als Ziel gesetzt. Allerdings wurden informationstechnische Angriffe bereits auf dem Gipfel 2006 in Riga als mögliche asymmetrische Bedrohungen genannt und gemeinsame Programme zum Schutz von Informationssystemen als notwendig festgehalten. Seit 2008 trainiert die NATO in gemeinsamen Manövern den Cyberkrieg.*

Und nach langer Zeit gibt es auch wieder die Kolumne *Betrifft: Faire Computer*, in der Sebastian Jekutsch in dieser Ausgabe zu den Rahmenbedingungen und Auswirkungen des Lieferkettengesetzes schreibt:

*Das deutsche Lieferkettengesetz sieht für Unternehmen eine Pflicht zur Risikoanalyse nicht nur sowieso bei direkten Auftragnehmern, sondern auch tiefer in der Lieferkette vor, wenn es substantielle Hinweise auf Menschenrechtsverletzungen gibt. Die liegen hier offensichtlich vor. Und China ist in Sachen IT und Elektronik überall in der Lieferkette, vom Zusammenschrauben bis zu den Rohstoffen. Etwas dumm für das zentrale Anliegen der Energiewende vielleicht, dass ausgerechnet für Solarzellen nun konkrete Nachweise von Zwangsarbeit im Westen Chinas vorliegen.*

Dazu kommen interne Beiträge, ebenfalls im Zusammenhang mit der FIF-Konferenz. Inzwischen hat sich auf den Konferenzen der Jahresrückblick etabliert; in diesem Jahr vorgetragen von Rainer Rehak und Stefan Hügel. Dazu gibt es das Protokoll der Mitgliederversammlung, die auch einen neuen Vorstand wählte. Die meisten Mitglieder wurden wiedergewählt. Jens Rinne hat nicht mehr kandidiert und scheidet aus dem Vorstand aus – vielen Dank für jahrelange engagierte Mitarbeit. Benjamin Kees wurde nach einer kurzen Pause wiedergewählt, Frieder Strauß wurde als neues Mitglied in den Vorstand gewählt. Allen Gewählten herzliche Glückwünsche und viel Erfolg in ihren Ämtern.

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

Stefan Hügel  
für die Redaktion



## Deutsche Sicherheitspolitik am Scheideweg?

*Jede und jeder Einzelne von uns muss jetzt eine dezidierte und verantwortungsvolle Entscheidung treffen und Partei ergreifen.*  
(Bundesaußenministerin Annalena Baerbock<sup>1</sup>)

*Es war gespenstisch.  
Die deutschen Parlamentarier feierten die größte Aufrüstung,  
die es in der deutschen Geschichte seit dem Zweiten Weltkrieg je gegeben hat.  
Schweigen und stiller Ernst wären angemessen gewesen.*  
(Jakob Augstein<sup>2</sup>)



Liebe Freundinnen und Freunde des Fiff, liebe Mitglieder,

es herrscht (wieder) Krieg in Europa. Aus aktuellem Anlass, und um es gleich unmissverständlich klar zu machen: Die Aggression von Präsident Putins Russischer Föderation gegen den souveränen Staat Ukraine ist durch nichts zu rechtfertigen. In diesem Moment wissen wir noch nicht, wie dieser Krieg weiter verlaufen und welche langfristigen Folgen er haben wird, und sicherlich wird einmal aufzuarbeiten sein, wie es dazu gekommen ist und welche Konsequenzen er haben muss. Doch zunächst gilt unsere Solidarität der Bevölkerung der Ukraine, die – wie immer – die Hauptlast des Krieges zu tragen hat. Kriege werden von (politischen und militärischen) Eliten geführt, auf Kosten der Menschen.

Diese Ausgabe enthält unsere Stellungnahme dazu.<sup>3</sup> Wir wurden dafür auch kritisiert, bleiben aber bei unserer Aussage zur akuten Situation. Natürlich wissen wir, dass dieser Konflikt – wie wohl immer in vergleichbaren Fällen – eine Vorgeschichte hat, und natürlich wissen wir, dass auch die NATO bereits völkerrechtswidrige Angriffskriege geführt hat – zu denen wir beizeiten Stellung bezogen haben. Das ändert aber nichts an der fehlenden Legitimität dieser Aggression wie auch jedes anderen völkerrechtswidrigen Angriffskrieges. Den vereinzelt gegen uns erhobenen Vorwurf, NATO-Propaganda zu betreiben, weisen wir entschieden zurück.

Mit großer Sorge müssen wir wohl auch die Konsequenzen betrachten, die in Deutschland daraus gezogen werden. Die Initiative der Bundesregierung, mit 100 Milliarden € „Sondervermögen“ ein gigantisches Rüstungsprogramm aufzulegen, ist erschreckend – noch erschreckender der große Beifall im Deutschen Bundestag, als Bundeskanzler Scholz diese bedrückenden Planungen verkündete. Bemerkenswert, dass es von einer Bundesregierung unter rot-grüner Beteiligung vorangetrieben wird. Schon tauchen aber auch die „Konservativen“ auf, die sich gegen die angeblich grassierende „Wohlstandsverwahrlosung“ wenden und dazu aufrufen, endlich wieder die aus ihrer Sicht notwendigen Schwerpunkte zu setzen: Sicherheitspolitik statt Klimapolitik, Ausbau der Bundeswehr, Wiederaufnahme der ausgesetzten Wehrpflicht. Wir befinden uns in einem komplexen Spannungsfeld, in dem es keine einfachen Lösungen gibt. Doch Zusammenhänge sind erkennbar: Klimapolitik steht nicht im Gegensatz zur Sicherheitspolitik, Klimapolitik ist Sicherheitspolitik. Hätten wir beizeiten auf erneuerbare Energien gesetzt, wären wir nicht im heutigen Maß von Energielieferungen einzelner Staaten abhängig. Die große Gefahr, die von Atomkraftwerken ausgeht, wird uns aktuell deutlich vorgeführt – nachdem

uns die Europäische Kommission gerade einreden wollte, Atomenergie sei *umweltfreundlich*.

Dieser Krieg ist auch ein Informationskrieg. Wir können aus der Ferne kaum einschätzen, welche Berichte wahr sind und welche nicht. Wir beobachten aus der Ferne die diplomatischen Bemühungen von Bundeskanzler Scholz und Außenministerin Baerbock, ohne wirklich zu wissen, was dort im Einzelnen mit welchem Ziel und welchem Ergebnis besprochen wurde. Doch das liegt in der Natur der Sache.

„Das erste Opfer des Krieges ist die Wahrheit“ gilt auch hier, mehr oder weniger, auf beiden Seiten. Wir kritisieren die russische Propaganda und die aktuell stattfindende Schleifung der Pressefreiheit in Russland. Doch wir sind stets darauf angewiesen, die Glaubwürdigkeit von Akteur:innen und Medien zu beurteilen und uns daraus ein Bild zu machen. Zwischen Berichten von Medien, von denen wir annehmen dürfen, dass sie seriös sind auf der einen Seite und aus dem Zusammenhang gerissenen Filmfetzen in den sozialen Medien auf der anderen Seite gibt es eine breite Grauzone. Einzelnen Tweets auf Twitter zufolge wurde ein verbreitetes deutsches Blatt dabei erwischt, wie es seine Berichterstattung aus der Ukraine mit emotionsheischenden Bildern garnierte, die mit der Ukraine nichts zu tun hatten: Falsches Jahr, falsches Land, falscher Krieg. Doch eigentlich wissen wir nicht einmal mit Sicherheit, ob wiederum *das* eigentlich stimmt.

Nicht nur dieser Krieg betont die Bedeutung vertrauenswürdiger Medien – und spiegelbildlich des Vertrauens in ihre Berichterstattung. Soziale Medien spielen dabei eine ambivalente Rolle: Sie können Falschinformationen verbreiten und sie können Nachrichten auf ihren Wahrheitsgehalt überprüfen. Nicht nur in diesem Konflikt lassen die Akteure die Grenzen zwischen Wahrheit und Falschinformationen immer mehr verschwimmen: Akteure, die sich davon politische Vorteile versprechen. Das dürfen wir nicht zulassen.

Die Covid-19-Pandemie mit wieder steigenden Inzidenzen haben wir darüber fast vergessen. Sie zeigt bereits seit zwei Jahren die Probleme wie in einem Brennglas auf: Eine unsichtbare Bedrohung, komplexe Zusammenhänge und Wechselwirkungen und zum Teil eine vergiftete öffentliche Debatte führen immer weiter in einen gesellschaftlichen Konflikt und sogar die Abwendung eines Teils der Gesellschaft von der Demokratie. Nachdem wir in unserem letzten Weihnachtsbrief positiv zum Impfschutz Stellung genommen haben, erreichte uns am ersten Weihnachtstag eine E-Mail über unseren Verteiler fiff-I, die ich hier auszugsweise zitiere:

*Ich hatte leider nie Zeit, die Arbeit des Fiff aktiv zu unterstützen oder auch nur zu begleiten. Trotzdem hatte ich den Eindruck, dass das Fiff eine wertvolle Arbeit leistete. Dafür bin ich dankbar.*

*Umso unverständlicher ist es, dass das Fiff trotz des Wissens um die Macht der Digitalkonzerne, deren Kriminalität und die Möglichkeiten der totalen Kontrolle, die Lüge von der Pandemie auch Ende 2021 noch nicht durchschaut hat. Wer darüber hinaus die Behauptung einer Pandemie unterstützt, beteiligt sich an Verbrechen gegen die Menschlichkeit.*

*Das Mitgliederanschreiben von Stefan Hügel und Rainer Rehak vom Dezember 2021 (per Post) unterstützt nicht nur die Pandemielüge sondern auch noch die mörderischen sogenannten „Impfungen“.*

Das sind schon heftige Aussagen: Wir beteiligen uns also an Verbrechen gegen die Menschlichkeit, weil wir glauben, dass es die Covid-19-Pandemie wirklich gibt? Wir unterstützen mörderische Impfungen? Eine detaillierte Stellungnahme zu solchen Anwürfen dürfte sich erübrigen. Aber was läuft in unserer Gesellschaft gerade schief, dass sich Menschen solch einer Rhetorik bedienen?

Das Fiff ist eine konsequent friedenspolitische Organisation, die insbesondere Angriffskriege ohne Wenn und Aber ablehnt. Wir richten uns an wissenschaftlichen Erkenntnissen aus, ohne in einen naiven Szientismus zu verfallen. Wir sind uns der komplexen Wechselwirkungen in Politik, Gesellschaft und Wissenschaft bewusst. Wir beziehen klar Stellung, wenn die Situation es verlangt. Und wir diskutieren divergierende Standpunkte mit Respekt voreinander. Wenn wir auch in der Sache streiten: darauf – und auf ein paar Punkte<sup>4</sup> mehr – sollten wir uns einigen können.

Mit Fiffigen Grüßen  
Stefan Hügel

## Anmerkungen

- 1 Vor der UNO-Generalversammlung, 1. März 2022, <https://www.auswaertiges-amt.de/de/newsroom/baerbock-vnga-ukraine/2514746>
- 2 Gigantisches Rüstungspaket von Olaf Scholz ist gefährlicher Irrweg, Der Freitag 9/2022, <https://www.freitag.de/autoren/jaugstein/gigantisches-ruestungspaket-ist-gefaehrlicher-irrweg>
- 3 Seite 12 in dieser Ausgabe und <https://www.fiff.de/kein-krieg-in-europa-und-anderswo>
- 4 <https://www.fiff.de/about>



## Das Fiff bittet um Eure Unterstützung

Viermal im Jahr geben wir die Fiff-Kommunikation heraus. Sie entsteht durch viel ehrenamtliche, unbezahlte Arbeit. Doch ihre Herstellung kostet auch Geld – Geld, das wir nur durch Eure Mitgliedsbeiträge und Spenden aufbringen können.

Auch unsere weitere politische Arbeit kostet Geld für Öffentlichkeitsarbeit, Aktionen und Organisation. Unsere jährlich stattfindende Fiff-Konferenz, der Weizenbaum-Preis, weitere Publikationen, Kommunikation im Web: Neben der tatkräftigen Mitwirkung engagierter Menschen sind wir bei unserer Arbeit auf finanzielle Unterstützung angewiesen.

**Bitte unterstützt das Fiff mit einer Spende.** So können wir die öffentliche Wahrnehmung für die Themen weiter verstärken, die Euch und uns wichtig sind.

### Spendenkonto:

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

Stefan Hügel und Hans-Jörg Kreowski

## Aufruf zur Einreichung von Beiträgen

Das Schwerpunktthema der Fiff-Kommunikation 2/2022 ist

### Künstliche Intelligenz – Zwischen hochgeschraubten Erwartungen und unkalkulierbaren Risiken

Der große Hype um die Künstliche Intelligenz scheint zumindest medial schon wieder etwas abzunehmen. In Politik und Wirtschaft sind die Erwartungen aber weiterhin groß, wie die nationalen Strategien für Künstliche Intelligenz (KI) vieler Regierungen in aller Welt zeigen. KI wird als Schlüsseltechnologie zukünftiger Wertschöpfung auserkoren und mit gigantischen Finanzmitteln gefördert. Selbst eine geostrategische Bedeutung wird darin gesehen, bei KI die Nase vorn zu haben. Interessanterweise wird in den Strategiekonzepten auch häufig auf ethische Aspekte hingewiesen. KI soll zum Wohle der Menschen genutzt und problematische Anwendungen vermieden werden.

Wir bitten um Beiträge für diesen Schwerpunkt an [redaktion@fiff.de](mailto:redaktion@fiff.de) im Umfang von 10.000 bis 20.000 Zeichen.

Der Redaktionsschluss ist der 6. Mai 2022. Wir wären aber dankbar für eine baldige Absichtserklärung mit Angabe zu den Autor:innen und zum Thema.

Mit Fiffigen Grüßen

Stefan (Hügel) und Hans-Jörg (Kreowski)

## NATO-Manöver im Cyberraum: Cyber Coalition, Locked Shields und Crossed Swords



Auf dem Warschauer Gipfel im Jahr 2016 hat die NATO den Cyberraum/Cyberspace zum Operationsgebiet erklärt und sich die Verbesserung ihrer operativen Reaktionen und die Entwicklung der Kriegsführung durch Übungen als Ziel gesetzt. Allerdings wurden informationstechnische Angriffe bereits auf dem Gipfel 2006 in Riga als mögliche asymmetrische Bedrohungen genannt und gemeinsame Programme zum Schutz von Informationssystemen als notwendig festgehalten. Seit 2008 trainiert die NATO in gemeinsamen Manövern den Cyberkrieg.

Die eingesetzten Waffen sind Werkzeuge aus dem Bereich der Informatik. Offensive Operationen umfassen Aktionen, die durchgeführt werden, um Daten von IT-Systemen des Ziels oder des Gegners zu exfiltrieren (Spionage), Informationen zu manipulieren, Informationsflüsse zu beeinträchtigen oder Systeme zu zerstören. Umgekehrt gehört zum Cyberkrieg die Bereitstellung und Aufrechterhaltung der eigenen Kommunikations- und Kommandostrukturen sowie die Abwehr gegnerischer Angriffe auf eigene Systeme. Entsprechend umfassen defensive Operationen die Maßnahmen, die ergriffen werden, um unbefugte Aktivitäten in den IT-Systemen und Computernetzwerken (einer Regierung) zu schützen, zu überwachen, zu analysieren, aufzudecken und darauf zu reagieren.

Da sich informationstechnische Angriffe wesentlich von konventionellen unterscheiden, macht das Aufkommen der Cyberkriegsführung es erforderlich, dass Politik, Strategien, Konzepte, Doktrinen, Verfahren sowie Fähigkeiten und Personalstruktur umgestaltet werden. Tätigkeiten, die klassisch Geheim- und Nachrichtendiensten zugeordnet sind, werden jetzt ebenfalls vom Militär praktiziert. Entsprechend sind diese Teile des Militärs oft den Geheim- und Nachrichtendiensten des Landes nahe stehend oder assoziiert. Das United Nations Institute for Disarmament Research hat bereits 2013 fast 100 Staaten identifiziert, welche sich innerhalb des Militärs für informationstechnische Kriegsführung rüsteten.<sup>1</sup>

Im Folgenden sollen die drei wichtigsten bekannten Manöver beleuchtet werden, die regelmäßig und in wechselnder Zusammensetzung von der NATO durchgeführt werden. Bei allen drei sind die Übungsszenarien fiktiv und finden in einer auf Europa basierenden Geografie statt. Des Weiteren handelt es sich um sogenannte *Multi-level Exercises*, bei denen unterschiedliche Schichten trainiert werden: Strategie, operative Ebene, Taktik und technische Ebene. In der Übung *Cyber Coalition* werden v. a. Entscheidungsstrukturen geübt, bei *Locked Shields* hingegen versuchen mehrere Teams Cyberangriffe abzuwehren, wohingegen bei dem Übungszyklus *Crossed Swords* offensive Cyber-Operationen zur Unterstützung von Spezialkräften geübt werden. Darüber/darunter liegende Schichten oder Teile davon werden simuliert.

Bei den technischen Manövern gibt es fünf Teams. Das rote Team greift an. Das blaue Team verteidigt. Darüber hinaus gibt es das weiße Team, welches die Übung leitet und verwaltet, das gelbe Team, welches für die Situationserfassung zuständig ist, und das grüne Team, welches die technische Infrastruktur entwickelt und verwaltet.

### Cyber Coalition

Seit 2008 findet jährlich im November das Manöver *Cyber Coalition*<sup>2</sup> statt. Es wird als die wichtigste Cyber-Übung der NATO, als Flaggschiff der kollektiven Cyberverteidigungsübung der NATO und eine der größten Übungen dieser Art weltweit beworben. Das Manöver dauert drei Tage.

*Cyber Coalition* ist eine kollektive Übung, d. h. die Teilnehmer:innen arbeiten gemeinsam auf ein bestimmtes Ziel hin, um Probleme zu lösen oder bestimmte Aufgaben zu erfüllen, anstatt miteinander zu konkurrieren. Das Manöver soll die Strategieplanung auf operationaler und taktischer Ebene sowie deren Umsetzung durch die NATO und seine Mitglieder trainieren.

Die Übung wird vom Allied Command Transformation<sup>3</sup> unter der Leitung des Militärausschusses – und damit formal auf der höchsten Ebene der militärischen Hierarchie – geplant und durchgeführt.

An der Übung sind zahlreiche NATO-Einrichtungen beteiligt, darunter das NATO Cyberspace Operation Centre und die NATO-Kommunikations- und Informationsagentur (NCIA), welche für die gemeinsame Standardisierung und Beschaffung von IT-Komponenten und -Dienstleistungen zuständig. Eine zentrale Rolle nimmt auch das im estländischen Tallinn ansässige NATO-Exzellenzzentrum für gemeinsame Cyberabwehr (Cooperative Cyber Defence Centre of Excellence, CCDCOE) ein.<sup>4</sup> Unterstützt werden sie von Akteuren aus der Industrie und der Wissenschaft. Sie finden im Cyber Security Exercise and Training Centre CR14 in Tallinn statt. Dieses stellt die Infrastruktur (virtuelle Umgebung), um die (technischen) Szenarien zu erproben. Über virtuelle Netze (VPN) nehmen die Teilnehmer:innen und die örtlichen

Aaron Lye

Aaron Lye hat an der Universität Bremen Informatik studiert und dort auch Ende 2021 seine Promotion abgeschlossen. Er ist seit Jahren beim FIF aktiv.

Ausbilder:innen aus ihren jeweiligen Staaten und Einrichtungen an der Übung teil, eine kleine Übungssteuerungsgruppe kommt in Estland zusammen, um die Übung durchzuführen.

In den letzten Jahren waren jeweils 700 bis 1.000 Menschen beteiligt. 2021 nahmen rund 1.000 Teilnehmer:innen aus 25 NATO-Mitgliedstaaten, vier Partnerstaaten und der Europäischen Union (EU) teil, darunter insbesondere der EU-Militärstab und das Computer Emergency Response Team für die EU.

Ziel der Übung ist es, neue Taktiken, Techniken und Verfahren zu prüfen. Das bedeutet, erstens die Zusammenarbeit zwischen NATO-Gremien, NATO-Verbündeten und Partnerstaaten als auch Behörden zu verbessern; zweitens die Verbesserung der Fähigkeit des Bündnisses zur Durchführung von sogenannten Cyberspace-Operationen für militärische und zivile Stellen durch die Entwicklung eines Lagebewusstseins, den Austausch von Informationen und die Bewältigung von Angriffen; drittens die Bereitstellung einer Plattform zur Ermittlung von Fähigkeitslücken und Ausbildungsanforderungen sowie zur Validierung von Verfahren der Cyber-Kriegsführung.

Mithilfe von Szenarien und Handlungsabläufen (u. a. Angriffe auf kritische Infrastrukturen, Eindringen in Netzwerke, Spionage, Insider-Bedrohungen, Exfiltration und Datenmanipulation) soll das Manöver die Koordinierung, die Zusammenarbeit und den Informationsaustausch innerhalb der NATO verbessern. Das Manöver umfasst mehrere gleichzeitige Cyberangriffe auf die NATO und NATO-Mitgliedstaaten. Das Übungsszenario konzentriert sich auf eine fiktive Insel – Icebergen genannt – im Nordatlantik und umfasst eine Reihe realistischer Szenarien. Zu den Szenarien 2021 gehörten ein Cyberangriff auf Gasversorgungspipelines, ein Cyberangriff, der die Verlegung von Truppen und die Logistik stört, und ein pandemiebezogener Ransomware-Angriff, bei dem Impfstoffdaten gestohlen und Impfprogramme gefährdet werden.

Das Training von Malware-Analyse, Netzwerk- und Computer-Forensik, also die Analyse der Urheber, Techniken und Taktiken der Angriffe, ist eher nebensächlich und nur ein kleiner Teil des Manövers. Es gibt zwar unterschiedliche Angriffe und Malware, die analysiert und abgewehrt werden sollen, das technische Personal soll aber vor allem Berichte für die operationelle Ebene produzieren.

## Locked Shields

Seit 2010 veranstaltet die NATO jährlich im April in Tallinn die Echtzeit-Netzwerkverteidigungsübung *Locked Shields*<sup>5</sup>. Diese Übung dauert zwei Tage.

Während *Cyber Coalition* primär kollaborativ ausgerichtet ist, ist dieses Manöver kompetitiv konzipiert. Nur ein (verteidigendes) blaues Team kann gewinnen. Die Übung ist als Wettbewerbsspiel aufgebaut, bei dem die verteidigenden Teams auf der Grundlage ihrer Leistung bewertet werden. Obwohl die Teams miteinander konkurrieren, ist die Übung so angelegt, dass sie die Teams ermutigt, Informationen auszutauschen und so weit wie möglich zusammenzuarbeiten.

Anfangs war es eine ausschließlich technische Übung. Mittlerweile handelt es sich ebenfalls um ein Multi-Level Exercise, welches ebenfalls die operative Ebene einbezieht (allerdings liegt der Fokus nach wie vor auf der technischen Ebene).

*Locked Shields 2021* wurde vom CCDCOE in Zusammenarbeit u. a. mit der NCIA, dem estnischen Verteidigungsministerium, den estnischen Streitkräften, dem NATO-Exzellenzzentrum für Strategische Kommunikation (Strategic Communications Centre of Excellence, STRATCOM COE), der Europäischen Verteidigungsagentur (EDA), dem US Federal Bureau of Investigation (FBI) sowie dem europäischen Kompetenzzentrum für die Bekämpfung hybrider Bedrohungen ausgerichtet. Hinzu kamen zahlreiche Industriepartner (siehe Kasten).

### Industriepartner bei *Locked Shields 2021*:

Arctic Security, Atech, Avibras, BHC Laboratory, Bittium, Bolt, Bytelife, Cisco, Clarified Security, Cyber Test Systems, Cybernetica, Elisa, Ericsson, Foundation CR14, GuardTime, Iptron, Microsoft, openvpn, PaloAlto networks, Sentinel, Siemens, SpaceIT, STM, Stamus Networks, Synopsys, SUTD iTrust Singapore, TalTech, Thred Systems, VTT Technical Research Centre of Finland

Die Übung findet im Hilton-Hotel in Tallinn statt. Des Weiteren werden die zu verteidigenden Systeme visuell oder modellhaft aufbereitet. Beides dient dazu, die Übung für Politiker:innen, Entscheider:innen und Sponsoren ansprechend zu machen.

Das CCDCOE stellt Personal für das weiße, gelbe, grüne sowie das offensive rote Team. NATO-Staaten, Partner, aber auch das NATO Computer Incident Response Capability stellen die blauen Teams. Zu den Teilnehmer:innen gehören Sicherheitsexpert:innen, die nationale IT-Systeme schützen, sowie politische Beamte und Rechtsberater:innen von NATO-Verbündeten und Partnern. Während sich die Organisatoren der Übung vor Ort treffen, haben die teilnehmenden blauen Teams via VPN Zugang zu den Übungsnetzen.

Die Teilnehmer:innenzahl erhöhte sich alle zwei bis drei Jahre signifikant (2012: 200, 2015: 400, 2018: 1000, 2021: 2000). Die Anzahl der teilnehmenden Staaten belief sich bis 2015 auf ca. 17, die zusammen mit 12 blauen Teams antraten. 2016 waren es schon 26 Staaten und 20 blaue Teams und ab 2018 fast 30 Staaten mit 22 blauen Teams.

Die blauen Teams haben die Aufgabe, die Netze und Dienste eines fiktiven Landes – Berylia – unter großem Druck aufrechtzuerhalten. Dazu gehören die Bewältigung und Meldung unterschiedlicher Angriffe auf eine Vielzahl von Systemen, die Lösung forensischer Herausforderungen sowie die Reaktion auf rechtliche, mediale und szenarienbedingte Einwirkungen. Umgesetzt wird das anhand von einem großen virtualisierten Netzwerk und einem fiktiven Szenario inkl. der simulierten Infrastruktur des fiktiven Inselstaats Berylia im Nordatlantik. Das Fachpersonal der Verteidiger wird mit einer Vielzahl von Angriffen herausgefordert und an Grenzen bzw. zum Scheitern gebracht, damit diese aus Fehlern lernen und extreme Situationen und damit auch übliche Angriffe abwehren können. 2500 Cyberangriffe pro Team werden simuliert. Die Anzahl der zu schützenden virtuellen Sys-

teme wurde entsprechend der Teilnehmer:innenzahl angepasst: 2017 waren es noch 3000 Systeme, 2018 schon 4000 und 2021 5000. Die Übung bezieht reguläre Unternehmens-IT, kritische Infrastruktur und militärische Systeme mit ein. Realistische Netzwerke, Systeme und Angriffsmethoden bildeten die technische Umgebung.

Um in *Locked Shields* erfolgreich zu sein, müssen die konkurrierenden Teams sowohl technische als auch soziale Fähigkeiten beherrschen, d. h. sie müssen in der Lage sein, mit Medien- und Rechtsanfragen umzugehen und gleichzeitig Angriffe abzuwehren.

Die Systeme und Aufgaben haben sich über die Jahre gewandelt und an Komplexität gewonnen. Bis 2014 bestand die Übung aus klassischen Client-seitigen Angriffen und aus Angriffen auf die Server via Exploits.

Neue Elemente im Jahr 2015 waren industrielle Steuerungssysteme (ICS/SCADA Systeme) und Windows 8 und 10 Betriebssysteme sowie ein Element von „aktiver Verteidigung“. Des Weiteren war eine Aufgabe, die Kontrolle über ein von Feinden übernommenes unbemanntes Luftfahrzeug (Unmanned Aerial Vehicle, UAV) zurückzuerlangen. Dabei standen die Teams unter Zeitdruck, da das bespielte Szenario lautete, dass die Drohne über einer Stadt kreise und nach drei Stunden aufgrund von Treibstoffmangel abstürzen werde. Zusätzlich zu technischen und forensischen Herausforderungen wurden Medien und rechtliche Fragestellungen erstmals Bestandteil der Übung.

Im Jahr 2017 hatten die blauen Teams die Aufgabe, die Dienste und Netze eines Luftwaffenstützpunkts des fiktiven Landes aufrechtzuerhalten, der dem Übungsszenario zufolge schweren Angriffen ausgesetzt war. Neben den Angriffen auf militärische Kommando- und Kontrollsysteme und andere operative Infrastrukturen waren Angriffe auf die Kontrollsysteme für ein von Siemens simuliertes Stromnetz sowie simulierte UAVs Teil der Übung. Die Übung ermöglichte den Umgang mit der simulierten Situation, in der ein unbekanntes Flugzeug über das Land fliegt. Die Flugdaten waren gefälscht bzw. simuliert und wurden vom roten Team in das System eingespeist.

Des Weiteren war die Übung in dem Jahr zum ersten Mal eine Multi-Layer Exercise. Während IT-Expert:innen die Verteidigung von Computernetzwerken und die Bewältigung rechtlicher und forensischer Herausforderungen trainierten, übten politische Entscheidungsträger ihre Entscheidungsverfahren. Insbesondere ging es darum, wie ein einzelner Staat auf einen Cyberangriff reagieren sollte und wie man Entscheidungen aus rechtlicher und diplomatischer Sicht treffen kann.

2018 wurde die Situation um die Verteidigung eines 4G-Mobilfunknetzes für die öffentliche Sicherheit sowie einer SPS-gesteuerten Wasseraufbereitungsanlage erweitert. 2019 waren neben diesen beiden auch maritime Überwachungssensoren Teil der Übung.

2021 enthielt die Übung neben neuen Systemen (Stromnetze, Satellitensteuerung, Luftverteidigung, Wasseraufbereitung, mobile und militärische Kommunikationsnetzwerke) auch mehrere neue Herausforderungen für den Bereich der strategischen

Entscheidungsfindung. Auch der Finanzdienstleistungssektor wurde als Angriffsfläche für feindliche Angriffe hervorgehoben. Die Übung untersuchte, wie neu entstehende Technologien, wie z. B. Deepfakes, zukünftige Konflikte beeinflussen werden.

## Crossed Swords

Seit 2014 findet jährlich in Riga die Übung *Crossed Swords*<sup>6</sup> statt. Diese technische und praxisnahe Übung dauert drei Tage und legt den Fokus auf das Training von Penetrations-Tester:innen und Expert:innen für digitale Forensik. Diese sollen lernen, besser mit verschiedenen Angriffsvektoren umzugehen, und offensive Fähigkeiten trainieren. Seit 2017 richtet sich das Training ebenfalls an Spezialkräfte und es wurden kinetische Elemente eingebettet. Nach und nach hat sich *Crossed Swords* von einem rein technischen Red-Teaming-Workshop zu einem Manöver entwickelt, bei dem verschiedene technische Fähigkeiten mit kinetischer Gewalt kombiniert werden. 2018 wurde die Übung in Umfang und Komplexität erheblich ausgeweitet und erstreckte sich über mehrere geografische Gebiete, wobei Anbieter kritischer Informationsinfrastrukturen einbezogen wurden.

Das Manöver wird seit 2016 ebenfalls vom CCDCOE organisiert. Im Gegensatz zu den anderen zwei Übungen findet *Crossed Swords* in Präsenz statt und ist wesentlich kleiner als die beiden anderen Manöver. Allerdings ist auch dieses über die Jahre gewachsen, und immer mehr NATO-Staaten nahmen daran teil: 2018 waren es ca. 80 Partizipierende aus 15, 2019 ca. 100 Partizipierende aus 21 und 2020 ca. 120 Partizipierende aus 26 Staaten.

Ziel der Übung ist das Erlernen von Fähigkeiten, IT-Systeme zu infiltrieren (client side targeting, web based attacks, malware and system exploitation, network and service based attacks). Neben klassischen Computer-Netzwerk-Operationen behandeln die Übungen auch Untersuchung und Angriffe auf Systeme, die oft für Automatisierung und industrielle Steuerung genutzt werden.

Zu den Übungszielen gehört aber auch die erfolgreiche Durchführung von verdeckten Angriffen und Ablenkung (deceptions) sowie die Zusammenarbeit, die es den Teilnehmer:innen ermöglicht, bereichsübergreifende Synergien zu nutzen und informationstechnische Angriffe in militärische Taktiken zu integrieren, um informationstechnische mit kinetischen Angriffen zu kombinieren. Dabei liegt der Fokus allerdings nach wie vor auf der technischen Ebene. Seit 2020 beinhaltet die Übung auch ein Führungsmodul.

Des Weiteren trainiert *Crossed Swords* die digitale Forensik (die Sammlung und Auswertung von Informationen). Die Analyse von Informationen dient auch der technischen Zuordnung (Attribution) sowie der Identifizierung bösartiger Aktivitäten. Auch was gemeinhin als *Hack-back* bekannt ist, also das Aufspüren und Infiltrieren von Systemen, von denen ein Angriff ausgeht, wird ebenfalls geübt (responsive cyber defense and adversarial information system infiltration).

Zur Verfügung stehen 200 virtuelle und physikalische IT-Systeme. Anzugreifende Ziele (siehe Kasten, siehe Blumbergs-Ottis-Vaarandi (2019), Fn 6) waren das Steuerungssystem einer

Bunkertür, ein Alarmsystem, IP-Kameras, Steuerungssysteme eines Stromnetzes, unbemannte Luft-, Wasser- und Bodenfahrzeuge, eine Eisenbahnkontrollstation, das Steuerungs- und Verfolgungssystem eines Schiffes sowie ein militärisches Funkkommunikationsnetz und die Basisstationen eines zivilen Mobilfunknetzes.

2018 wurden beispielsweise Mobilfunktechnologien zur Identifizierung einer Zielperson, Drohnenüberwachung und 5G-Sensoren zur Erfassung seines Standorts und zum Sammeln weiterer Informationen eingesetzt. 2019 wurden mehrere kinetische und Cyber-Operationen gleichzeitig durchgeführt, darunter Angriffe auf industrielle Kontrollsysteme, physische Sicherheitssysteme, UAVs und maritime Überwachungssysteme. Ein neues Element waren die unbemannten Bodenfahrzeuge (UGV), die informativ-angegriffen werden sollten.

#### Anzugreifende Ziele bei Crossed Swords bis 2019:

**Bunkertür:** Steuersystem, das eine Reihe von miteinander verbundenen, von Siemens entwickelten S7-1200 basierten PROFINET IO-Geräten verwendet. Das rote Team muss das Kommunikationsprotokoll rekonstruieren, um die Befehle zur Steuerung der Bunkertür über das Netzwerk einzugeben.

**Alarmsystem:** Geschützte Räumlichkeiten durch das Paradox-Alarmsystem, das durch Analyse des verwendeten Busprotokolls und Erfassung und Dekodierung des PIN-Codes über das Netzwerk angesprochen werden muss.

**CCTV-IP-Kamera:** Das rote Team muss die Schwachstellen in der Webschnittstelle der IP-basierten Überwachungskamera finden und ausnutzen, um die vollständige Kontrolle über das Netzwerk zu erlangen.

**Verteiltes Stromnetz:** Die industrielle Ethernet-Protokollserie IEC-60870-5-104 und eine von Martem hergestellten Remote-Terminal-Unit wird zur Verwaltung und Überwachung des Stromnetzes verwendet. Das rote Team muss das Protokoll rekonstruieren und Befehle über das Netzwerk injizieren, um die Energieversorgung zu steuern.

**Unbemanntes Luftfahrzeug (UAV):** Die von Threod hergestellten UAVs, die das geschützte Gebiet überfliegen, müssen ins Visier genommen werden, um die Kontrolle über sie zu erlangen.

**Unbemanntes Bodenfahrzeug (UGV):** Die von Milrem entwickelten UGVs dienen als vom Gegner kontrollierte Panzertruppe und das rote Team hat die Aufgabe, die vollständige Kontrolle über sie zu übernehmen, indem entweder die verwendeten Netzwerkprotokolle oder die steuernde Workstation angegriffen werden.

**Maritime Navigation:** Das Steuerungs- und Verfolgungssystem eines Schiffes, das auf dem maritimen AIS-Protokoll (Automatic Identification System) basiert, wird vom roten Team angegriffen, um die Kontrolle über das Schiff zu erlangen und gefälschte Marine-Tracks zu injizieren.

**Funkkommunikationsnetz:** Das Harris-basierte militärische Datennetz muss vom roten Team durch Extraktion der Verschlüsselungsschlüssel infiltriert werden.

**Basisstationen des Mobilfunknetzes:** Das rote Team muss die vom Betreiber LMT (Latvian Mobile Telephone) bereitgestellten Basisstationen, die mit dem tatsächlichen Mobilfunknetz verbunden sind, infiltrieren und die abgefangene Kommunikation analysieren, um den Nachrichtenaustausch (SMS) eines gegnerischen Agenten zu entschlüsseln und seinen physischen Standort zu bestimmen, damit Spezialkräfte zugreifen können.

**Eisenbahnkontrollstation:** Ein System, das auf einer von Siemens entwickelten S7-1200 SPS mit s7comm+ Protokoll basiert, steuert das simulierte Eisenbahnnetz. Das rote Team hat die Aufgabe, die Kontrolle über die Eisenbahnkontrollstationen zu erlangen, um den Zug zu stoppen oder entgleisen zu lassen.

#### Fazit

Das Ausspähen und Nutzen von Sicherheitslücken im Vorfeld und bei geheimdienstlichen Operationen und militärischen Auseinandersetzungen ist längst Alltag. Durch das Bekanntwerden der Operation Olympic Games (gemeinhin als Stuxnet bekannt) ist auch seit 2010 eine neue Qualität von geheimdienstlich-militärischen Cyberangriffen bekannt. In diversen Manövern trainieren Armeen (und Geheimdienste) den Cyberkrieg. Insgesamt wird deutlich, dass Cyber-Operationen in großem Maßstab vorbereitet und seit 2008 systematisch im Manöver geübt werden. Da informationstechnische Angriffe in der Regel wesentlich kostengünstiger sind als konventionelle Angriffe und ihre Attribution äußerst schwierig ist, ist die Schwelle niedrig, diese Angriffe durchzuführen. Entsprechend sind diese Manöver Brandbeschleuniger für aktuelle und bevorstehende Konflikte. Eine internationale Ächtung dieser Angriffe ist dringend notwendig, erscheint aber aktuell unwahrscheinlich.

#### Anmerkungen

- 1 *United Nations Institute for Disarmament Research (UNIDIR) (2013): The Cyber Index – International Security Trends and Realities. Genf.*
- 2 *Selbstdarstellung des Manövers Cyber Coalition siehe <https://www.act.nato.int/cyber-coalition>*
- 3 *Das Allied Command Transformation (ACT) ist neben dem Allied Command Operations eines der beiden strategischen Hauptquartiere der NATO. Es ist zuständig für die Analyse von Herausforderungen und Chancen, die sich aus der Innovation und der Aufrechterhaltung eines technologischen Vorsprungs im Kampf ergeben, sowie die Entwicklung von Verfahren und Technologien, welche der NATO-Kriegsführung nutzen, durch ein großes Netz aus Industrie, Hochschulen, militärischen und zivilen Stellen in den NATO-Staaten, in NATO-Agenturen und NATO-Exzellenzzentren.*
- 4 *Das NATO Cooperative Cyber Defence Centre of Excellence (CCD-COE) ist eines von 21 akkreditierten Centre of Excellence der NATO mit Sitz in Tallinn in Estland. Das Zentrum wurde 2008 gegründet und als internationale militärische Organisation akkreditiert. Es ist eine Wissensdrehscheibe, Denkfabrik und Ausbildungseinrichtung. Kernaufgaben sind interdisziplinäre angewandte Forschung und Entwicklung*

sowie Beratungen, Schulungen und Übungen im Bereich der Cybersicherheit. Zur Rolle der NATO-Exzellenzzentren siehe u. a.: Christopher Schwitanski: Nato-Exzellenzzentren – Planen für den nächsten Krieg, IMI-Studie 2016/06.

- 5 Selbstdarstellung des Manövers Locked Shields siehe <https://ccdcoe.org/exercises/locked-shields/>. Weitere Informationen sind den jährlichen Stellungnahmen des CCDCOE sowie den After Action Reports

(<https://ccdcoe.org/library/publications>) zu finden.

- 6 Selbstdarstellung des Manövers Crossed Swords siehe <https://ccdcoe.org/exercises/crossed-swords/>. Details siehe Blumbers-Ottis-Vaarandi (2019): Crossed Swords: A Cyber Team Red Oriented Technical Exercise. Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019: University of Coimbra, Portugal, 4-5 July 2019.



Sebastian Jekutsch

## Betrifft: Faire Computer

Fair wie in Fairer Honig

Beginnen wir am besten mit dem Koalitionsvertrag der Bundesampel. Bezüglich der sozial-ökologischen Transformation ist auffallend die EU im Blick: EU-Handelsabkommen sollen verbindliche Klauseln enthalten, die Menschenrechte, soziale und ökologische Standards schützen. Ein *effektives* Lieferkettengesetz soll auf EU-Ebene vorangetrieben werden, bei unveränderter Umsetzung und ggf. Verbesserung der deutschen Variante. EU-Vorschläge zum Importverbot von Produkten aus Zwangsarbeit sollen unterstützt werden.

Und mindestens beim letzten Punkt sind wir auch bei der Elektronik angekommen. China ist in den Medien, im Jahr des Tigers, mit Olympia, Schulterschluss mit Putin und eben der Zwangsarbeit der muslimischen Uiguren in der Westprovinz Xinjiang. Intel hatte seine Zulieferer Anfang Dezember dazu aufgerufen, sich aus der Provinz zurückzuziehen. Das deutsche Lieferkettengesetz sieht für Unternehmen eine Pflicht zur Risikoanalyse vor, nicht nur sowieso bei direkten Auftragnehmern, sondern auch tiefer in der Lieferkette, wenn es *substanzielle* Hinweise auf Menschenrechtsverletzungen gibt. Die liegen hier offensichtlich vor. Und China ist in Sachen IT und Elektronik überall in der Lieferkette, vom Zusammenschrauben bis zu den Rohstoffen. Etwas dumm für das zentrale Anliegen der Energiewende vielleicht, dass ausgerechnet für Solarzellen nun konkrete Hinweise von Zwangsarbeit im Westen Chinas vorliegen.

Diese werden aus Quarzsand gefertigt, bislang nicht gerade als einer jener Transitionsrohstoffe im Gespräch. Es gibt ihn sprichwörtlich wie Sand am Meer, ganz anders als beim Lithium in den Akkus der vielen noch kommenden E-Autos und sowieso auch unserer mobilen IT: Das baut man zum einen oft im Meer ab, es kommt in Salzseen angereichert vor. Zum anderen ist es knapp und wird immer teurer. Bolivien versucht seit Jahren daraus Gewinn zu schlagen, wird aber nicht produktionsreif, wie jüngst resümiert wurde. Sie wollen es bis zur Batterie alleine hinkommen, also ohne Ausbeutung durch etablierte Rohstoffindustrie, was eine wichtige Voraussetzung für die nationale Entwicklung ist. Die Multis orientieren sich daher lieber gen Argentinien. Die



Regierung ist da offener für fremdes Know-how, Kapital und Knebelverträge, ja, wenn nicht die indigene Bevölkerung sich dem entgegenstellen würde, um ihre Wasserversorgung zu retten. In Serbien jedenfalls hat Rio Tinto im Januar aufgrund lokaler Proteste aufgegeben, Lithium zu fördern. Ein anderer Transitionsrohstoff, ebenfalls für die Batterien, ist Kobalt aus dem Kongo mittels Kinderarbeit, ein lange bekannter Zusammenhang, was die IT-Hersteller nur zögerlich akzeptierten. Eine Klage indes gegen u. a. Apple und Microsoft in dieser Sache ist im November abgewiesen worden: Man könne ob der Komplexität der Handelsbeziehungen keinen einzelnen Verantwortlichen konkret benennen.

Und was machen die Pionierprojekte? Fairphone hatte im Herbst überraschend früh die Version 4 ihres Smartphones veröffentlicht, das im Dezember nun die TCO-Zertifizierung erhalten hat und im Januar die vom Blauen Engel. Enttäuschend ist vielleicht, dass sie sich aus optischen Gründen gegen Recycling-Alu im Gehäuse entschieden haben, immerhin nun aber auf der Suche nach fairem Aluminium sind. Neu aus Fairnessicht ist der Ausbau des Unterstützungsprogramms in Ruanda für den Abbau von Wolfram für den Vibrationsalarm, und das Fairtrade-Gold, das schon die Leiterplatten enthalten, ist nun auch in den Bauteilen des Herstellers Hirose, wie im Dezember verraten wurde. Vermutlich in Steckkontakten, leider wird das nicht verraten. Das Tragische an der vorbildlichen Modularität des Fairphones ist, dass sie mehr Steckkontakte benötigt, in denen typischerweise Gold ist, was sich negativ auf die Sozial- und Ökobilanz auswirkt. Nun ist es immerhin fair. Fairer jedenfalls als das immerhin konfliktfreie Zinn, über das eine sehr lesenswerte Artikelserie beim Onlinemagazin *Das Lamm* erschien, mit deutlich geäußerten Zweifeln an der sozialen Wirksamkeit dieser Maßnahme. Auch sonst wird dort nicht an Zweifeln gespart: Viele Angestellte seien enttäuscht gegangen, weil der neue Geldgeber nur auf die Zahlen schaue.

Sebastian Jekutsch

Sebastian Jekutsch ist Sprecher der AG Faire Computer des Fiff. Wer sich für die Quellen oder das Thema überhaupt interessiert, kann gerne Kontakt aufnehmen per [sebastian.jekutsch@fiff.de](mailto:sebastian.jekutsch@fiff.de).

So erklärt es sich vielleicht, dass Fairphone auch nie für so etwas wie ein Lieferkettengesetz gekämpft hat, es könnte ja ihr Alleinstellungsmerkmal gefährden. Andere lobbyieren auf EU-Ebene direkt dagegen, wie Misereor im Februar zusammenstellte. Gibt es einen Zusammenhang mit der im Dezember schon dritten Verschiebung der Veröffentlichung eines ersten Entwurfs durch die Kommission? Das war auch in Deutschland so, überhaupt ähnelt sich einiges. So gibt es auch hier eine Gruppe von Firmen, die sich ebenfalls im Februar in einem öffentlichen Brief

klar für eine solche Regulierung aussprechen. Fairphone ist wie gesagt nicht dabei, aber z. B. Shift, die so genannte Alternative aus Deutschland. Als einziger Groß-IT-Produzent hat Epson unterschrieben. Es ist vielleicht ein Versuch sich abzusetzen von Billigprodukten. So hat China Labor Watch im November bei zwei Herstellern für nachgemachte Tonerkartuschen für Drucker u. a. von Epson Arbeitsrechtsverletzungen und gefährliche Arbeitsbedingungen aufgedeckt. Wo? In China. Es hängt alles zusammen.



## Call for Contributions

# Schwerpunkt *Digitalisierung in Staat, Politik & Verwaltung* der FfF-Kommunikation 3/2022

Redaktion: Jörg Pohle & Stefan Hügel

Seit mehr als sechzig Jahren folgt in der (bundes-)deutschen Politik und Verwaltung eine Welle der Computerisierung, Informatisierung und Digitalisierung auf die andere. Die Corona-Pandemie und der Umgang damit haben gezeigt, wie vieles dabei noch im Argen liegt – trotz aller Erfolgsmeldungen aus der Vergangenheit. Zugleich waren sie aber auch Auslöser einer neuen Digitalisierungswelle. Wird jetzt endlich alles gut? Oder ist auch „4.0“ nur einfach „mehr vom Alten“?

Im Heftschwerpunkt *Digitalisierung in Staat, Politik & Verwaltung* der FfF-Kommunikation 3/2022 wollen wir einen Blick auf das breite Feld staatlicher Informationssysteme werfen, vor allem, aber durchaus nicht nur, in Deutschland. Es geht um eingesetzte und geplante, aber auch um längst überholte und bereits wieder abgeschaffte Systeme in Kommunen, Ländern und im Bund. Es geht um mit diesen Systemen erbrachte staatliche Leistungen, etwa der Verwaltung, um Meinungsbildung, Demokratie und politische Entscheidungsfindung, um die Organisation solcher Systeme und ihren praktischen Einsatz, um Transparenz und Rechtsstaatlichkeit staatlichen Handelns, aber auch die Auswirkungen dieser Systeme auf Individuen, Gruppen und die Gesellschaft insgesamt. Es geht aber auch um die Prozesse der Digitalisierung, wie sie ablaufen und ablaufen sollten, um Fragen der Mitbestimmung und Intervention, um Erfolge und um Scheitern.

Wir freuen uns über Arbeiten, die in alle Richtungen schauen: in die Vergangenheit, die Gegenwart und die Zukunft, auf die Sonnen- und die Schattenseiten, auf die Theorie und die Praxis, auf die Versprechungen und ihre Umsetzungen in Parlamenten und Amtsstuben, auf Gestaltungs-, Verwendungs- und Wirkungszusammenhänge. Wir freuen uns über Praxisberichte ebenso wie über politische Forderungen an die Digitalisierung und deren Begründung, über lokale Erfahrungen ebenso wie über nationale oder supranationale Entwicklungen, über informatische Perspektiven ebenso wie über die anderer Disziplinen, über Analysen ebenso wie über Gestaltungsoptionen, über Fragen ebenso wie über mögliche Antworten.

Die möglichen Themen sind so breit gefächert wie der Einsatz staatlicher Informationssysteme und die Möglichkeiten von Bürger:innen, mit solchen Systemen in Kontakt zu kommen

oder konfrontiert zu werden. Aus Sicht von Bürger:innen stellt sich etwa die Frage, ob und wie der Einsatz technischer Systeme als Schnittstelle der Verwaltung nach außen das Verhältnis zwischen Bürger:innen und Staat, deren Interaktion und Kommunikation, aber auch deren jeweiliges Selbstverständnis ändert. Aus der Sicht der Informatik würde sich daran anschließen, welche Gestaltungsforderungen an diese Schnittstellen sich daraus ergeben. Der Blick ins Innere von Politik und Verwaltung wirft hingegen unter anderem die Frage auf, wie mit der zunehmenden „Verdatung“ (Herbert Fiedler 1975) aller Lebensbereiche Prozesse und Ergebnisse von Planungen und Entscheidungen in diesen Bereichen geändert werden oder werden sollten. Auch hier gibt es informatische Anschlussfragen, etwa zur Gestaltbarkeit und Gestaltung von Systemen, die Transparenz und Interventionsmöglichkeiten ermöglichen oder erzwingen. Und auf der Ebene von Staat und Gesellschaft kann etwa gefragt werden, wie sich Gewaltenteilung und Dezentralität unter der Bedingung durchgreifender Digitalisierung aufrecht erhalten oder gar stärken lassen.

Wir freuen uns über Einreichungen von Beiträgen mit ca. 20.000 Zeichen (inklusive Leerzeichen) bis zum 8. Juli 2022 per E-Mail an Jörg Pohle ([joerg.pohle@fiff.de](mailto:joerg.pohle@fiff.de)) und Stefan Hügel ([sh@fiff.de](mailto:sh@fiff.de)). Alle Beiträge zum Schwerpunkt werden peer-reviewed, und die Autor:innen erhalten bis zum 22. Juli Rückmeldungen zu ihren Beiträgen. Die finalen Fassungen der Beiträge sind bis zum 5. August einzureichen.

Wir freuen uns über die Nutzung der Open-Access-Lizenz *Creative Commons – Namensnennung / CC BY* für Ihren Text und die verwendeten Bilder.

## Termine

Einreichungsfrist:	8. Juli 2022
Rückmeldung vom Review:	22. Juli 2022
Redaktionsschluss /	
Einreichung der finalen Fassung:	5. August 2022

## Hinweise für Autor:innen

vorläufig: <https://pads.fiff.de/p/klausurOkt2021-G3Leitfaden>

## Kein Krieg in Europa und anderswo!

### Das FfF verurteilt den russischen Angriffskrieg gegen die Ukraine

Pressemitteilung vom 28. Februar 2022 – *Was noch vor einigen Jahren wenig wahrscheinlich schien, ist wieder Wirklichkeit geworden: In Europa herrscht offener Krieg zwischen Nationen. Die russische Aggression in der Ukraine bricht das Völkerrecht und ist durch nichts zu rechtfertigen. Erstes Opfer ist die ukrainische Bevölkerung – doch auch die europäische Friedensordnung wird dadurch angegriffen. Das friedliche Europa stellt sich nun als Illusion heraus. Wer die Aggression zum Mittel der Politik macht, verabschiedet sich damit aus dem Kreis der zivilisierten Gesellschaft.*

*Wir verurteilen den völkerrechtswidrigen Angriff und fordern die sofortige Einstellung aller Kampfhandlungen und den Rückzug der russischen Truppen. Der Krieg muss sofort beendet werden. Wir fordern die Kriegsparteien dazu auf, umgehend eine diplomatische Lösung des Konflikts auf Grundlage der UN-Charta anzustreben.*

Die Eskalation zeigt aber auch, dass die NATO strategisch versagt und Präsident Putin geostrategisch falsch eingeschätzt hat. Dies darf jedoch keinen neuen Rüstungswettlauf bedeuten, sondern wir brauchen eine neue Sicherheitsarchitektur in Europa. Bei einer anzustrebenden langfristigen friedlichen Lösung des Konflikts müssen die Sicherheitsinteressen aller Beteiligten berücksichtigt werden, also die Interessen der EU, aber auch die Interessen der Ukraine und die Russlands.

#### **Ende der Aggression in der Ukraine. Ende aller Militäroperationen. Rückzug der russischen Truppen.**

Das FfF fordert Präsident Putin und die Russische Föderation auf, die Aggression in der Ukraine sofort zu beenden. Wir fordern die russischen Truppen auf, alle laufenden Operationen sofort abzubrechen, sich hinter die ukrainisch-russische Grenze zurückzuziehen, die territoriale Integrität der souveränen Ukraine – inklusive der Krim – wieder herzustellen und an den Verhandlungstisch zurückzukehren.

#### **Hilfe für die Kriegsopfer. Aufnahme von Flüchtlingen aus Krisengebieten. Humanitäre Hilfe.**

Im Vordergrund unserer Gedanken müssen die Opfer der Aggression stehen: die ukrainische Bevölkerung. Sie leidet am meisten unter dem Konflikt. Wir stehen solidarisch an ihrer Seite und fordern die Regierungen Europas auf, schnell und unbürokratisch Hilfe zu leisten. Auch stehen wir an der Seite derer, die in Russland Widerstand gegen den Krieg leisten. Die Grenzen Europas dürfen für Flüchtlinge nicht geschlossen werden. Jede Abschottungspolitik spielt den Aggressoren in die Karten und zeigt, wie wenig Europa sich selbst an die UN-Charta und Menschenrechte hält.

#### **Kein weiteres Anheizen des militärischen Konflikts. Keine Waffenlieferungen in Krisengebiete.**

Durch Waffenlieferungen wird die Ukraine unterstützt, sich gegen den Aggressor zu verteidigen. Doch Waffenlieferungen sind ein ambivalentes Mittel: Sie heizen die Krise weiter an, der Nutzen für die Ukraine ist fragwürdig und sie bringen noch mehr Tod und Zerstörung. Sie ändern wenig daran, dass die Russische

Föderation in dem Konflikt militärisch weit überlegen ist, bis hin zu Atomwaffen.

#### **Entschlossenes Handeln der Europäischen Union. Wirtschaftliche und diplomatische Sanktionen. Isolation der Aggressoren in der russischen Regierung.**

Die Europäische Union und vor allem Deutschland haben sich durch eine verfehlte Energiepolitik in eine verhängnisvolle Abhängigkeit von Russland begeben. Deutschland bezieht bisher ca. 50 % seines Bedarfs an Gas aus Russland. Die Abhängigkeit von den fossilen Energieträgern Öl und Gas muss reduziert werden.

Doch auch die Finanzierung des Kriegs muss unterbunden werden. Solange die Aggression andauert, muss Russland von den Internationalen Finanzströmen abgekoppelt werden. Das schließt den Ausschluss aus dem internationalen Zahlungssystem SWIFT ein. Zudem muss auch das gesamte Umfeld der russischen Regierung – die Milliardäre der russischen Oligarchie – schleunigst sanktioniert werden, bevor alle Gelder in die Schweiz oder anderswohin transferiert werden.

#### **Informations- und Cyberkrieg beenden.**

„Das erste Opfer des Krieges ist die Wahrheit.“ Der Krieg wurde durch einen Informationskrieg in den Medien vorbereitet, mit Falschinformationen und Manipulation der Bevölkerung. Cyberangriffe und IT-Sabotage werden gegen die ukrainische Regierung unternommen. Doch auch westliche Medien rüsten zum Informationskrieg. Stakkatoartige Kriegsberichterstattung ohne Hintergrundeinordnung in den europäischen Leitmedien heizt den Konflikt weiter an. Auch damit muss Schluss sein.

#### **Keine neue Militarisierung. Sozial-ökologische Herausforderungen in den Vordergrund.**

Die Aggression trifft Europa zu einem Zeitpunkt, an dem große Herausforderungen auf uns warten. Die Pandemie hat die gesellschaftlichen Ungerechtigkeiten aufgezeigt, die von interessierten Gruppen vorangetrieben wird. Die Auswirkungen der

Klimakrise zeigen sich immer deutlicher und werden zur Katastrophe. Die soziale Ungleichheit verschärft sich. Auch eine frühzeitige Umstellung auf erneuerbare Energien hätte die Abhängigkeit von Russland minimiert, die nun offenbar härteren Sanktionen im Wege steht.

Der Angriff auf die Ukraine darf nicht der Beginn einer neuen Militarisierungswelle in Europa werden. Auch die enttäuschende, nun diskutierte milliardenschwere Aufstockung der Deutschen Bundeswehr muss – da sie nun politisch gewünscht ist, obwohl das Geld anderswo seit Jahren fehlt – auf jeden Fall defensiv ausgelegt werden, bewaffnete Drohnen etwa zählen nicht dazu.

## Putins Krieg

Dies ist nicht der Krieg der russischen Bevölkerung, es ist Präsident Putins Krieg. In vielen Städten Russlands finden Demonstrationen statt, die in Russland medial zensiert, technisch durch diktatorische Internetfilter erschwert und vor Ort teilweise gewaltsam unterbunden werden. Wir dürfen nicht mehr zulassen, dass einzelne Autokraten ungehindert auf Kosten der Bevölkerung ihre militärischen Interessen verfolgen. Das 20. Jahrhundert ist vorbei.



## Wissenschaft & Frieden 1/2022

### Täter:innen

Im Februar 2020 überfällt ein rechtsradikaler Täter mehrere Cafés, Kioske und Bars und tötet mindestens neun Menschen aus rassistischen Motiven. Auch 2021 kommt es in mehreren Städten Deutschlands inmitten einer laufenden Debatte zu rassistischer und exzessiver Polizeigewalt zu tödlicher Gewalt gegen Menschen in Polizeigewahrsam. Die Zahl gemeldeter Fälle häuslicher Gewalt schießt im Verlauf der Lockdowns während der Covid-19-Pandemie abrupt in die Höhe.

All diese Fälle werfen Fragen nach den Täter:innen der Gewalt auf. Wer sind sie? Wen verstehen „wir“ als Täter:innen und weshalb? Wie können wir Taten erkennen, verstehen und bearbeiten und wen gilt es zur Rechenschaft zu ziehen? Sind Täter:innen intentional handelnde Akteure oder Opfer der Umstände?

Wissenschaft & Frieden hat daher eine Reihe von Autor:innen gebeten, ihre Forschungserkenntnisse mit uns zu teilen und uns zu zeigen, wie komplex es ist, Täter:innen und Täter:innenschaft zu verstehen. Ihre Beiträge können dabei helfen, Taten auch gesellschaftlich besser aufzuarbeiten und ihnen dadurch in der Zukunft präventiv zu begegnen.

Mit Beiträgen von Christian Gerlach, Sylvia Karl, Gisela Notz, Eva Willems und weiteren.

W&F 1/2022 | Februar | 60 Seiten | 12€ (print) / 9€ (epub) | [wissenschaft-und-frieden.de](http://wissenschaft-und-frieden.de)

### Dossier 94: Frauen, Friedensforschung, Feminismus

Aus der heutigen Friedens- und Konfliktforschung sind gendersensible und feministische Ansätze kaum noch wegzudenken. Das ist auch den Bemühungen jener Frauen zu verdanken, die sich seit 1990 innerhalb der Arbeitsgemeinschaft für Friedens- und Konfliktforschung (AFK) im Netzwerk Friedensforscherinnen organisieren.

Dieses Dossier ist Dokumentation und Würdigung der Geschichte, Entwicklung und Wirkung dieses spezifischen Netzwerks einerseits und ein Werkzeug für die Übertragbarkeit dieser Erfahrungen auf weitere Kontexte andererseits. Das Netz-

werk Friedensforscherinnen in der AFK ist ein Beispiel von vielen, an denen sich Entwicklungen und Debatten zu Frauensolidarität und Feminismus nachzeichnen lassen.

Christine Buchwald und Michaela Zöhrer legen mit dem vorliegenden Dossier in (selbst-)kritischer Reflexion den Auftakt zur Geschichtsschreibung des Netzwerks Friedensforscherinnen.

Dossier 94 | 20 Seiten | 2€ zzgl. Versand | [wissenschaft-und-frieden.de](http://wissenschaft-und-frieden.de)



## Das Verschwinden des Computers

*Mir ist etwas über die westliche Zivilisation und Kultur eingefallen. Gandhi wurde in Indien aus dem Gefängnis geholt, um in England etwas mitzumachen, und als er in Southampton ankam, wurde er von Reportern interviewt. Einer fragte ihn: „Mr. Gandhi, what do you think of western civilisation?“ Er hat einen Moment nachgedacht und antwortete: „I think, it would be a good idea.“ Ich glaube, das ist immer noch so.*



Joseph Weizenbaum (8. Januar 1923 – 5. März 2008),  
Quelle: Pressematerial zum Film *Plug & Pray*,  
[www.farbfilm-verleih.de/filme/plug-and-pray/](http://www.farbfilm-verleih.de/filme/plug-and-pray/)

Ich bin sozusagen ein Computermensch. Ich habe mein ganzes Leben lang, weit über 50 Jahre, mit Computern gearbeitet. Vor 25 Jahren habe ich ein Buch geschrieben *Die Macht der Computer und die Ohnmacht der Vernunft*. Es ist erstaunlicherweise immer noch auf dem Markt und wie man mir sagte, immer noch aktuell. Unter anderem sicher, weil es nicht über einen speziellen Computer spricht, sondern über die Idee *Computer*.

Es ist sehr viel passiert in den letzten 25 Jahren. Die Computer sind schneller, billiger, leichter geworden. Ja, da könnte man sich fragen, wie passiert das überhaupt. Ich habe mal – auch vor langer Zeit – ein Papier geschrieben über den Einfluss der Computer auf die Gesellschaft. Kurz danach fiel mir ein, der Titel ist falsch, es sollte heißen der Einfluss der Gesellschaft auf den Computer und nicht umgekehrt, denn dass der Computer kleiner, schneller und leichter geworden ist, war nicht die Folge irgendeines natürlichen Gesetzes. Nein. Ich erinnere mich: In einem technischen Museum in Berlin sieht man eine Rakete, die sagen wir einen Meter lang ist. Das Ding sieht aus wie eine Rakete und vorn ist Glas, da ist eine Fernsehkamera drin. Dann wird in diesem Museum erklärt, diese Fernsehkamera wurde während des Zweiten Weltkrieges von den Deutschen entwickelt und die Idee war, man schießt diese Rakete ab und das Fernsehen zeigt, wo sie ist und hinten sitzen Leute, die sie steuern können und da kann man das Ziel sehr genau erreichen. Aber das Ding wurde nie verwendet, unter anderem weil es überhaupt keinen Platz für den Sprengstoff gab, nachdem die ganze Elektronik drin war. Und dem Feind Fernsehkameras zu liefern, das war nicht die Idee. Da sieht man – wir sprechen von 1944 – etwas von der Entwicklung des Computers. Das Militär musste den Computer und die ganze Elektronik, die damit zusammenhängt, sehr viel kleiner, sehr viel leichter haben, es muss fliegen können, schneller sein. Ob billiger oder nicht, das ist eine andere Sache. Es hat etwas zu tun mit der Gestaltung unserer Gesellschaft. Die amerikanische Gesellschaft ist leider in den letzten 40 Jahren eine hochmilitarisierte Gesellschaft geworden und man kann viele Entwicklungen

sehen und ganz besonders im Computerbereich, die von den Militärs gewollt, man kann auch sagen: bestimmt waren.

Computer wurden schneller, leichter, kleiner und natürlich sehr weit verbreitet, sie finden sich in allen möglichen Sachen, ganz besonders in Waffensystemen. Die sind vielleicht die Konsequenz einer Ideologie, eines sehr alten Wunsches, dass das Militär und die Kriegsführung effizient sein sollen. Und jetzt kommt die Frage: was ist effizient, was bedeutet effizient? Meistens denken wir, dass eine Fabrik effizienter ist als eine andere, wenn es mehr Profit gibt oder wenn es billiger ist, dort etwas herzustellen als irgendwo anders. Das ist Effizienz. Aber tatsächlich hat Effizienz eine viel breitere Bedeutung. Effizienz bedeutet die Optimierung eines Parameters in einem System mit sehr vielen Parametern auf Kosten eines anderen Parameters. Bei einer Automobilfabrik, der es gelingt, 50.000 Arbeiter zu entlassen und trotzdem Automobile herzustellen, steigen die Aktienpreise. Optimiert wird der Einsatz von Geld auf Kosten anderer Parameter, in diesem Fall auf Kosten dieser 50.000 entlassenen Leute. Und wenn man vom effizienteren Militär spricht, dann sehen wir die Idee vom sauberen Krieg. Das war nicht nur im Kosovo so, sondern auch im Golfkrieg. Präsident Bush tauchte im Fernsehen auf und wurde auf den Schultern von Soldaten getragen. Es war ein sehr großer Krieg, und der Präsident ist in das Fernsehen gekommen und hat gesagt: Hier haben wir einen sauberen Krieg, sogar einen menschlichen Krieg geführt. Unsere Waffen, wie wir im Fernsehen gesehen haben, haben ihre Ziele getroffen, natürlich nur militärische Ziele. Nicht solche Bombardements von großen Städten wie im Zweiten Weltkrieg. Also haben wir viel weniger Menschen getötet. Was nicht erwähnt wurde – und wir wissen es immer noch nicht – wie viele vom „Feind“ ermordet worden sind gegenüber den viel weniger Soldaten, die wir verloren haben. Wir sprechen von Hunderttausenden gegen eine Handvoll. Dies haben die Waffen möglich gemacht, die sogenannten *fire-and-forget*-Waffen. Das heißt, zum Beispiel eine Cruise Missile von einem Schiff abzuschießen und ihr dann den Rücken zudrehen, man kann sie vergessen, sie wird das Ziel schon erreichen, man muss sie nicht steuern, sie steuert sich selbst. Das gab es vor 25 Jahren nicht. Wir haben sehr sehr große Fortschritte gemacht und über manche Sachen freut man sich riesig, zum Beispiel darüber, dass von unseren Soldaten nur ein Bruchteil der des Feindes umgekommen sind.

Wenn man über den riesigen Fortschritt der letzten Jahre sprechen will, dann muss man natürlich über die Biologie sprechen und ganz besonders darüber, dass es uns gelungen ist, den *human genome* zu identifizieren. Diese Leistung, die wir gemacht haben – mit mir meine ich die Gesellschaft oder die Menschheit – wäre ohne den Computer unmöglich gewesen. Soviel Rechenarbeit ist da dabei, man könnte es nicht versuchen ohne Computer. So haben wir eine Verbindung zwischen der Biologie und dem Computer und es wird sich herausstellen, dass die

Biologie in einem gewissen Sinn viel größere Nebenwirkungen oder Wirkungen haben wird an unserer Gesellschaft, an uns als Menschen als der Computer. Aber die beiden sind sehr eng verbunden. Zum Beispiel wird an der Vereinigung von Mensch und Computer sehr viel gearbeitet. So ist der Traum, dass zum Beispiel kleine Computerchips ins Gehirn eingestellt werden können. Was sie tun sollen, weiß ich nicht. Aber die Idee, dass das Gehirn selbst ein „Computer“ ist und „verbessert“ werden kann – alles in Anführungsstrichen – diese Idee ist am Leben. Daran wird sehr sehr hart gearbeitet an den besten Universitäten in Amerika und ich nehme an, auch anderswo. Eine andere Folge von der Biologie und unserer Fähigkeit, mithilfe eines Computers sehr komplexe Rechnungen zu vollenden, hat auch Konsequenzen. Die Wissenschaftler in den USA stellen an Geldgeber Anträge, und wenn es sehr viel Geld ist, dann ist es das Militär, an das man den Antrag stellt. Und manchmal geht es auch umgekehrt, dass das Pentagon wissen lässt, dass sie irgendeine technische Entwicklung brauchen und sie wollen Leute finden, die das vollenden. Es scheint möglich zu sein, mit dem Fortschritt in der Biologie, dass wir Menschengruppen bestimmen können mittels ihres Genoms, sagen wir zum Beispiel eine bestimmte Bevölkerung in der Türkei oder in Afrika. Wir hoffen also herauszukriegen, wie die Gene in ihnen funktionieren und hoffen, dass da etwas besonderes ist, denn dann könnte man eine chemische oder eine biologische Waffe entwickeln, die gerade diese Leute angreift, für die aber andere Leute, sagen wir weiße Amerikaner, eine Immunität haben. Das macht natürlich die Kriegsführung noch effizienter und wir sollen uns alle freuen.

Natürlich, man kann heute über Computer gar nicht sprechen, ohne das Internet zu erwähnen. Man sollte ein bisschen nachdenken. Ich benutze das Internet jeden Tag und habe angefangen, den Vorgänger des Internet, das hieß Arpanet, ungefähr 1964 zu benutzen. Also bin ich schon 40 Jahre dabei mit dem Internet und glaube, es zu verstehen. Es wurde hier schon erwähnt, dass viele Leute glauben, dass das Internet das gesamte Wissen der Menschheit enthält. Es gibt den Glauben, dass dann, wenn man etwas nicht mit konventionellen Mitteln herausfindet, man doch immer zum Computer gehen und ihn fragen kann. Natürlich kann man das nicht. Dafür gibt es verschiedene Gründe. Zunächst sind wir sehr weit davon entfernt, dass auch nur das geschriebene Wissen der Menschheit im Internet ist. Ein Beispiel. Ich wollte mal in einem Vortrag etwas sagen über die Schlacht von Passchendaele im Ersten Weltkrieg. Ich wollte etwas darüber sagen und ich frage Sie, was wissen Sie darüber? Es ist erstaunlich. Die Schlacht von Passchendaele hatte etwa die Bedeutung für den Ersten Weltkrieg wie Stalingrad für den zweiten Weltkrieg. Und niemand weiß davon. In dieser furchtbaren Schlacht sind mindestens 250.000 Soldaten umgekommen. Und man muss sagen, der Erste Weltkrieg war eines der wichtigsten Ereignisse in der Geschichte der Menschheit überhaupt. Er hat das 20. Jahrhundert völlig verändert. Man kann fragen, wieviel Geschichte, wie viel Dokumentation usw. des Ersten Weltkrieges man überhaupt im Internet findet, es ist erstaunlich wenig. Ich habe versucht, Passchendaele zu finden und ich habe nichts gefunden. Schließlich ist mir eingefallen, dass ein gewisser englischer General Haig die Idee hatte, so eine Schlacht zu inszenieren. Er hat sie inszeniert, hat einen großen Teil der britischen Jugend ermordet und natürlich auch viele Deutsche und wurde belohnt, indem er Feldmarschall geworden ist. Ich habe General Haig nachgeschaut im Internet, ihn habe ich gefunden und dort ist in fünf Zeilen auch

Passchendaele erwähnt. In gewissem Sinn ist das Internet – ich wiederhole, ich benutze es jeden Tag, ich denke nicht, dass es ein Schrotthaufen ist – ein Zerstörer von Geschichte. Es passiert jetzt schon und es wird weitergehen: was nicht drin ist, existiert nicht. Und ich kann mir vorstellen, dass in 50 Jahren, wenn wir das überhaupt überleben, der Erste Weltkrieg einfach aus dem Bewußtsein der Menschen verschwunden sein wird.

Es ist interessant, dass der Glaube überhaupt existiert, dass das Internet die Hauptquelle für Wissen sein wird, was immer Wissen ist. Heute haben viele Menschen PCs und Laptops zuhause und ich glaube, sie haben herausgefunden, dass das Internet nicht das ist, was sie dachten. Es gibt große Schwierigkeiten und es ist mühsam, etwas herauszufinden. Was vielleicht nicht jedem eingefallen ist: Um etwas zu lernen, muss man die Fähigkeit haben, eine gute Frage zu stellen. Und eine gute Frage ist wie ein gutes Experiment in der Physik, das entworfen werden muss. Ein Experiment in der Physik ist eine Frage, die wir an die Natur stellen. Man muss schon sehr viel wissen, um ein gutes Experiment zu entwickeln. Man muss auch wissen, was die Form der Antwort sein wird. Es könnte eine einfache Zahl sein, „17“ zum Beispiel oder es könnte eine ganz komplexe Architekturzeichnung sein. In jedem Fall muss man wissen, in welcher Form man die Antwort erwartet und was man mit der Antwort machen möchte, wenn man sie hat. Um eine gute Frage zu stellen, muss man sehr viel wissen. Man muss auch die Fähigkeit, gute Fragen zu stellen, gelernt haben. Leider wird die Kunst, in einer Bibliothek zu arbeiten, nicht mehr gelehrt in unseren Schulen. Computer sind sehr teuer. Um sie in der Schule aufzustellen, da muss irgendetwas weggelassen werden. Also wird die Bibliothek geschlossen, die Bibliothekarin wird gefeuert.

Ich möchte etwas sagen zum Computer in der Schule. Ich kenne vernünftige Leute, aber wenn ich sage, in fünf Jahren werden sogar die Politiker erkennen, dass es eine riesige Katastrophe war zu verlangen, die Schulen der „zivilisierten“ Welt zu vernetzen. Und es wird nicht leicht sein, das wieder gut zu machen. Da sagen mir Leute, ja, die Kinder müssen doch erst mal lernen, mit dem Computer umzugehen. Dann frage ich: ja warum? Und auch viele von Ihnen würden sagen, naja, Computer sind überall heute in unserer Gesellschaft und wenn die Kinder zum Jobmarkt kommen, dann werden jene, die nichts vom Computer wissen, einen Nachteil haben gegenüber denen, die schon in der Schule über den Computer gelernt haben. Ich könnte auch fragen, was haben sie gelernt, aber ich lass das. Es ist falsch.

Der Computer wird in den nächsten fünf oder zehn Jahren aus unserem Bewusstsein verschwinden. Wir werden einfach nicht mehr über ihn reden, wir werden nicht über ihn lesen, außer natürlich Fachleute. Und wenn ich sage, dass in zehn Jahren Computer überall sind, in der Kamera, in der Waschmaschine, im Auto und werden einfach vergessen, dann fragen Sie, was hat das mit der Schule zu tun? Schon heute, wenn man behauptet, in jedem Job hat man mit dem Computer zu tun, wenn man zum Flughafen geht und der tippt etwas in seinen Computer, obwohl das nur eine Tastatur und ein Bildschirm ist, der Computer ist ganz woanders, heißt es, siehst du, da ist ein Computer. Oder noch besser, nehmen wir einen Piloten in einem modernen Flugzeug mit zehn oder sechs Computern. Frage: Was muss der Pilot wissen über Computer? Antwort: Nichts. Er muss wissen, wie ein Flugzeug zu fliegen ist auch ohne Computer.

Ich muss Ihnen etwas erzählen, aber es ist ein Geheimnis und sie dürfen es nicht weitererzählen. Heute gibt es Flugzeuge, von denen man sagt, sie sind *fly-by-wire*, das heißt der Pilot hat nicht mehr ein Steuerrad in der Hand, das er hin und her ziehen kann. Sondern da ist auf der linken Seite beim Piloten, auf der rechten Seite beim Ko-Piloten ein Knüppel und den kann er bewegen und das ist das, was das Flugzeug steuert. Das ist natürlich mit einem Computer verbunden und der Computer interpretiert, was der Pilot da macht und der Computer schickt dann Signale zu den Maschinen und Motoren, die dann die Flugflächen ändern, so dass das Flugzeug steigt oder längs dreht oder was auch immer. Das ist *fly-by-wire*. Naja, jetzt kommt das Geheimnis: ich war mal in einem Flugzeug über dem Atlantik, von Europa in die USA und das war ein ganz neues Flugzeug und ich hatte das große Glück, dass der Pilot mich in das Cockpit eingeladen hat und der Pilot hat mir alles das gezeigt, was da neu ist. Unter anderem sieht man die üblichen Instrumente überhaupt nicht mehr. Da sind Bildschirme, vielleicht acht oder zehn und da kann man umschalten, man kann die hydraulische Pumpe sehen, wenn man will, man kann da einzoomen und natürlich wird das ganze Flugzeug gesteuert mit dem Computer.

Also, der Pilot zeigt und erklärt mir alles, es ist das schönste Spielzeug, das man sich überhaupt vorstellen kann. Ja und dann sagt er: Augenblick mal. Er dreht sich um und holt oben was runter und zeigt es mir. Es ist eine elektrische Sicherung. Er zeigt sie mir und steckt sie wieder ein. Ja, das ist die Sicherung zum Hauptcomputer. Dann sagt er mir, wenn etwas schief geht mit dem Computer, dann ziehen wir die Sicherung raus, stecken sie wieder ein und dann ist alles o. k. Jeder von Ihnen, der mal einen Computer bedient hat, kennt das. Wir nennen es ein *rebooting*. Wenn man den Computer aus der Tasche holt und will ihn starten, das wird *to boot the computer up* genannt, upbooten auf deutsch. Das mit der Sicherung heißt also *rebooting*. Das habe ich ihm auch gesagt. Er hatte noch nie davon gehört. Er wusste gar nichts von dem Computer, außer im Trouble nimmt man die Sicherung raus und steckt sie wieder ein. Einige Sekunden muss man schon warten, ehe man sie wieder einsteckt, das weiß er. Er ist sicher nicht der einzige, der das macht. Ich nehme an, dass das auf der Fliegerschule gelehrt wird. Der hat das doch nicht selbst erfunden. In diesem Sinn ist es schon heute falsch zu sagen, siehst Du, er benutzt den Computer und bekommt deshalb den Job eher als jemand, der noch nie einen Computer gesehen hat. Nein, das stimmt nicht. Es ist auch kein Computer am Flugschalter. Es ist eine Art Schreibmaschine, sehr sehr vereinfacht. Das heißt, man muss kein Papier reinstecken mit einem Formular drauf. Nein, es wird auf dem Bildschirm gezeigt und da tippt man rein. Und wenn er zuviel oder zuwenig tippt, dann sagt er „he!“, das war zuwenig oder zuviel. Also der Computer ist sogar schon heute überall und es ist überhaupt kein Vorteil für die meisten Jobs, dass man etwas von einem Computer versteht.

Man könnte ja sagen, o. k. es ist kein Vorteil, aber es ist eine gute Idee, dass die Kinder darüber etwas wissen. Es kommt aber dann auch darauf an, wie viel die Schule darüber weiß und der Lehrer oder die Lehrerin. Aber man muss sich daran erinnern: Die Schule hat einen Haushalt, nicht nur an Geld, sondern auch an Zeit. Es gibt soundsoviele Stunden, in denen man die Kinder in der Schule gefangen hat und wenn man etwas neu einführt, ob es eine Fremdsprache ist oder Tennis oder was auch immer, muss etwas anderes rausgeschmissen werden. Und wenn man etwas

neu reinstellt, dann wird klar, dass das eine Frage der Prioritäten ist. Und dann muss man das Neue sich ansehen gegenüber dem, was man rausschmeißen möchte, zum Beispiel die Bibliothek. Man muss sich fragen: Bedient das eine eine höhere Priorität als das andere? Ob man es tatsächlich so macht, ob man überhaupt darüber nachdenkt, ob einem diese Frage überhaupt einfällt, das ist etwas anderes. Ich glaube, wenn Präsident Bush sagt, die Schulen müssen vernetzt werden, hat er nicht daran gedacht, welches die Prioritäten sind. Was ist die höchste Priorität der Schule? Ich glaube die Antwort zu haben. Ich würde sogar wagen zu behaupten, dass in der modernen Welt, vielleicht auch in der alten Welt, jede Schule dieselbe erste Priorität hat wie jede andere. Das hört sich komisch an, die deutsche Schule, die Dorfschule, die City-Schule, ob in England, Afghanistan und wo auch immer. Ich glaube, es ist ganz einfach: Das allerallerwichtigste ist, den Schülern ihre eigene Sprache beizubringen, damit sie sich klar und deutlich artikulieren können, nicht nur in der Sprache, auch in der Schrift. Und das bedeutet, dass sie lesen können, dass sie verstehen, was sie lesen. Das bedeutet, dass sie kritisch denken können. Ich will keinen Vortrag darüber halten, wie das miteinander verbunden ist, aber das ist es: die Sprache hat die höchste Priorität für alle Schulen. Die Sprache ist gerade das, was heute fehlt.

Unsere Regierung erzählt uns, dass ein Drittel der Jugend *functional analphabetic*s sind. Das bedeutet per Definition, sie können Straßenschilder lesen und Comics, aber sie können keine Anzeige in einer Zeitung lesen für einen Job, den sie vielleicht erfüllen könnten. Und sie könnten bestimmt keinen Brief schreiben an den, der die Anzeige aufgegeben hat, um sich für irgendeinen Job zu bewerben. So ist das mit unserer Sprache und ich glaube, es ist fast so schlimm oder genauso schlimm in Deutschland. Meine Universität – das MIT – ist eine private Universität. Wir wählen unsere Studenten sehr, sehr vorsichtig aus. Das sind die besten, die Amerika zu bieten hat. Und ich würde sagen, ein Drittel von ihnen kann keine ganze Seite in Handschrift – wenn sie überhaupt mit der Hand schreiben können – in englischer Sprache schreiben.

Noch ein Wort zum Ende. Eines der wichtigsten Phänomene unseres Zeitalters, wenn nicht das wichtigste, ist die Schnelligkeit, mit der wir leben und ganz besonders die Schnelligkeit der Entwicklung unserer Naturwissenschaft und Technologie. Es gibt dafür keine Parallele in der Geschichte. Nur zur Erinnerung: Im ersten Jahrzehnt des 20. Jahrhunderts sind die Wright-Brüder einen halben Kilometer zwei Meter über dem Boden in einem Flugzeug geflogen. Das war das erste Mal, dass ein Flugzeug flog, das gesteuert werden konnte. 60 Jahre später hatten wir Menschen, die auf dem Mond herumliefen. Oder was genauso beeindruckend ist: 1938 hat die Menschheit erfahren, dass das Atom gespalten werden kann und dass diese Spaltung ungeheuer viel Energie produzieren kann. Weniger als zehn Jahre später hatten wir die Atombombe. Die Welt hat sich geändert und sie wird sich in den nächsten zehn Jahren furchtbar schnell ändern. Jemand, der bis 18 in die Schule geht, muss gelernt haben, wirklich zu denken, zu überlegen, eine kritische Mentalität auszubilden. Und ich komme zurück: das geht nicht ohne Sprache, das Wichtigste ist die Sprache.

Ein kleines Rätsel. Damit Sie glauben können, was ich über das Verschwinden des Computers aus unserem Bewusstsein sage, gebe ich Ihnen ein Rätsel auf. Es gibt ein kleines Gerät, von die-

sem Gerät gibt es in Deutschland mehr als Menschen. Gerade hier, wo wir sitzen, gibt es viele. Ich habe es jetzt nicht bei mir, aber viele von Ihnen haben es bei sich. Jedenfalls haben wir alle das Gerät heute benutzt und wir werden es noch sehr oft heute benutzen. Ich könnte sagen, es ist kein Gerät, sondern es ist Sauerstoff, es ist überall und wir würden alle tot sein, wenn es nicht hier wäre. Aber wir sehen es nicht, es ist uns nicht bewußt, wir haben es vergessen. So ist das mit diesem Gerät. Bevor Sie anfangen zu raten, was das sein könnte, muss ich dazu sagen, vor 150 Jahren gab es dieses Gerät nicht, überhaupt nicht. Und sollte der liebe Gott ein neues Naturgesetz aussprechen, das zur Folge hat, dass dieses Gerät nicht mehr funktionieren kann, dass es weg ist, dann würde in zwei Wochen in allen Städten der Erde Blut wie Wasser fließen. Menschen würden sich ermorden, es ist eine furchtbare Vision. Und Tausende von Jahren ist die Menschheit ohne dieses Gerät ausgekommen! Was ist das für ein Gerät? Ich sage einfach: hier ist etwas, es ist so nah, es ist überall. Sie haben es heute schon mehrmals benutzt und gerade weil es überall ist, so total universal, sehen wir es nicht. Wir den-

ken nicht dran. Ich muss auch sagen, in der Universität gibt es Lehrveranstaltungen, in denen gelehrt wird, wie es funktioniert, was es ist, wie man es entwirft. Das ist ein Fach.

Ein kleiner Hinweis für die Auflösung. Heutzutage wird die Bremse in einem Auto mit diesem Gerät gesteuert: dem Computer! Wenn ich bremse, dann ist es nicht meine Kraft, die etwas bewirkt, sondern das Betätigen des Pedals ist ein Signal, das zu einem Computer geht, der dann die Bremse einstellt. Und warum ist da ein Computer? Weil es eine kleine Kunst ist, ein Auto bei Glatteis zu bremsen. Und der Computer ist so programmiert, dass er die Kunst verkörpert, ein Auto bei Glatteis zu bremsen ohne zu schlittern. Stellen Sie sich vor, Sie sind mit mir in einem solchen Auto, wir kommen auf Glatteis, ich bremse und auf einmal schlittert das Auto hin und her, es stimmt etwas nicht, da ist ein Fehler im Bremscomputer. Würden Sie sich freuen, dass Sie gerade mit jemandem fahren, der sehr viel über Computer weiß? Nein, Sie würden sich freuen, wenn ich auch weiß, wie man ein Auto fährt. Genauso mit dem Flugzeug.

Andrea Knaut und Stefan Ullrich

## Joseph Weizenbaum: Das Verschwinden des Computers

Joseph Weizenbaum mahnte schon recht früh vor gesellschaftlichen Fehlentwicklungen, die durch Computer verstärkt werden können. Auch Jahrzehnte nach Erscheinen seines Hauptwerks *Die Macht der Computer und die Ohnmacht der Vernunft* haben zentrale Thesen nichts an ihrer Bedeutung verloren, wie wir bereits in der letzten *FfF-Kommunikation* gesehen haben. Dies scheint ihn selbst überrascht zu haben in diesem Vortrag von 2001.

Menschen, die ihn kennengelernt haben, werden seine Stimme regelrecht heraushören, da wir uns gegen eine sprachliche Glättung entschieden haben, auch wenn dies an der einen oder anderen Stelle etwas sprunghaft wirkt; Satzstruktur und Vokabular des Englischen, das er viele Jahrzehnte hauptsächlich gesprochen hatte, scheinen überall durch. Er hielt den Vortrag am 10. Mai 2001 im Rahmen des vom Ulmer Museum und dem HfG-Archiv Ulm ausgerichteten Symposiums *Vom Handeln im Netz. Dimensionen der Globalisierung*. Nur wenige Jahre danach wird eine große US-amerikanische Firma ein ikonisches Smartphone vorstellen, das inzwischen längst ein ständiger Begleiter unseres Lebens geworden ist und erneut stellen wir fest, dass seine Prognosen eingetroffen sind, mit einer kleinen Korrektur: Wenn Weizenbaum das damals noch drei Monate alte Projekt namens »Wikipedia« gekannt hätte, wäre seine Beurteilung des Internets wohl weniger kulturpessimistisch ausgefallen; wobei, wahrscheinlich auch nicht, denken wir nur an *fake news* und das faktenbefreite Weltbild von einigen Messenger-Gruppen. Doch zum Inhalt.

Der Umgang mit vernetzten und versteckten Computern ist inzwischen so selbstverständlich, dass wir diese Interaktion nicht mehr wahrnehmen, der Computer verschwindet, so Weizenbaum, regelrecht aus unserem Bewusstsein. Mehr noch, der Computer ist längst ein Mittler zwischen unseren Entscheidungen und unseren Handlungen geworden. Dies ist bei Flugzeugen als *fly-by-wire* bekannt. Bei Weizenbaum geht es immer

wieder darum: Welche Personen verstehen diese hochkomplexen Systeme so gut, dass sie die Folgen des Einsatzes abschätzen können?

Informatikfachleute beobachten mit Sorge, dass grundlegende mathematisch-technische Kompetenzen in der breiten Bevölkerung nicht so weit verbreitet sind wie die auf diesen Prinzipien basierenden Geräte. Doch im Sinne Weizenbaums heißt das nicht, dass alle Programmiersprachen beherrschen sollten. Das wäre zu kurz gegriffen. Es bedeutet zu lernen, wie Sprache, abstrakte Modelle, Konzeptbildung und Formalisierung funktionieren, wo die Grenzen des Programmierens liegen, was natürliche und formale Sprache unterscheidet und dass es „nur“ Computer sind, die in der ganzen Digitalisierungsmagie stecken. Es bedeutet auch zu begreifen oder mit guten Argumenten darüber streiten zu können, dass die Computer aus militärischen Gründen immer kleiner wurden und nicht, weil Moore's law etwa ein Naturgesetz wäre. Denn wo solchen ein Begreifen fehlt, entgleitet uns die Kontrolle und die informationelle Hoheit über unsere IT-Systeme. Damit wird die Frage wichtiger, ob wir in dieser technisierten Gesellschaft etwaige Fehlentwicklungen überhaupt bremsen können, oder ob nicht auch die Gesellschaft inzwischen „by wire“ funktioniert. Ein Hinweis darauf, wie wir die Selbstbestimmung in der so vernetzten Gesellschaft (zurück-)erlangen, versteckt sich in der Anekdote über Mahātmā Gandhi: Es ist das Nachdenken, das zwar etwas Zeit kostet, uns aber weise Antworten ermöglicht. „Mister Gandhi, what do you think of Western civilisation?“ He thought about it for a moment and then answered: „I think it would be a good idea.“

*Das Vortragstranskript erschien zuerst auf Deutsch und in englischer Übersetzung unter dem Titel *Das Internet im Magazin form+zweck 19, Vom Handeln im Netz. Dimensionen der Globalisierung*, 2002, 34. Jahrgang, form+zweck Verlag. Der Wiederabdruck des deutschen Texts erfolgt mit freundlicher Genehmigung des Verlags. Er ist leicht gekürzt und vorsichtig redaktionell bearbeitet.*



Dagmar Boedicker

## Selbstbestimmung in digitalen Räumen

FifF-Konferenz 2021 vom 12. bis 14. November in München

### Editorial zum Schwerpunkt

*Das allseits bekannte und wenig beliebte Virus hat den Besucherinnen, Vortragenden, dem Vorbereitungs-Team und unseren Helferinnen in München haufenweise Scherereien gemacht. Viele konnten gar nicht kommen, was ein guter Grund ist, so viele Inhalte wie möglich hier in mehr oder weniger gekürzter Form abzubilden. Für alle, die zusätzlich oder stattdessen den O-Ton verfolgen möchten: Der findet sich unter <https://media.ccc.de/c/fiffkon21>. Ohne die tüchtigen Kollegen (es waren tatsächlich nur Männer) vom Münchner CCC-Team wäre manches schlechter gelaufen. Tatsächlich haben wir alle eine prima Aufzeichnung und die Vortragenden hatten eine kompetente, gelassene technische Betreuung, von der andere nur träumen können. Danke, liebes CCC-Team, für Eure herausragende Hilfe!*

In vielen FifF-Jahren habe ich erlebt, dass Mitglieder von Regionalgruppen Wissen, Zeit und Begeisterung in die Organisation einer Tagung gesteckt haben, manche haben darüber sogar vorübergehend die Lust verloren. Die gute Nachricht aus München: Das Team hat zusammengehalten und ist gestärkt. Und das, obwohl es bisher keine FifF-Konferenz gegeben hat, bei der noch zwei Wochen vorher unklar war, ob sie nur im Netz oder doch auch an einem Tagungsort stattfinden kann. Einen besonderen Schlag gab es in letzter Minute: Der fertig konzipierte und organisierte Schul-Track musste abgesagt werden. Sehr wahrscheinlich wird die Veranstaltung im Frühjahr nachgeholt, wir informieren.

Jetzt freuen wir uns, Euch und Ihnen mit diesem Schwerpunkt eine Nachlese der Inhalte zu präsentieren. Sie erscheinen in der Reihenfolge, wie sie im Programm angekündigt sind, gefolgt von den Beiträgen der Studienpreisträgerinnen. Leider fehlen zwei Vorträge, die hoffentlich für das nächste Heft nachgeliefert werden.

### Die Vorträge im Programm

*Digitale Risikokompetenz: Wer steuert unser Verhalten?* von Gerd Gigerenzer. In seinem Einführungsvortrag bot Prof. Dr. Gigerenzer eine anschauliche, detailreiche Tour de Force des Themas, die er uns leider nicht schriftlich zur Verfügung stellen konnte. Er behandelte die Aspekte der uninformierten Einwilligung als Voraussetzung für das Nutzen von Online-Angeboten und die generell fehlende Transparenz, oft damit begründet, dass Geschäftsgeheimnisse auf dem Spiel stünden. Wir drucken einen Auszug aus seinem Buch *Klick*.

*Automatisierte Fehlerreduktion in sozialen Daten* von Frauke Kreuter. Sie verwies darauf, dass für den erfolgreichen Einsatz automatisierter Entscheidungssysteme wichtige Fragen zu stellen sind: „Wer fehlt hier in meinen Daten?“, „Von welchen gesellschaftlichen Gruppen wissen wir zu wenig, um gute Vorher-

sagen zu treffen?“ oder auch „Messen meine Daten überhaupt das, was uns interessiert?“ Auch warnte sie davor, dass Gruppen am Rande der Gesellschaft aus Furcht oder aufgrund fehlenden Zugangs weniger Daten zur Verfügung stellen könnten.

Philipp Staabs Vortrag *Digitale Gesellschaft zwischen Herrschaft und Innovation* beleuchtete das Thema aus der ökonomischen Perspektive auf die Veränderung von Märkten und den (Eliten-) Konflikt zwischen Konsumenten und Kapital auf der einen und Produzenten auf der anderen Seite. Er machte Hoffnung mit dem *Plattform-Kommunalismus* und erklärte dessen Voraussetzungen.

*Voreingenommenheit im Gehirn und im Algorithmus* von Abigail Morrison bot verblüffende Einblicke in die Unzulänglichkeit menschlicher Wahrnehmung, wenn es darum geht, Entscheidungen über die Wahrscheinlichkeit von Ereignissen zu fällen. Auch bei Algorithmen können Voreingenommenheiten auftreten, Morrison beschrieb technische Ansätze, diese zu reduzieren.

In ihrem Vortrag *Kontrollierte Selbstbestimmung. Wie Überwachung im Gesundheitswesen unter die Haut geht* zeigte Silja Samerski sich skeptisch, was die Versprechen betrifft, Selbstbestimmung im Gesundheitswesen mithilfe der Digitalisierung zu verwirklichen. Angesichts des Datenhungers von Forschung und Industrie spielten wohl eher andere Ziele die erste Geige, wie ein umfassendes Erziehungsprojekt und die Optimierung des Nutzerverhaltens. Pointiert zusammengefasst sollten Patientinnen aktiv eingebunden werden, damit das System besser läuft.

Heiner Heiland fasste in *Soziale Konstruktion von Algorithmen. Interpretationen und Praktiken algorithmischen Managements* die Entwicklung zusammen, die in der Arbeitswelt Herrschaft *automatisierte*. Es geht ihm allerdings um mehr, nämlich um die wechselseitigen Einflüsse und die soziale *Konstruktion* von technischen Prozessen. Es existiere eine interpretative Flexibilität, der zufolge Technik zwar meist eine dominante Nutzungsweise bedeute, aber immer auch anders genutzt werden könne.



Leider lagen uns nicht zu allen Konferenzbeiträgen bis zum Redaktionsschluss Ausarbeitungen vor. Weitere Beiträge drucken wir gerne in der kommenden Ausgabe der FfF-Kommunikation.

## Die Studienpreise

Stefan Hügel hat die Einleitung zu den Studienpreisen verfasst, siehe Seite 38. Weil wir auch die Laudationes drucken (ab Seite 39), gibt es hier nur eine Übersicht.

- *Warum YouTubes KI gefährlich ist und was wir dagegen tun können* von Hendrik Heuer

- *Digitale Identifikationssysteme und das Recht auf Privatsphäre im Asyl-Kontext: Eine Analyse der Umsetzungen im Bundesamt für Migration und Flüchtlinge* von Helene Hahn
- *Zur (Mit-)Gestaltung der digitalen Gesellschaft durch rationales Vertrauen* von Silke Meiser
- *Die Digitalisierung der Kreditwirtschaft* von Martin Schmitt

Eine anregende Lektüre und viel Vergnügen beim Nachhören und -sehen von der Redaktion und aus München und drumrum.



Stefan Hügel

# FfF-Konferenz 2021: Selbstbestimmung in digitalen Räumen

## Begrüßung

Liebe Mitglieder des FfF,  
liebe Freundinnen und Freunde,  
liebe Gäste,  
liebe Teilnehmer:innen an den Geräten,

„Denn man sieht nur die im Lichte, die im Dunkeln sieht man nicht.“ Bertolt Brecht steht Pate für die diesjährige FfF-Konferenz, die, wie bereits im vergangenen Jahr, wieder weitgehend online stattfindet. Eine „hybride“ Möglichkeit gibt es dabei für Teilnehmer:innen, die aus persönlichen Gründen eine Teilnahme vor Ort vorziehen. Dabei gilt 2G, also Einlass erhält nur, wer geimpft oder genesen ist. Wir wollen das Infektionsrisiko auf ein Minimum reduzieren.

Menschen, die Freunde oder Verwandte durch die Pandemie verloren haben, haben besonders schmerzlich erfahren müssen, was diese Krankheit bedeutet. Die im Dunkeln sieht man nicht, auf den Intensivstationen der Kliniken. Erschreckend, wenn manche behaupten, das sei alles nicht so schlimm, gar, dass Corona nur eine Täuschung der Mächtigen sei. Stimmungsmache, auch in den Medien, verstärkt diese Einstellung noch. Geimpft oder ungeimpft wird zur ideologischen Frage. „Querdenker“, viele davon aus der rechtspopulistischen Szene, erkennen in dieser Frage eine Spaltung der Gesellschaft, die sie in Wirklichkeit selbst betreiben.

Wir haben es bei den Covid-19-Infektionen mit exponentiellen Prozessen zu tun. Es zeigt sich immer wieder, wie schwer wir uns tun, solche Prozesse einschätzen zu können. Das zeigt sich nicht nur bei der Covid-19-Pandemie, sondern auch bei anderen gesellschaftlichen Entwicklungen: der Klimakrise oder der Digitalisierung. Dazu kommen irreversible Kippunkte, die zu einer zusätzlichen Beschleunigung führen.

„Denn man sieht nur die im Lichte, die im Dunkeln sieht man nicht.“ *Erstens:* Die immer noch grassierende Covid-19-Pandemie ist eines der großen Themen, die politisch heute im Vordergrund stehen und die wohl zu einer der größten Herausforderungen

für die sich gerade bildende Bundesregierung gehören. Sie wirft bürgerrechtliche Fragen wie in einem Brennglas auf: Welche Rolle soll die persönliche Freiheit spielen, wenn sie potenziell in Konkurrenz zur Gesundheit steht? *Zweitens:* Die drohende Klimakatastrophe stellt ähnliche Fragen vielleicht noch viel drängender, da ihre Auswirkungen im Gegensatz zur Pandemie nicht zeitlich begrenzt werden können. Auch hier werden wir möglicherweise mit großen Einschränkungen rechnen müssen – die gleichzeitig notwendig sind, um unsere Freiheit langfristig zu schützen. An der Frage, wie wir mit den damit verbundenen Konsequenzen umgehen und wie erfolgreich wir damit sind, entscheidet sich vielleicht die Zukunft der Menschheit. *Drittens:* Die Digitalisierung, die großartige Chancen bietet – aber gleichzeitig auch bürgerrechtliche Risiken, durch die Umwälzung von Kommunikation und Wirtschaft, durch staatliche und wirtschaftliche Überwachung. All diese Prozesse sind exponentielle Prozesse. Sie wachsen immer schneller, und nicht alle können dieser Entwicklung folgen. Der schwedische Mediziner Hans Rosling postulierte in seinem Buch *Factfulness*, dass viele von uns immer noch eine Weltsicht wie in den 1960-er Jahren hätten, darunter auch Menschen, die auf internationaler Ebene Verantwortung tragen.

Von diesen Prozessen ist vor allem die Digitalisierung eines der wichtigsten Themen für das FfF. Auch die Digitalisierung entwickelt sich exponentiell – erinnert sich noch jemand an eine Zeit ohne allgegenwärtiges Smartphone, Tablet, Notebook? Weiß noch jemand, was eine „Wahlscheibe“ oder „Bandsalat“ ist? Wer hat am letzten Wochenende (wie ich) „Wetten dass ...?“ gesehen – eine Fernsehsendung wie aus einem anderen Zeitalter. Die Digitalisierung hat aber Gewinner und Verlierer – dies werden wir in den kommenden Tagen diskutieren. Wir schauen Elon Musk und Jeff Bezos bei ihren Raumflügen zu, zwei „im Lichte“, die so unermesslich viel Geld mit der Digitalisierung verdienen, dass sie nicht mehr wissen, wohin damit. Diejenigen, die für wenig Geld im fahlen Licht ihres Displays Hinrichtungsvideos aus dem Netz fischen, sehen wir nicht.





„Denn man sieht nur die im Lichte, die im Dunkeln sieht man nicht.“ Informationstechnik verändert rasant, wie wir kommunizieren, denken, uns bewegen und handeln. Sie dringt in persönliche und zwischenmenschliche Bereiche vor und beeinflusst unser Verhalten, ohne dass wir uns dessen immer bewusst sind. Wo wir uns als handelnde Subjekte sehen, werden wir oft als Objekte vermessen, bewertet und behandelt. Auf Plattformen und in sozialen Netzen, in smarten Infrastrukturen und in Scoring-Systemen wirken höchst profitable Algorithmen und Geschäftsmodelle, die wir kaum durchschauen, geschweige denn (selbst) bestimmen können. Die Plattformen und ihre Betreiber profitieren von einem ungeheuren Machtgefälle, das sich aus der asymmetrischen Verteilung von Daten, Informationen und Wissen ergibt. Das gilt für den Zuboff'schen Überwachungskapitalismus wie für die staatliche Überwachung, die seit den Enthüllungen von Edward Snowden kaum geringer geworden ist. Julian Assange – als Person viel kritisiert, möglicherweise nicht nur zu Unrecht – der versucht hat, Licht in das Dunkel zu bringen, muss gerade erfahren, was es bedeutet, Staaten und ihre Institutionen herauszufordern. Gefangen im Hochsicherheitsgefängnis, bedroht mit völlig absurden Strafen. Auch die deutsche Bundesregierung hat erkennbar bisher keinen Finger krumm gemacht, um dieses Unrecht zu verhindern, das Nils Melzer, der UN-Sonderberichterstatter über Folter in seinem kürzlich erschienen Buch auf beklemmende Weise beschreibt. Dürfen wir bei der sich gerade bildenden Koalition auf mehr Bewusstsein für Menschenrechte hoffen?

„Denn man sieht nur die im Lichte, die im Dunkeln sieht man nicht.“ Wenn wir die Selbstbestimmung als Voraussetzung für unser demokratisches Gemeinwesen zurückerlangen und bewahren wollen, brauchen wir sowohl den Einblick in die Technik

als auch den Überblick über die handelnden Akteure und ihre verschiedenen Interessen. Wir wollen beispielsweise wissen, wo Bonus-Systeme von Versicherungen die Daseinsvorsorge untergraben, wo Profiling diskriminiert oder Plattformen Ungleichheit verstärken. Diesen Fragen werden wir auf der FIF-Konferenz anhand einiger Anwendungen nachgehen. Sie müssen Teil der Allgemeinbildung werden: Es geht nicht um Programmierunterricht, der gerne publikumswirksam gefordert wird; es geht um die Frage, wie komplexe technische Systeme funktionieren und was sie bewirken. Es geht um einen informierten Blick in den Maschinenraum, und es geht auch wieder um die Machtstrukturen, die Systeme und ihre Wirkungen prägen.

„Denn man sieht nur die im Lichte, die im Dunkeln sieht man nicht.“ Wir wollen auch mit der diesjährigen Konferenz dazu beitragen, Lichter zu setzen. Wir wollen den Scheinwerfer auf die wichtigen Themen der Digitalisierung richten. Dafür gibt es die Vorträge, Workshops und Diskussionen der kommenden Tage. Und wir richten das Licht auf die Persönlichkeiten, die sich damit in herausragender Weise beschäftigen. Dafür verleihen wir morgen die Weizenbaum-Medaille und den Weizenbaum-Studienpreis.

Im Namen des FIF-Vorstands und des Organisationsteams – dem ich für viel Arbeit unter erschwerten Bedingungen herzlich danke – wünsche ich viel Freude bei der Konferenz, viele neue Anregungen und viele Erkenntnisse – über Selbstbestimmung in digitalen Räumen. Lasst uns gemeinsam den Blick auf die richten, die sonst im Dunkeln sind.

Vielen Dank.



Gerd Gigerenzer

## Digitale Risikokompetenz:

### Wer steuert unser Verhalten?

*Der Einführungsvortrag bot eine anschauliche, detailreiche Tour de Force des Themas, die Professor Dr. Gigerenzer uns leider nicht schriftlich zur Verfügung stellen konnte. Er behandelte die Aspekte der uninformierten Einwilligung als Voraussetzung für das Nutzen von Online-Angeboten und die generell fehlende Transparenz, oft damit begründet, dass Geschäftsgeheimnisse auf dem Spiel stünden. Weiter ging es um die Qualität von Algorithmen und Daten für das maschinelle Lernen, von resultierenden Scores und Super Scores. Seine These lautet, dass KI sich nur in einer stabilen Welt bewährt, aber selbst dann nicht immer besser abschneidet als schlecht bezahlte Menschen, beispielsweise bei Amazon Turk. So wurde Watson Oncology nach einiger Zeit von IBM zurückgezogen. Gigerenzer erläuterte, wie problematisch die Überwachung durch staatliche und private Akteure ist, besonders im Bereich Polizei und Justiz. Wir seien bereits auf dem Weg zur Blackbox-Justiz. Wenn der Gesetzgeber Unternehmen und nicht Bürger schützt, bleibt es den Bürgern überlassen, sich nicht hinter dem paradoxen Wunsch nach Privatsphäre zu ducken, vielmehr sollten sie bedenken, dass das Netz kein Gratis-Cafe ist, in dem sie zwar kostenlos verzehren können, aber selbst zum Produkt werden. Die Dienstleistung der großen Anbieter würde 2 € / Monat kosten.*

*Gigerenzer geht es um kognitive und Handlungskompetenz. In seinem lesenswerten Buch Klick,<sup>1</sup> aus dem wir einige Seiten mit freundlicher Genehmigung von Autor und Verlag abdrucken, finden sich detaillierte Analysen, konkrete Beispiele aus der Netzwelt und Vorschläge zur Ermächtigung der Nutzerinnen und Nutzer. Die folgenden Seiten (213 bis 221) behandeln den Aspekt der Transparenz.*

© für die deutschsprachige Ausgabe C. Bertelsmann Verlag, München.



## Einfach zählen

Transparente Algorithmen lassen sich in mehrere Familien unterteilen. Die „Ein guter Grund“-Familie besteht, wie der Name sagt, aus Algorithmen, die ihre Vorhersage auf einen einzigen, aber aussagekräftigen Grund stützen.<sup>2</sup> Wie wir im Fall der Grippevorhersage gesehen haben, kann das zu besseren Vorhersagen führen als mittels der Big-Data-Analytik. Eine zweite Familie besteht aus Algorithmen, die nur einige wenige Gründe verwenden, ihnen aber unterschiedliche, wenn auch einfache Gewichte geben, so der Zahlen-Sie-wie-Sie-fahren-Algorithmus in Abbildung 1 und der PSA. Eine dritte Familie besteht aus kurzen Entscheidungslisten wie derjenigen für die Vorhersage, ob ein Angeklagter rückfällig wird. Beim Maschinenlernen gibt es solche Entscheidungslisten schon lange.<sup>3</sup> Im Folgenden beschreibe ich eine weitere Familie, die sogenannte Strichliste (Tally), die einfach die Gründe für und gegen ein mögliches Ergebnis zählt.<sup>4</sup> Alle diese Regeln entsprechen der psychologischen KI, die wie die menschliche Psychologie, besonders geeignet ist, Vorhersagen unter ungewissen Bedingungen zu treffen.

Merkmal (Ereignis)	Gewicht
Starke Beschleunigung oder starkes Bremsen	40
Überhöhte Geschwindigkeit (mehr als 20 % mehr als 30 Sekunden lang)	30
Nachfahrten zwischen 23:00 und 5:00 Uhr	20
Stadtfahrten	10

Abbildung 1: Zahlen Sie, wie Sie fahren. Eine Blackbox im Auto übermittelt vier Merkmale des Fahrerverhaltens an die Telematikversicherung. Die Fahrsicherheit wird durch einen transparenten Algorithmus berechnet.

### Der Schlüssel zum weißen Haus

Am 8. November 2016 gab es nicht wenige Menschen auf dem Globus, die ihren Augen nicht trauen mochten. Umfragen, Wahlbörsen und Big-Data-Analytik hatten Hillary Clintons Sieg mit großem Vorsprung vorausgesagt. „Wenn Sie an Big-Data-Analytik glauben, sollten Sie sich jetzt auf Hillary Clintons Präsidentschaft einstellen“, erklärte der Kolumnist Jon Markman in *Forbes*.<sup>5</sup>

Am Ende erlitt Big Data eine Bruchlandung. Zugegeben ist die richtige Prognose, wer die Schlüssel zum Weißen Haus bekommt, leichter gesagt als getan. Es ähnelt weniger einer Lotterie, bei der wir wissen, wie wahrscheinlich Gewinn oder Verlust ist, als der ungewissen Vorhersage des Verlaufs einer Grippe oder einer anderen Virusinfektion. Der Statistiker Nate Silver und sein Team von der Nachrichtenwebseite *FiveThirtyEight* hatten Obamas Siege richtig vorhergesagt, aber irrten sich bei Trumps Sieg in den Vorwahlen und attestierten in ihrer Wahlprognose Clinton eine 71,4-prozentige Siegchance. Zwei Wochen vor der Wahl, als er Clinton mit 85 Prozent vorne sah, erörterte Silver eingehend, in welchem Maße die Wahrscheinlichkeit von den zugrunde liegenden Annahmen abhängt. Wenn sein Modell nur Daten seit 2000 berücksichtigte, und nicht seit 1972,

stiegen Clintons Aussichten auf 95 Prozent. Wenn es eine Normalverteilung der Stimmen voraussetzte (ein Konzept, das auf den Mathematiker Carl Friedrich Gauß zurückgeht; siehe Abbildung 2) statt dicker Enden (fat tails) – ein Begriff, der in Nassim Nicholas Talebs Buch *Schwarzer Schwan* eine zentrale Rolle spielt –, wäre Clinton dadurch auf 87 Prozent gekommen, und bei der Annahme, dass die Ergebnisse der Einzelstaaten nicht mit einander korrelierten, wäre ihre Gewinnchance auf 98,2 Prozent gestiegen.<sup>6</sup> Silvers wertvolle Überlegungen führen uns eine häufig vergessene Erkenntnis vor Augen: *Big Data spricht nicht für sich*, vielmehr sind die Ergebnisse von den zugrunde liegenden Annahmen abhängig. Mehr Daten und mehr Rechenleistung sind keine Garantie für die Wahrheit. Deshalb ist statistisches Denken so wichtig.



Abbildung 2: Die 10-DM-Note zeigt das Porträt von Carl Friedrich Gauß und, unter anderem, die von ihm entwickelte Normalverteilungskurve. Der Geldschein wurde 1991 ausgegeben und war bis zur Einführung des Euro im Jahr 2002 in Umlauf. Die Normalverteilung ist die Grundlage vieler Modelle in Maschinenlernen, Wirtschaftswissenschaft, Psychologie und anderen Disziplinen. Gauß gehörte zu den letzten Mathematikern, die wegen ihrer Kopfrechenkünste gefeiert wurden.

Silvers Erörterung offenbart noch einen weiteren interessanten Punkt: Sie beschäftigt sich mit den Gründen für oder gegen statistische Modelle, nicht mit den konkreten Gründen, warum Menschen gegen Clinton und für Trump wählen könnten. Sie verzichtet auf psychologische, politische oder wirtschaftliche Theorien. Die Alternative ist, mit der Psychologie der Wählermotive zu beginnen. Genau das hat Allan Lichtman getan.

Lichtman, ein angesehener Geschichtspräsident, war eine der wenigen abweichenden Stimmen von der überwältigenden Mehrheit der Experten, die einen klaren Sieg von Clinton vorhersagten. Er prognostizierte, Trump würde gewinnen. Es war nicht das erste Mal, dass er richtiglag; er hatte alle Wahlen seit 1984 richtig vorhergesagt.<sup>7</sup> Seine Methode stützt sich weder auf die Analyse von Big Data, noch liefert sie scheinbar exakte Wahrscheinlichkeiten für den Sieg. Sie sagt einfach vorher, wer gewinnen wird. Das System heißt „Schlüssel zum Weißen Haus“ und beruht auf einer historischen Analyse der Gründe, warum Amerikaner so wählen, wie sie es eben tun.

Ein Schlüssel ist ein Grund, der für Wähler zählt. Es gibt dreizehn solche Gründe, alle in Gestalt einer Aussage, die mit „Ja“ oder





„Nein“ beantwortet werden kann. Ein „Ja“ begünstigt die Wahl oder Wiederwahl eines Kandidaten der amtierenden Partei, ein „Nein“ nicht.

- Schlüssel 1: *Mandat der amtierenden Partei*. Nach der Zwischenwahl hat die regierende Partei mehr Sitze im Repräsentantenhaus als vorher.
- Schlüssel 2: *Nominierungswettbewerb*. Es gibt in der regierenden Partei bei der Nominierung des Kandidaten keinen ernsthaften Wettbewerb.
- Schlüssel 3: *Amtsausübung*. Der Kandidat der regierenden Partei ist der aktuelle Präsident.
- Schlüssel 4: *Drittpartei*. Es gibt keine nennenswerte Kampagne einer Drittpartei oder eines parteilosen Kandidaten.
- Schlüssel 5: *Kurzfristige Wirtschaftslage*. Die Wirtschaft befindet sich während der Wahlkampagne nicht in Rezession.
- Schlüssel 6: *Langfristige Wirtschaftslage*. Reales jährliches Wirtschaftswachstum pro Kopf während der Amtszeit ist gleich oder höher als das mittlere Wachstum während der beiden vorhergehenden Amtszeiten.
- Schlüssel 7: *Politikwechsel*. Die amtierende Regierung hat größere Veränderungen in der nationalen Politik bewirkt.
- Schlüssel 8: *Soziale Unruhe*. Es hat während der Amtszeit keine längere soziale Unruhe gegeben.
- Schlüssel 9: *Skandal*. Die amtierende Regierung ist in keinen größeren Skandal verwickelt gewesen.
- Schlüssel 10: *Außenpolitischer oder militärischer Misserfolg*. Die amtierende Regierung ist nicht von einem größeren Misserfolg in der Außen- oder Militärpolitik betroffen.
- Schlüssel 11: *Außenpolitischer oder militärischer Erfolg*. Die amtierende Regierung erzielt einen größeren Erfolg in der Außen- oder Militärpolitik.
- Schlüssel 12: *Charisma*. Der Kandidat der regierenden Partei ist charismatisch oder ein Nationalheld.
- Schlüssel 13: *Charisma des Herausforderers*. Der Kandidat der herausfordernden Partei ist weder charismatisch noch ein Nationalheld.

Vielleicht ist Ihnen etwas Merkwürdiges aufgefallen. Fast alle Schlüssel betreffen die amtierende Partei und ihren Kandidaten, jedoch nur ein einziger (der letzte) den Herausforderer. Einige der Schlüssel erfordern kein Urteil – zum Beispiel die Frage, ob der Kandidat der amtierenden Partei der aktuelle Präsident ist –, andere, so das Thema Charisma, schon. Dieses Problem löste Lichtman, indem er die wenigen charismatischen Präsidenten wie Dwight Eisenhower und John F. Kennedy definierte und dann vor der Wahl ein „Ja“ oder „Nein“ setzte. Im Fall von Clinton und Trump ordnete er weder sie noch ihn als charismatisch ein.

Die Frage lautet: Wie werden die Schlüssel miteinander verknüpft, sodass sie eine Prognose ergeben? Der erste Reflex vieler Datenwissenschaftler würde wohl darin bestehen, wie beim Online-Dating oder Kredit-Scoring ein Punktesystem zu entwickeln, in dem jeder Schlüssel ein „optimales“ Gewicht erhält. Doch es gibt nicht genügend Präsidentschaftswahlen für eine breite Datenbasis. Außerdem wird die Aufgabe durch unberechenbares Wahlverhalten noch erschwert. Stattdessen entwickelte Lichtman einen transparenten Algorithmus, der einfach die Neins zählt:

- Wenn sechs oder mehr Schlüssel negativ („Nein“) sind, wird der Herausforderer gewinnen.

Diese Abzählregel ist extrem einfach. Ende September 2016, Wochen vor der Wahl, kam Lichtman zu dem Schluss, dass die Schlüssel sich „gesetzt“ hätten, und nahm die Zählung vor.<sup>8</sup> Sechs Schlüssel sprachen gegen Hillary Clinton, die Kandidatin der regierenden Partei.

- Schlüssel 1: Die Demokraten erlitten eine krachende Niederlage in den Zwischenwahlen.
- Schlüssel 3: Der aktuelle Präsident war kein Kandidat.
- Schlüssel 4: Es gab eine nennenswerte Kampagne einer Drittpartei, der Libertären Partei mit Gary Johnson, der nach den Prognosen mindestens 5 Prozent erhalten sollte.
- Schlüssel 7: Es gab in Obamas zweiter Amtszeit keinen größeren Politikwechsel.
- Schlüssel 11: Obama hatte keinen durchschlagenden außenpolitischen Erfolg.
- Schlüssel 12: Hillary Clinton ist nicht charismatisch im Vergleich zu, sagen wir, Franklin Roosevelt.

Sechs negative Merkmale bedeuteten, dass die Prognose für den Sieg von Trump sprach. Sechs ist die erforderliche Mindestzahl, das heißt, der Ausgang der Wahl war eng und sicherlich nicht leicht vorherzusagen. Allerdings ist eine Einschränkung angebracht. Die Regel soll vorhersagen, wer die absolute Stimmenmehrheit erringt, was Trump nicht gelang. Aber kein Vorhersagesystem ist vollkommen, und Lichtmans Strichliste kam dem Endergebnis näher als alle Umfragen, Prognosemärkte und Big-Data-Analytik.<sup>9</sup>

Die Schlüssel zum Weißen Haus sind transparent. Dank der Transparenz können wir die Theorie erkennen, die den Prognosen zugrunde liegt. Und sie beruhen tatsächlich auf einer Theorie, im Gegensatz zu den typischen Maschinenlernverfahren, in denen es nur darum geht, die beste Prognose zu erhalten, egal wie. Wie erwähnt, betreffen die meisten Schlüssel die regierende Partei und ihren Kandidaten. Es geht um Wirtschaft, soziale Unruhen, außenpolitische Erfolge, Skandale und politische Erneuerung. Das heißt, wenn die Menschen den Eindruck haben, dem Land sei es in der zurückliegenden Amtszeit gut gegangen, wird der Kandidat der regierenden Partei gewählt. Wenn ein Herausforderer wie Trump gewinnt, hat der Sieg wenig mit seiner Persönlichkeit zu tun, sondern beruht einzig auf dem Eindruck, den

die regierende Partei in der letzten Amtszeit bei den Wählern hinterlassen hat, und auf dem, was diese von dem Kandidaten der Partei erwarten.

Viele Menschen waren am Wahltag wie vor den Kopf geschlagen und fragten sich, was um alles in der Welt die Amerikaner dazu bewogen hatte, einen Mann zu wählen, der unter anderem Frauen, Muslime und den Papst beleidigt hatte. Die radikale Logik hinter der Strichliste lässt darauf schließen, dass das die falsche Frage ist. Die amerikanischen Wähler haben nicht für Trump gewählt; sie haben gegen Obama und Clinton gewählt. Vergessen Sie Fernsehdebatten, Spendensammlungen und Werbebudgets. Glauben Sie nicht, dass Wahlkampfleiter und Berater großen Einfluss auf das Ergebnis hätten. Wenn die Theorie, auf der die Schlüssel basieren, richtig ist, gibt es eine gute Nachricht für die politischen Parteien: Konzentriert euch auf das Regieren, nicht auf teure Werbung und Wahlkampfstrategien.

## Gesucht: Das Recht auf Transparenz beim Scoring

In einer Blackbox-Gesellschaft benutzen die Mächtigen die Software häufig dazu, das Verhalten der anderen besser vorherzusagen und zu manipulieren, ohne ihre Algorithmen offenzulegen. Warum wird bestimmten Menschen Bewährung oder Kredit gewährt und anderen nicht? Warum führt uns YouTubes Empfehlungssystem zu extremeren Videos und Fake News?<sup>10</sup> Das charakteristische Merkmal von Blackbox-Gesellschaften ist nicht der Mangel an Transparenz, sondern ihre Asymmetrie, die wie ein Einwegspiegel funktioniert.<sup>11</sup> Blackbox-Gesellschaften gibt es seit unvorstellbaren Zeiten. Jahrhundertlang konnten die einfachen Leute in Europa nicht lesen. Für sie waren die Bibel und andere schriftliche Quellen Blackboxes, die auf Latein oder Griechisch verfasst waren und nur von den Gebildeten aus wohlhabenderen Schichten verstanden wurden. Mithilfe der von Johannes Gutenberg erfundenen Druckerpresse öffneten Übersetzer wie Martin Luther die Blackbox. Dank dieses technologischen Fortschritts wurden Bücher und Übersetzungen allmählich allen zugänglich gemacht. So konnten Menschen leichter lesen lernen und sich selbst davon überzeugen, was in der Bibel stand. Gutenbergs Erfindung verringerte die Ungleichheit zwischen Priestern und Laien, zwischen eingeweihten und Gefolgsleuten. Als sich das Internet in den 1990-er Jahren ausbreitete, malten sich viele Ärzte eine ähnliche Revolution aus: „Das Internet kann uns helfen, die Ungleichheit zwischen Arzt und Patient, zwischen dem Unfehlbaren und dem Uninformierten aufzuheben.“<sup>12</sup> Vielleicht brauchen wir einen neuen Gutenberg, der die Blackboxes öffnet und das Verhalten der Menschen verändert.

Einer unserer Vorschläge im Sachverständigenrat für Verbraucherfragen lautete, *alle Blackboxes, die zum Scoring von Menschen verwendet werden und schwerwiegende Konsequenzen in ihrem Leben haben, für die Allgemeinheit transparent zu machen und einer Qualitätskontrolle zu unterziehen.*<sup>13</sup> Schwerwiegende Konsequenzen drohen unter anderem bei Gesundheits-Scoring, Kredit-Scoring, Bewertung der Rückfallwahrscheinlichkeit und Predictive Policing. Der Vorschlag betrifft Algorithmen, die den Menschen aufgezwungen werden, und nicht solche, die freiwillig gewählt werden und der Unterhaltung oder der persönlichen Entwicklung dienen wie Videospiele oder Liebesalgorithmen. Alle Merkmale eines Algorithmus sowie seine Logik (etwa Ent-

scheidungslisten oder Punktsysteme, Abbildung 3 und 4) sollten offengelegt werden.

<b>WENN</b>	Alter 18–20 Jahre und Geschlecht männlich	DANN sage Haft voraus (binnen 2 Jahren)
<b>SONST WENN</b>	Alter 21–23 Jahre und 2–3 Vorstrafen	DANN sage Haft voraus
<b>SONST WENN</b>	mehr als 3 Vorstrafen	DANN sage Haft voraus
<b>SONST</b>	sage keine HAFT voraus	

Abbildung 3: Ein transparenter Algorithmus für die Vorhersage, ob ein Angeklagter innerhalb der nächsten zwei Jahre verhaftet wird (von CORELS generiert). Die Kombination dieser vier Regeln bezeichnet man als Entscheidungsliste.

Merkmale	Risikopunkte für »Ja«
Anhängige Klagen zur Zeit der Haft?	1
Frühere Verurteilung?	1
Früheres Nichterscheinen, älter als zwei Jahre?	1
Früheres Nichterscheinen während der letzten zwei Jahre?	einmal: 2 öfter: 4

Abbildung 4: Public Safety Assessment (PSA) ist ein transparenter Algorithmus zur Risikobewertung. Mithilfe von vier Merkmalen wird das Risiko geschätzt, dass ein Angeklagter nicht zu seinem Gerichtstermin erscheint. Wenn die Antwort bei einer der vier Fragen »Ja« lautet, wird ihm die entsprechende Anzahl von Risikopunkten zugewiesen.

Als wir den Vorschlag mit internationalen Wirtschaftsauskunften erörterten, erhoben sie berechtigte Einwände. Der erste war, ihre Algorithmen seien Geschäftsgeheimnisse. Doch genau darum geht es in dem Vorschlag: das Gesetz zu ändern und an dieser kritischen Stelle den Rechten der Menschen Vorrang vor dem wirtschaftlichen Profit einzuräumen. Im übrigen haben Telematik- und Gesundheitsversicherer ihre Scoring-Algorithmen bereits vollkommen offengelegt, und es scheint ihnen nicht zu schaden. Der nächste Einwand lautete, die Konsumenten würden den Quellcode (das Programm des Algorithmus) nicht verstehen, daher blieben sie genauso schlau wie vorher. Aber wir forderten sie nicht auf, den Quellcode transparent zu machen, mit dem die meisten Verbraucher tatsächlich wenig anfangen könnten, sondern die Merkmale und die Logik des Algorithmus offenzulegen. Wenn die Konsumenten die Merkmale kennen würden, könnten sie beispielsweise herausfinden, warum sie hohe Zinsen für einen Kredit zahlen müssen. Der Grund könnte einfach sein, dass sie in einem Wohnblock wohnen, in dem einige Mieter ihre Kredite nicht rechtzeitig bedienen. Das nennt man Geo-Scoring.

Als Nächstes brachten die Unternehmen vor, es gebe keine Möglichkeit, tiefe neuronale Netze transparent zu machen. Das ist zwar richtig, aber wir stellten fest, dass kommerzielle Scoring-Systeme für Kredite, Krankenversicherungen, Telematik-Versicherungen und Rückfallwahrscheinlichkeit selten, wenn überhaupt, mit neuronalen Netzen arbeiten. Ein letzter Ein-





wand lautete schließlich, Nutzer könnten, wenn sie die Merkmale kennen würden, ihr Verhalten verändern und den Algorithmus austricksen. Doch genau das ist eines der bekundeten Ziele des Kredit-Scorings, Gesundheits-Scorings oder Telematik-Scorings: Menschen zu gesünderem oder finanziell vernünftigerem Verhalten zu veranlassen. Wenn Verbraucher zum Beispiel herausfinden, dass sie einen niedrigen Kredit-Score haben, weil sie zu viele Kreditkarten besitzen, können sie etwas dagegen tun. Austricksen wird nur dann zum Problem, wenn Algorithmen Ersatzmerkmale anstelle echter Merkmale verwenden, das heißt, wenn beispielsweise ein Krankenversicherer Kunden Bonuspunkte für die Mitgliedschaft in einem Fitnessstudio gibt, ohne zu prüfen, ob sie dort auch wirklich trainieren.

In der Europäischen Union markiert die Datenschutz-Grundverordnung (DSGVO) den Beginn einer neuen Ära im Datenschutzrecht. Sie verlangt, dass „aussagekräftige Informationen über die involvierte Logik bei einer automatisierten Entscheidungsfindung geliefert werden und dass die betroffene Person „das Recht hat, nicht einer ausschließlich auf einer automatisierten Verarbeitung [...] beruhenden Entscheidung unterworfen zu werden“, die sich „rechtlich“ oder „in ähnlicher Weise erheblich“ nachteilig auf sie auswirkt.<sup>14</sup> Doch in dem Augenblick, da am Ende der Kette ein menschlicher Entscheidungsträger – ein Richter oder Polizist zum Beispiel – in Erscheinung tritt, gelten diese Bestimmungen nicht mehr. Grundsätzlich bleibt die DSGVO sehr abstrakt, was zeigt, dass sie ein Problem erkannt, aber nicht gelöst hat. Inzwischen haben sich Hunderte von Mathematikern zu Wort gemeldet und verlangt, dass alle Arbeiten am Predictive Policing eingestellt werden, um möglichen Machtmissbrauch zu verhindern.<sup>15</sup> Bürger haben gegen die Geheimhaltungspolitik der Schufa und anderer Auskunftsteien protestiert und für alle Betroffenen das Recht verlangt, Einsicht in die Logik zu bekommen, der die Algorithmen folgen, wenn sie unser Verhalten vorhersagen und bewerten. Regierungsbehörden werden aufgerufen, sich eingehender über die Motivation zu informieren, die diesen Algorithmen zugrunde liegt, und etwas gegen den fortwährenden Mangel an Qualitätskontrollen zu unternehmen.

Geheimniskrämerei und Mystifizierung sind ein Aspekt der „Blackbox“. Doch der Begriff hat eine doppelte Bedeutung, er bezeichnet auch ein Aufzeichnungsgerät. Im nächsten Kapitel beschäftigen wir uns mit der anderen Seite der Blackbox.

[...]

## Anmerkungen

- 1 Gigerenzer G (2021) *KLICK. Wie wir in einer digitalen Welt die Kontrolle behalten und die richtigen Entscheidungen treffen*, München: Bertelsmann.
- 2 Im Maschinennlernen bezeichnet man diese einfachen Heuristiken als 1-Regeln, erlernt durch das 1R-Programm, siehe Holte CH (1993) *Very*

*simple classification perform well on most commonly used datasets. Machine Learning*, 11, 63-91.

- 3 Rivest RL (1987) *Learning decision lists. Machine Learning*, 2, 229-246.
- 4 *Der Umstand, dass einfache Strichlisten (Tallying) bei Ungewissheiten ebenso genau oder genauer als komplexe Algorithmen sein können, ist in der Psychologie seit Dawes R und Corrigan B (1974) Linear models in decision making. Psychological Bulletin* 81(2), 95-106, Einhorn HJ und Hogarth R (1975) *Unit weighting schemes for decision making. Organizational Behaviour and Human Performance*, 13(2), 171-192, Czerlinski J et al. (1999) *How good are simple heuristics?* In: Gigerenzer G, Todd PM, ABC Research Group (1999) *Simple heuristics that make us smart*. New York: Oxford University Press, bekannt. Katsikopoulos K et al. (2020) *Classification in the wild*. Cambridge, MA: MIT Press vergleichen Strichlisten mit Maschinenlernalgorithmen.
- 5 Markman J (2016) *Big data and the 2016 election. Forbes*. <https://www.forbes.com/sites/jonmarkman/2016/08/08/big-data-and-the-2016-election/#29fe5d7b1450>.
- 6 Silver N (2016) *Election update: Why our model is more bullish than others on Trump. FiveThirtyEight*. <https://fivethirtyeight.com/features/election-update-why-our-model-is-more-bullish-than-others-on-trump>.
- 7 Lichtman AJ (2016) *Predicting the next president. The keys to the White House*. Lanham MD: Rowman and Littlefield. Die folgende Darstellung stützt sich auf Katsikopoulos et al. (2020) a. a. O.
- 8 Stevenson PW (2016) *Trump is headed for a win, says professor who has predicted 30 years of presidential outcomes correctly. Washington Post*. [https://www.washingtonpost.com/news/the-fix/wp/2016/09/23/trump-is-headed-for-a-win-says-professor-who-has-predicted-30-years-of-presidential-outcomes-correctly/?utm\\_term=.e3a8b731325c](https://www.washingtonpost.com/news/the-fix/wp/2016/09/23/trump-is-headed-for-a-win-says-professor-who-has-predicted-30-years-of-presidential-outcomes-correctly/?utm_term=.e3a8b731325c).
- 9 *Bei der US-amerikanischen Präsidentschaftswahl 2020 sagten die Schlüssler richtig vorher, Biden werde gewinnen. Die Umfragen jedoch unterschätzten Trump abermals, wenn auch die meisten beim Endergebnis richtiglagen.*
- 10 Spinelli L und Crovella M (2020) *How YouTube leads privacy-seeking users away from reliable information. Adjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization*, 244-251. <https://doi.org/10.1145/3386392.3399566>.
- 11 Pasquale F (2015) *The black box society*. Cambridge MA, Harvard University Press.
- 12 Siehe Gigerenzer G (2003) *Calculated risks: How to know when numbers deceive you*. New York: Simon and Schuster, S. 91.
- 13 Sachverständigenrat für Verbraucherfragen des Bundesministeriums der Justiz und für Verbraucherschutz (2018). *Die Mitglieder des Rates waren geteilter Meinung in der Frage, ob Wirtschaftsauskunfteien alle Merkmale offenlegen sollten oder nur die für die Öffentlichkeit relevantesten Informationen.*
- 14 Siehe die Artikel 13 und 22 der DSGVO: Europäische Union. (2016). *Datenschutzgrundverordnung*. <https://dsgvo-gesetz.de/>.
- 15 Letter to AMS Notices: *Boycott collaboration with police To the Mathematics Community*: <https://docs.google.com/forms/d/e/1FAIpQLSfdmQGrgdCBCexTrpne7KXUzpbil9LeEtdoAm-qRFimpwuv1A/view-form>.

**Gerd Gigerenzer**

Prof. Dr. Gerd Gigerenzer ist Direktor des Harding-Zentrums für Risikokompetenz an der Universität Potsdam.

## Potenziale und Grenzen automatisierter Fehlerreduktion

### Welche Versprechen Systeme automatisierter Entscheidungen halten können und welche nicht

*Mit dem Fortschreiten der Digitalisierung und der stetig anwachsenden Datenverfügbarkeit steigt auch der Einsatz von automatisierten Entscheidungsalgorithmen. Ein typischer Anwendungsfall von automatisierten Entscheidungen in der öffentlichen Verwaltung ist die Bearbeitung von Anträgen. Die Familienkasse nutzt derzeit zum Beispiel erfolgreich Software zur Bild- und Texterkennung, um Kindergeldanträge schneller bearbeiten zu können. Systeme dieser Art sind attraktiv, nicht nur wegen ihres Potenzials zur Beschleunigung von Verwaltungsvorgängen und Entlastung von Mitarbeitern, sondern auch wegen ihres Potenzials zur Objektivierung von Entscheidungsvorgängen.*

In der Praxis sind diese Versprechen nicht immer so einfach einzulösen. Die eingesetzten Algorithmen werden oft zunächst mit historischen Daten angelernt. Das heißt, es können subjektive, möglicherweise fehlerhafte Entscheidungen aus der Vergangenheit erlernt und in die Zukunft fortgeschrieben werden. Das kann vor allem dann passieren, wenn sich gesellschaftliche Normen ändern, zum Beispiel das Verständnis darüber, welche gesellschaftlichen Gruppen besonders unterstützt werden sollen oder welche Charakteristika und Fähigkeiten schulische oder berufliche Erfolge vorhersagen. Das Training der Algorithmen kann aber auch dann scheitern, wenn für bestimmte gesellschaftliche Gruppen fehlerhafte oder unzureichende Daten vorliegen.

Für den erfolgreichen Einsatz automatisierter Entscheidungen sind deshalb vor allem zwei Aspekte von Bedeutung. Zum einen müssen die Ergebnisse von Entscheidungsalgorithmen immer wieder auf Fairness abgeklöpft und gegebenenfalls korrigiert werden. Dazu bedarf es in vielen Situationen zunächst eines gesellschaftlichen Diskurses darüber, welche Ziele erreicht werden sollen und welche Entscheidungen als gerecht angesehen werden. Weder Daten noch Algorithmen können uns Menschen diese Entscheidung abnehmen. Insbesondere dann nicht, wenn verschiedene Ziele nicht miteinander kompatibel sind. Zum Beispiel können nicht gleichzeitig alle ähnlich viel Unterstützung bekommen und die Bedürftigsten am meisten unterstützt werden. Zum anderen bedarf es einer genauen Betrachtung und eines genauen Verständnisses über die Prozesse, aus denen die Daten generiert werden, die zum Training der Algorithmen ver-

wendet werden. Fragen wie „Wer fehlt hier in meinen Daten?“, „Von welchen gesellschaftlichen Gruppen wissen wir zu wenig, um gute Vorhersagen zu treffen?“ oder auch „Messen meine Daten überhaupt das, was uns interessiert?“ sollten immer wieder aufs Neue gestellt werden.

Zeigen sich Lücken in den Daten oder Unschärfen in der Messung, ist das nicht das Ende der Fahnenstange. Aber es bedarf einer statistischen Nachbesserung, der Kombination verschiedener Datenquellen oder einer systematischen Nacherhebung, um die Qualität der Daten zu erhöhen. Damit dies möglich ist, muss an vielen Stellen neu über Datenschutz nachgedacht werden. Derzeit werden alle personenbezogenen Daten weitestgehend auf die gleiche Weise geschützt, unabhängig vom Kontext der Datenerhebung und der geplanten Datennutzung. Der Weitergabe von personenbezogenen Daten von einem behandelnden Arzt zum nächsten muss genauso aktiv zugestimmt werden wie der Weitergabe von Browser-Daten an Online-Werbeagenturen. In beiden Fällen obliegt die Entscheidung über die Nutzung den Individuen. Auch wenn diese Entscheidungsfreiheit ein hohes Gut ist und nicht leichtfertig aufgegeben werden sollte, kann sie doch zu ungewollten, negativen Konsequenzen führen. Zum Beispiel dann, wenn Gruppen am Rande der Gesellschaft aus Furcht oder aufgrund fehlenden Zugangs weniger Daten zur Verfügung stellen. In beiden Fällen vernachlässigen spätere, automatisierte Entscheidungen die spezifischen Lebensumstände dieser Gruppen, da beim Training Daten fehlten.



Frauke Kreuter

**Frauke Kreuter** ist Professorin für Statistik und Datenwissenschaft für die Sozial- und Geisteswissenschaften an der Ludwig-Maximilians-Universität München und Professorin am Joint Program in Survey Methodology an der University of Maryland und Mitbegründerin und Co-Direktorin der Data Science Centers an der University of Maryland (USA) und Mannheim (Deutschland). Sie ist Fellow der International Statistical Association und der American Statistical Association. In 2020 erhielt sie den Warren Mitofsky Innovators Award der American Association for Public Opinion Research. Neben ihrer akademischen Arbeit ist Dr. Kreuter Gründerin des International Program for Survey and Data Science, das als Reaktion auf die steigende Nachfrage von Forschern und Praktikern nach geeigneten Methoden und Werkzeugen für ein sich veränderndes Datenumfeld entwickelt wurde; Mitbegründerin der Coleridge Initiative, deren Ziel es ist, evidenzbasierte Politikgestaltung zu beschleunigen, indem ein effizienter, effektiver und sicherer Zugang zu sensiblen Daten über Gesellschaft und Wirtschaft ermöglicht wird; und Mitbegründerin des deutschsprachigen Podcasts digdeep.de.



## Digitale Gesellschaft zwischen Herrschaft und Innovation

Heute bildet der digitale, globale Kapitalismus den politökonomischen Rahmen gesellschaftlichen Wandels. Er ist gekennzeichnet durch Wachstumskrisen, ein spezifisches Akkumulationsmuster von Macht und die doppelte Enteignung von Arbeit. Kann soziale Innovation aus den Konflikten um den digitalen Kapitalismus entstehen?

Die Kommerzialisierung des Internet seit den 1990er Jahren ist untrennbar mit dem Aufstieg einer spezifischen Kapitalsorte bzw. einer spezifischen Klasse von Investor:innen verbunden: privatem Risikokapital. Heutige Leitunternehmen des kommerziellen Internets, wie Google, Apple, Facebook, Amazon, Alibaba oder Tencent expandierten in der Folge rasant. Das lässt sich nicht nur an deren Bewertungen ablesen. Auch ihr Vordringen in immer neue ökonomische Felder – von klassischen Unterhaltungsindustrien über urbane Infrastrukturen und industrielle Anwendungen bis in den Gesundheitsbereich – verdeutlicht die expansive Logik der Technologiebranche. Diese speist sich nicht zuletzt aus der Motivation, die immensen Cash-Reserven der mittlerweile führenden Unternehmen lukrativ anzulegen: Google verfügte zum Ende des Finanzjahres 2019 über Rücklagen in Höhe von 120 Milliarden US-Dollar, Microsoft über 134 Milliarden und Apple gar über 206 Milliarden. Zum Vergleich: Daimler verzeichnete zur gleichen Zeit finanzielle Mittel in Höhe von rund 23,9 Milliarden, Volkswagen 23,1 Milliarden und BASF 1,2 Milliarden US-Dollar.



Stellt man sich nun die Frage, wofür all das Geld genau verwendet wird, welche Strategien der Umgestaltung die betreffenden Firmen verfolgen, dann sieht man vor allem zweierlei: Marktkontrolle und die Übernahme basaler Infrastrukturen. Firmen wie Google, Apple, Facebook oder Amazon werden oft als Plattform-Unternehmen bezeichnet. Nach geläufiger Definition sind Plattformen intermediäre digitale Infrastrukturen, die es Akteuren erlauben, miteinander zu interagieren. Handelt es sich bei diesen Interaktionen um ökonomische Tauschprozesse, haben wir es mit digitalen Marktplätzen zu tun, auf denen Produzent:innen, Dienstleister:innen, Konsument:innen und Werbetreibende miteinander Handel treiben. Die Plattformen erwirtschaften Profite durch die Besteuerung von Marktteilnahme. Wer Zugang zu Nachfrage möchte, muss, je nach Bereich, zwischen 20 bis zu 90 % der eigenen Umsätze an die Plattformbetreiber abführen. Dieses Geld fehlt nicht nur bei den Produzent:innen. Die Profite der Plattformen lassen sich auch als Renten beschreiben, weil die Pflege und der Erhalt der digitalen Handels- und Infrastrukturmonopole im Vergleich zu den erzielten Gewinnen kaum Kosten produziert. Plattformen entziehen der Wirtschaft also Werte durch dieses Akkumulationsmuster, die auf den aufgeblähten Finanzmärkten landen (Abbildung 1).

Plattformen bestimmen:

- Wer welche Daten liefert oder erhält (Überwachung)
- Welche Anbieter am Markt zu finden sind (Zugangskontrolle)
- Welche Preise verlangt werden können (Preiskontrolle)
- Wie Leistungen erbracht werden (Leistungskontrolle)
- Sie repräsentieren ein bisher ungekanntes Ausmaß wirtschaftlicher Macht.

### Öffentliche Infrastrukturen

Durch die Übernahme der Marktfunktion etablieren digitale Leitunternehmen aber nicht nur Marktmacht, sondern auch infrastrukturelle Macht. Anders gesagt: Ohne sie geht nichts mehr. So hat insbesondere die laufende Pandemie deutlich gemacht, dass die privatisierten Digitalmärkte zu einem fundamentalen Rückgrat unseres Marktgeschehens geworden sind. Amazon beispielsweise wurde zeitweise zum wichtigsten Anlaufpunkt für Konsum überhaupt und war gleichzeitig gezwungen, Entscheidungen über Versorgungsfragen zu treffen: Welche Güter sollen prioritär behandelt werden? Welche Waren werden noch angenommen bzw. versendet? Wie teuer dürfen Desinfektionsmittel und Mund-Nasenschutz in einer Situation knappen Angebots und gigantischer Nachfrage sein? Das sind essentielle Versorgungsfragen der digitalen Gesellschaft, die außerhalb jeder effektiven demokratischen Kontrolle stehen.

Infrastrukturelle Macht wird zunehmend auch im Bereich der industriellen Wertschöpfung und im Bereich der öffentlichen Güter erkennbar. Nehmen wir urbane Mobilitätsdienstleistungen – eigentlich ein Heimspiel öffentlicher Unternehmen mit Bus und Bahn:

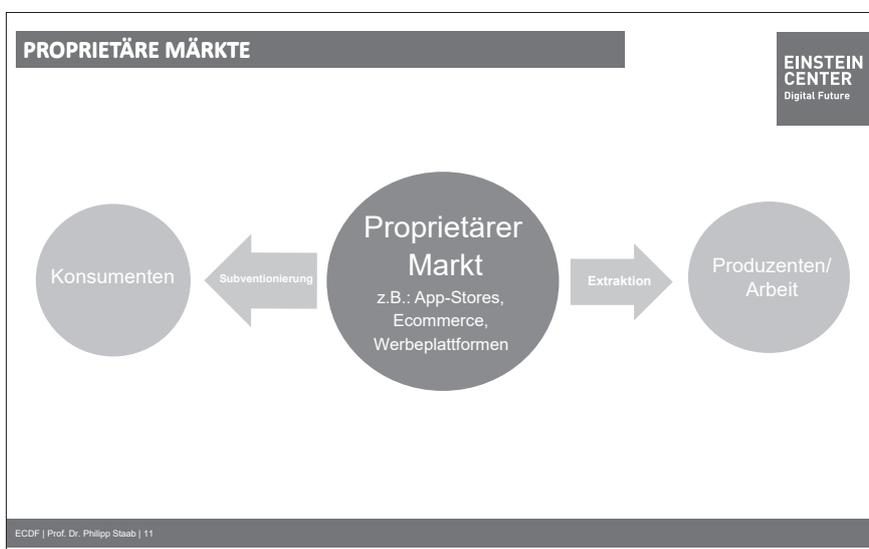


Abbildung 1: Proprietäre Märkte

Wenn Leihfahrräder chinesischer Anbieter, wie in den Jahren 2017/18, zu Tausenden in deutschen Innenstädten abgeladen werden oder das Gleiche zwei Jahre später mit elektrischen Tretrollern geschieht, stehen dahinter nicht nur die Logiken überschüssigen Kapitals. Es geht mittlerweile um die Umformung urbaner Mobilität im großen Stil – darum, wer den Markt für geteilte städtische Mobilität kontrolliert. Die größten Chancen darauf, die dominante Plattform für urbane Mobilität zu liefern, hat wohl Google. Stück für Stück hat das Unternehmen den hauseigenen Kartendienst Maps um diverse Mobilitätsdienstleistungen erweitert: Hier können Sie in Berlin etwa Leihautos, E-Scooter, oder Taxi-Dienste buchen (mit den Vermittlungen verdient Google natürlich Geld).

Das Rückgrat von Maps als Meta-Plattform urbaner Mobilität bildet dabei ausgerechnet der ÖPNV. Nutzer:innen können Fahrzeiten und Verbindungen in Echtzeit einsehen, weil zahlreiche Verkehrsverbünde Google ihre Verkehrsdaten überlassen. Was Google hier gewinnt, wird der demokratischen Kontrolle entzogen – was zu einem erheblichen Steuerungsdefizit führt. Da es bei den privaten Plattformen um Profit und nicht mehr um Versorgungssicherheit geht, haben sie einen hohen Anreiz beispielsweise Taxi-Fahrten, an denen sie Geld verdienen, gegenüber öffentlichen Verkehrsmitteln zu fördern.

Ressourcenverschwendung ist Programm: So lange genug Geld zum Verbrennen da ist, spielt es beispielsweise keine Rolle, dass E-Scooter-Anbieter jährlich ein Drittel ihrer Flotte durch Vandalismus und mangelnde Wartung verlieren. Die digitale Privatisierung verschlimmert so auch den ökologischen Fußabdruck der sogenannten Smart City, indem demokratische Kontrolle über öffentliche Güter verloren geht. Öffentliche Alternativen zu den privaten Plattformen kommen nicht vom Fleck, weil die öffentlichen Verkehrsunternehmen zwar Google mit ihren Daten füttern, selbst aber kaum etwas zurückbekommen.

## Konflikte um den digitalen Kapitalismus

Warum machen Firmen, wie Amazon oder Zalando immer wieder Schlagzeilen mit grenzwertigen Strategien der Arbeitskontrolle? Das Tracking von Konsument:innen spiegelt sich in der zunehmend digitalen Überwachung von Beschäftigten wider und die Gestaltung von Betriebssoftware durch

DOPPELTE ENTEIGNUNG VON ARBEIT



- Mechanismus 2: **Algorithmisches Management** als neues Leitparadigma der Arbeitssteuerung
- Herrschaftsmechanismen auf proprietären Märkten... übersetzen sich als algorithmisches Management auf den Faktor Arbeit
  - Informationskontrolle → Tracking
  - Zugangskontrolle → Rating
  - Preiskontrolle → Scoring
  - Leistungskontrolle → Informationsasymmetrien
- Ungleichheit: Instrument zur Exklusion (Zugangskontrolle), Lohnunterdrückung (Preiskontrolle) and Intensivierung von Arbeit (Leistungskontrolle)

ECDF | Prof. Dr. Philipp Staab | 17




Abbildung 2: Doppelte Enteignung von Arbeit

BLOCKIERTER KONFLIKT...



- Nicht-Unterscheidbarkeit von Konfliktgruppen – Blockierter Konflikt
- Aber: Es gibt Konflikte um den digitalen Kapitalismus!
  - Europäischer Rahmen digitaler Rechte (DSGVO)
  - Neue Industriepolitik (e.g. Gaia-X, Airbus of everything)
  - Digitale Geopolitik (‘Digitale Souveränität’, e.g. European Semiconductors)
  - Vor allem aber: **Politisches Marktdesign** (DMA/DAS, Data Act, Data Governance ACT,...)
- Leitbegriff: „Digitale Souveränität“

ECDF | Prof. Dr. Philipp Staab | 22




Abbildung 3: Blockierter Konflikt

ABER...



- Wessen Souveränität?
  - Konsumenten statt Arbeitenden (z.B. Datenschutz)
  - Unternehmen statt öffentlicher Akteure (Gaia-X)
  - Private statt öffentliche Infrastrukturen (z.B. Mobilität, Gesundheit,...)
  - Politisches Marktdesign als Versuch eines gegenhegemonialen Neoliberalismus (Dominanz von Marktsteuerung, Konkurrenz, Wachstum)
- Konsequenz: Sozialer Konflikt als reiner Elitenkonflikt

ECDF | Prof. Dr. Philipp Staab | 24




Abbildung 4: Um wessen Souveränität geht es im neoliberalen Marktdesign?





**ÖKOLOGISCHES MARKTDESIGN**

EINSTEIN CENTER  
Digital Future

- Stattdessen...
  - ...Nachhaltigkeitsziele direkt im politisches Marktdesign verankern
  - ...vom Kapitalismus der Personendaten zur Ökonomie der Umweltdaten
  - ...dadurch echte Kosten in Märkten einpreisen und
  - ...neue zirkuläre Wirtschaftsweisen ermöglichen

ECDF | Prof. Dr. Philipp Staab | 27

Abbildung 5: Ökologisches Marktdesign

dels groß sind. Von der verstärkten Extraktion aus dem Produktionsfaktor Arbeit profitieren sowohl die Konsument:innen als auch das Kapital, und das blockiert den Konflikt. Er wird zu einem Elitenkonflikt mit unverändert neoliberalen Zielen wie Privatisierung und bessere Wettbewerbsbedingungen (Abbildung 3).

Für wen werden die digitalen Märkte gestaltet? Und ist das ein Design, das weiterhilft (Abbildung 4)?

Ein alternatives Marktdesign sollte politisch sein statt privatisiert und andere Leitbilder haben: Bürger:innen statt Konsument:innen, Kreislaufwirtschaft und ökologischer Wandel auf der Basis von Umweltdaten statt personenbezogenen Daten, öffentliche Güter und kommunale Plattformen statt Konsumentenmärkten (Abbildung 5).

**DAGEGEN**

EINSTEIN CENTER  
Digital Future

### Öffentliche Plattformen als Gegenmodell – the „public stack“

Öffentliche Trägerschaft und Kontrolle (ggf. private Leistungserfüllung mit engmaschiger Regulierung über öffentliche Vergabe)

Interface	Public Interest Design
Algorithmen	Open-Source
Server	Datentreuhänder
Schnittstellen	Interoperabilität

ECDF | Prof. Dr. Philipp Staab | 30

Abbildung 6: Plattform-Kommunalismus

So ließen sich die bestehenden öffentlichen Initiativen in der digitalen Daseinsvorsorge erweitern und aus dem Zangengriff privater Plattform-Unternehmen und Software-Zulieferer befreien, das Gemeinwohl durch Kreislaufwirtschaft und Nachhaltigkeit verfolgen und externe Kosten internalisieren, so dass die Preise die Wahrheit sagen. Die Voraussetzungen sind nicht trivial aber umsetzbar (Abbildung 6).

### Wie kann das gelingen?

Plattform-Kommunalismus kann gelingen, weil kommunale Anbieter durch ihre lokalen Netze und ihr lokales Wissen Wettbewerbsvorteile haben. Voraussetzungen sind, dass demokratische Datenverwaltung und transparente Algorithmen den Bürger:innen wieder Vertrauen geben, das sie in partizipative Entscheidungsverfahren einbringen können. Dazu gehört, dass die digitale Zivilgesellschaft (beispielsweise CCC, FfF, Verbraucherschützer:innen, fsfe, ...) als Ressource wahrgenommen und genutzt wird, und dass kooperative Open Source-Entwicklungen den Lock-in durch Software-Hersteller durchbrechen.

externe Anbieter:innen und betriebsinterne Manager:innen bestimmt die Handlungsspielräume in digitalisierten Arbeitssituationen (Abbildung 2).

Dabei bleiben die größeren Themen akut – finanzielle Ungleichgewichte, Markt- und Infrastrukturmacht, digitale Privatisierung und algorithmische Arbeitskontrolle. Es geht daher um die Politisierung ungleicher Machtressourcen – etwa im Sinne einer Industriepolitik für die Vielen, statt eines digitalen Kapitalismus für die wenigen. Es sind Themen, die zusammenhängen, nicht auf den Arbeitsprozess beschränkt sind und die Transformation des Kapitalismus als Ganzes betreffen. Kann aus den Konflikten um diese Themen soziale Innovation entstehen? Trotz partieller Mobilisierungen ist eine breite soziale Bewegung gegen den digitalen Kapitalismus unwahrscheinlich. – Warum ist das so? Vielleicht weil wir bei Amazon kaufen, obwohl wir längst wissen, dass die Arbeitsbedingungen miserabel und der ökologische Fußabdruck des Versandhan-



**Philipp Staab**, geboren 1983 in Nürnberg, ist Professor für die Soziologie der Zukunft der Arbeit an der Humboldt-Universität zu Berlin und am Einstein Center Digital Future. 2019 erschien sein Buch *Digitaler Kapitalismus. Markt und Herrschaft in der Ökonomie der Unknappheit*.

### Philipp Staab

## Voreingenommenheit im Gehirn und im Algorithmus

Was ist überhaupt eine Voreingenommenheit? In der Alltagssprache bedeutet voreingenommen zu sein, dass man eine vorgefertigte Meinung hat, eine starke Präferenz für oder gegen etwas; sei es eine Idee, eine Ideologie, eine Person oder Personengruppe. Häufig führen solche Voreingenommenheiten, die bewusst oder unbewusst sein können, zu diskriminierendem Verhalten. Im kognitionspsychologischen Kontext hat der Begriff Voreingenommenheit eine etwas andere Bedeutung: nämlich unbewusste, systematische Fehler beim Wahrnehmen, Erinnern, Denken und Urteilen. Solche kognitiven Verzerrungen sind universal, unabhängig von Bildungsgrad oder Kultur; sie sind zudem äußerst hartnäckig und beeinflussen uns, auch wenn wir davon wissen und versuchen sie zu kompensieren.

Es gibt eine reiche Vielfalt an kognitiven Voreingenommenheiten.<sup>1</sup> Für den Vergleich zwischen den Fehlern menschlicher Gehirne und lernender Algorithmen ist das wichtigste Phänomen die Repräsentativitäts-Heuristik. Diese Heuristik beschreibt die Erkenntnis, dass Entscheidungen über die Wahrscheinlichkeit von Ereignissen dadurch beeinflusst werden, wie sehr sie einem Prototyp entsprechen. Die Repräsentativitäts-Heuristik ist die Ursache für sehr viele Denkfehler, zum Beispiel der Spielerfehlschluss, der Verknüpfungsfehlschluss und der Prävalenzfehler. Letzterer lässt sich durch ein einfaches Denkeperiment verdeutlichen:

### Szenario

Andi ist ein schmaler Brillenträger mit ruhiger Stimme. Er hat eine Vorliebe für Ordnung und sein Lieblingskomponist ist Khachaturian.

Was ist wahrscheinlicher?

1. Andi ist Universitätsbibliothekar
2. Andi ist LKW-Fahrer

Unser instinktives Urteil ist, dass Andi sicherlich Bibliothekar ist – weil die Beschreibung doch viel besser zu unserer Vorstellung eines Bibliothekars passt. Auch wenn wir etwas von Statistik verstehen, und uns ein Bild machen, wie viele LKW-Fahrer es im Vergleich zu Universitätsbibliothekaren gibt, kostet es uns Mühe, das instinktive Urteil zu überwinden. Diese Wechselwirkung zwischen schnellem, instinktivem und langsamem, mühseligem Denken wurde gründlich und umfassend von Tversky und Kahneman untersucht (siehe Kahneman 2011 für eine zugängliche und unterhaltsame Zusammenfassung ihrer Recherchen).

Dieses Phänomen entsteht nicht nur wegen gesellschaftlicher Vorurteile, sondern auch wegen der Hardware des Gehirns. Wahrscheinlichkeit zu berechnen, so wie es der Bayes'sche Satz verlangt, um über den Beruf von Andi zu entscheiden, ist keine natürliche Operation für Populationen von Nervenzellen, die über exzitatorische (erregende) oder inhibitorische (hemmende) Synapsen verbunden sind. Was das Gehirn allerdings sehr gut kann, ist Konzepte assoziieren (siehe Abbildung 1). Die stärkeren Verbindungen zwischen den Eigenschaften von Andi und ‚Bibliothekar‘ im Vergleich mit ‚LKW-Fahrer‘ führen dazu, dass ‚Bibliothekar‘ intensiver angeregt wird. Diese intensivere Aktivität wird vom Gehirn als höhere Wahrscheinlichkeit interpretiert, wobei die Häufigkeit der beiden Berufsgruppen nicht berück-

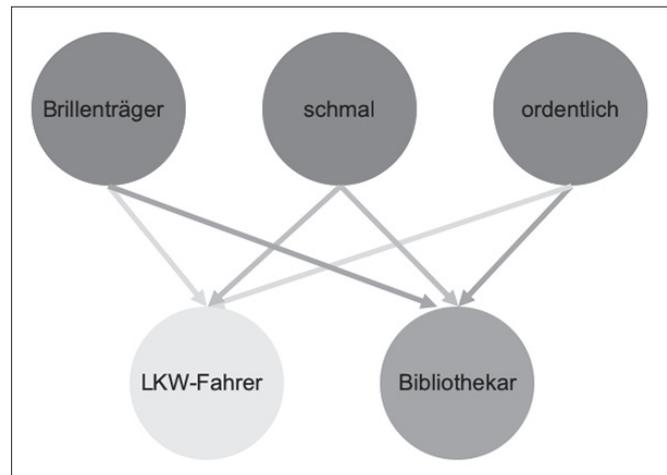


Abbildung 1: Assoziative Arbeitsweise des Gehirns. Die neuronalen Populationen, welche die Eigenschaften von Andi beschreiben, sind stärker mit Bibliothekar als mit LKW-Fahrer assoziiert und regen deshalb ersteres stärker an.

sichtigt wurde. Somit ist das Gehirn auch in Abwesenheit von Vorurteilen für solche Prävalenzfehler anfällig.

Es ist einfach zu sehen, wie die Repräsentativitäts-Heuristik unbewusst zu diskriminierenden menschlichen Urteilen führen kann. Wie kommt es zur Diskriminierung bei Algorithmen? Du et al. (2020) führen hierzu zwei Kategorien ein: 1) Diskriminierung bezüglich des *Ergebnisses* einer Klassifizierung, und 2) Diskriminierung bezüglich der *Qualität* der Klassifizierung. Die erste Kategorie kann weiter in 1a) Diskriminierung mittels *Input*, und 1b) Diskriminierung mittels *Repräsentation* unterteilt werden.

*Diskriminierung mittels Input* bedeutet, dass anhand der Trainingsdaten auf eine sensible Kategorie, beispielsweise eine gesetzlich geschützte, geschlossen wird. Obwohl solche Kategorien (wie zum Beispiel Geschlecht, ethnische Herkunft, usw.) in vielen Anwendungen nicht explizit angegeben werden, gibt es häufig korrelierte Eigenschaften (wie Postleitzahl, Name, Hobbys, Körpergröße, ...). Diese sogenannten Proxy-Variablen sind besonders dann problematisch, wenn die Evaluationsfunktion durch menschliche Voreingenommenheit beeinflusst wurde. Ein mögliches Szenario ist ein KI-Werkzeug, um Lebensläufe zu evaluieren, bei dem die positiven Beispiele aus den Trainingsdaten die Kandidaten sind, die früher erfolgreich in der Firma aufgenommen wurden (siehe <https://tinyurl.com/r8sxx8xy>). Hatte die Firma historisch überwiegend Männer eingestellt, so lernt der Algorithmus, die Proxy-Variablen für Geschlecht zu identifizieren und in direkter Analogie zur Repräsentativitäts-Heuristik





die Lebensläufe männlicher Kandidaten an Hand dieser Variablen positiver zu evaluieren als die der Kandidatinnen. In den letzten Jahren konnten gehäuft Benachteiligungen von Minderheiten nachgewiesen werden, nicht nur bei der Rekrutierung, sondern auch in diversen und fundamentalen Lebensbereichen wie Gesundheit, Sicherheit, Zugang zu Krediten und der Behandlung im juristischen System. Diese Ergebnisse verdeutlichen, dass KI-Werkzeuge nicht dort naiv eingesetzt werden dürfen, wo historische Diskriminierungen in einer *Black Box* widergespiegelt und verstärkt werden können.

*Diskriminierung mittels Repräsentation* bedeutet, dass die sensible Kategorie nicht im Input selber zu finden ist (entweder direkt oder als Proxy), sondern erst in tieferen Schichten eines Deep-Learning Netzwerks identifiziert werden kann. Dieses Problem tritt insbesondere bei Image-Daten auf; eine häufige Ursache dafür ist eine ungleichmäßige Repräsentation bei den Trainingsdaten, wenn zum Beispiel die Gruppe der positiven Beispiele mehr männliche als weibliche aufweist. Da viele Netzwerke durch Bilder aus dem Internet trainiert werden, ist das durchaus problematisch. Um sich selbst davon zu überzeugen, kann man „Consultant Doctor“ und „Nurse“ (die Begriffe auf Englisch für Facharzt/ärztin und Krankenpfleger:in sind geschlechtsneutral) in Google-Suchen angeben, und die Anzahl von Männern und Frauen zählen (zur Kontrolle die Information: in Deutschland sind 40 % der Ärzt:innen und 80 % der Krankenpfleger:innen weiblich). Natürlich geht es bei Diskriminierung nicht nur um das Geschlecht. Wenn man bei den obigen Suchergebnissen nach Repräsentationen von z. B. schwarzen Frauen, Frauen über 50, oder Menschen mit Behinderung sucht, würde man, allein nach den Bildern zu beurteilen, zu dem Schluss kommen, dass solche Menschen wohl keine Fachärzte sein können. Algorithmen, die mit solchen Datensätzen trainiert werden, werden zwangsläufig voreingenommen, da sie nicht über das strukturelle Hintergrundwissen verfügen, um Repräsentations-Missstände der Trainingsdaten zu kompensieren.

Auf *Diskriminierung bezüglich der Qualität der Klassifizierung* gehe ich nur kurz ein. Es heißt, dass ein bestimmtes Klassifizierungstool besser für eine demografische Gruppe funktioniert als für eine andere. Zum Beispiel können viele gängige Gesichtserkennungsanwendungen die Gesichter von Menschen mit heller Hautfarbe viel besser als die mit dunkler Hautfarbe erkennen und männliche Gesichter deutlich besser als weibliche. Der Unterschied im Identifikationserfolg zwischen weißen Männern und schwarzen Frauen kann bis zu 34 % betragen (Buolamwhini et al., 2018; Zou & Schiebinger, 2018). Dieses Problem ist normalerweise auf ungleiche Verteilungen in den *Trainingsdaten*

zurückzuführen. Als Beispiel: im Imagenet Dataset 2012<sup>2</sup>, welches als Basis für sehr viele Image-Klassifizierungs-Algorithmen dient, zeigen nur 41,6 % der Bilder von Menschen eine Frau; zudem gibt es praktisch keine Menschen über 60. In diesem Szenario passiert das *Parameterfitting* automatisch zugunsten der Mehrheitskategorie. Außerdem gibt es zwangsläufig mehr Variabilität bei den Minderheitskategorien, was die Performanz des Algorithmus in diesen Fällen reduziert.

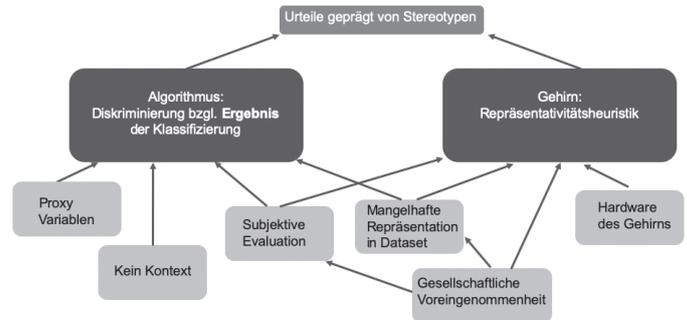


Abbildung 2: Die gemeinsamen und unterschiedlichen Ursachen diskriminierender Urteile beim Gehirn und beim Algorithmus

Insgesamt kann man argumentieren, dass Diskriminierung bezüglich des Ergebnisses einer Klassifizierung ein analoges Phänomen zur Repräsentativitäts-Heuristik ist. Sie haben ähnliche Effekte, nämlich Urteile, die von Stereotypen geprägt sind, und Gemeinsamkeiten bei ihren Ursachen, obgleich sie auch eigene Faktoren haben. Die Zusammenhänge sind (unvollständig) in Abbildung 2 illustriert.

Diese Erkenntnis heißt weder, dass wir diskriminierende Ergebnisse einfach hinnehmen, noch, dass wir auf den Einsatz von KI-Algorithmen verzichten müssen. In der Tat gibt es eine Reihe von technischen Ansätzen, um die Voreingenommenheit eines Algorithmus zu reduzieren. Ich werde hier ein paar davon kurz schildern:

- Erstens, Trainingsdaten können angepasst werden, um die Repräsentation unterschiedlicher Gruppen auszugleichen. Yang et al. (2020) haben dies mit großer Wirkung bei dem ImageNet-DataSet durchgeführt.
- Zweitens, um Proxy-Variablen zu vermeiden, kann man das Netzwerk analysieren, um die Variablen der Input-Daten zu identifizieren, die besonders wichtig für die Klassifizierung



## Abigail Morrison

Prof. Dr. **Abigail Morrison** ist Forscherin in Computational Neuroscience am Forschungszentrum Jülich und an der RWTH Aachen. Ihr wissenschaftlicher Fokus ist Lernen und Informationsverarbeitung in puls-gekoppelten neuronalen Netzwerken, mit weiteren Interessen an den Schnittstellen zwischen Neurowissenschaften und künstlicher Intelligenz und am Einsatz von Hochleistungsrechnern in der Neurowissenschaft.



sind. Im nächsten Schritt kann man eine Korrelationsanalyse durchführen, um mögliche Zusammenhänge zwischen den so gefundenen Variablen und Mitgliedschaft in einer gesetzlich geschützten Kategorie zu identifizieren. Besteht so eine Korrelation, so hat man eine Proxy-Variablen gefunden, die aus den Daten ausgeschlossen werden kann.

- Drittens, um Diskriminierung mittels Repräsentation zu kontern, steht die *Concept-Activation-Vector*-Technik zur Verfügung (Kim et al., 2018). Hier untersucht man, ob das Netzwerk indirekt geschützte Kategorien mitlernt, und verwendet diese Information als Trainingssignal, um diesem Lernen entgegenzuwirken.

Selbstverständlich verlangen diese Ansätze mehr Reflektion, mehr Arbeit und mehr Zeit als einfach mal schnell ein Netzwerk zu trainieren. Dennoch haben Algorithmen den großen Vorteil, im Gegensatz zum menschlichen Gehirn, dass sie technische Systeme sind, die beliebig auseinandergenommen und inspiziert werden können, so dass wir wirksame technische Lösungen erarbeiten können. Daher besteht die Hoffnung, dass der richtige, reflektierte Einsatz von KI Diskriminierung in der Gesellschaft reduziert – allerdings nur, wenn wir auf jeder Ebene darauf bestehen, dass KI-Werkzeuge diesbezüglich kritisch geprüft und unabhängig validiert werden.

## Referenzen

Buolamwini J, Gebru T (2018) Gender shades: Intersectional accuracy disparities in commercial gender classification. In Conference on fairness, accountability and transparency (pp. 77-91). PMLR.

Du M, Yang F, Zou N, Hu X (2020) Fairness in Deep Learning: A Computational Perspective. IEEE Intelligent Systems.

Kahneman D (2011) Thinking, Fast and Slow. Macmillan. ISBN 978-1-4299-6935-2

Kim B, Wattenberg M, Gilmer J, Cai C, Wexler J, Viegas F, Sayres R (2018) Interpretability beyond feature attribution: Quantitative testing with concept activation vectors (TCAV). International Conference on Machine Learning (ICML)

Yang K, Qinami K, Fei-Fei L, Deng J, Russakovsky O (2020) Towards Fairer Datasets: Filtering and Balancing the Distribution of the People Subtree in the ImageNet Hierarchy. Conference on Fairness, Accountability and Transparency (FAT\*)

Zou J, Schiebinger L (2018) AI can be sexist and racist—it's time to make it fair. Nature 559 (pp. 324-326)

## Anmerkungen

- 1 Siehe [https://de.wikipedia.org/wiki/Liste\\_kognitiver\\_Verzerrungen\\_für\\_eine\\_ausführliche\\_Liste](https://de.wikipedia.org/wiki/Liste_kognitiver_Verzerrungen_für_eine_ausführliche_Liste).
- 2 <https://www.image-net.org/index.php>



Silja Samerski

# Kontrollierte Selbstbestimmung

## Wie Überwachung im Gesundheitswesen unter die Haut geht

*Die Digitalisierung des Gesundheitswesens verbessert die Versorgung und verhilft Patient:innen zu mehr Selbstbestimmung, so versprechen IT-Unternehmen, Krankenkassen und Expertengremien. Die elektronische Patientenakte (ePA) soll beispielsweise nicht nur Ärzt:innen, sondern auch den Patient:innen selbst einen besseren Überblick u. a. über Befunde, Arztbriefe und Abrechnungsdaten ermöglichen. Digitale Angebote wie Gesundheitsportale, virtuelle Gesundheitsassistenten und Symptom-Checker sollen zudem die Gesundheitskompetenz der Bevölkerung und damit auch die Patientensouveränität erhöhen (Sachverständigenrat Gesundheit 2021; Techniker-Krankenkasse). Wird die lang geforderte Patienten-Selbstbestimmung im Gesundheitswesen mithilfe der Digitalisierung endlich Wirklichkeit?*

Es gibt gute Gründe, diesem Versprechen gegenüber skeptisch zu sein. Bereits heute zeichnet sich ab, dass die viel beschworene Datensouveränität von Patient:innen im digitalisierten Gesundheitswesen kein großes Gewicht hat. Angesichts des Datenhungers von Forschung und Industrie haben zahlreiche Gremien und Experten das Recht auf informationelle Selbstbestimmung bereits für veraltet erklärt und neue Datenschutzkonzepte vorgelegt, die Big Data nicht behindern (Deutscher Ethikrat 2017, SVR Gesundheit 2021). Unter dem Banner *Sharing is caring*, oder noch drastischer: *Datenschutz tötet* arbeiten Wissenschaftler:innen und Digitalunternehmen an der Aufweichung von Datenschutz und Datensouveränität. Bisher ist vorgesehen, dass Patient:innen selbst darüber entscheiden können, welche Daten sie in der ePA speichern lassen und mit welchen Ärzt:innen sie diese teilen möchten. Werden die begehrten Gesundheitsdaten jedoch erst in einer Datenbank gespeichert, wird es schwierig sein, den gläsernen Patienten langfristig zu verhindern. Der Sachverständigenrat (SVR)-Gesundheit schlägt in seinem aktuellen Gutachten (2021) bereits vor, die ePA allen Men-

schen qua Geburt zuzuweisen und dort alle medizinischen Daten automatisch zu speichern. Patienten hätten dann nur noch das Recht, bestimmte Dokumente und Informationen zu „verschatten“ – in Estland beispielsweise ist ein solches Opt-out-System realisiert. Auch die Corona-Krise zeigt, wie groß die Bereitschaft ist, Datenschutz und Persönlichkeitsrechte angesichts von Gesundheitsbedrohungen und Gesundheitsverheißungen hintanzustellen. Binnen kürzester Zeit ist es normal geworden, sich im Alltag mit sensiblen Gesundheitsdaten wie dem Immunitätsstatus auszuweisen, um Zugang zum Restaurant oder Theater zu erhalten. Die Infrastruktur und die Gewöhnung, die in Krisenzeiten geschaffen wurden, sollen nach der Krise nicht abgebaut, sondern ausgebaut werden: Der französische Rüstungskonzern *Thales* hat beispielsweise vor, die Impfpässe zu einer digitalen ID weiterzuentwickeln: „So-called digital *vaccination passports* will play a key role in enabling citizens to access all manner of services and will act as a precursor to the rollout of mobile digital ID“ so ist auf der Webseite von Thales zu lesen (Theyras 2021).

## Verhaltenssteuerung durch Information

Im digitalisierten Gesundheitswesen bedroht jedoch nicht nur die Aushöhlung des Datenschutzes die Selbstbestimmung, sondern auch eine Verkehrung dessen, was Selbstbestimmung bislang bedeutet hat. Patientenautonomie, Patientensouveränität und die informierte Entscheidung sind zentrale Schlagworte im Gesundheitswesen. Sie stehen jedoch weniger für Freiheitsrechte, sondern in erster Linie für ein umfassendes Erziehungsprojekt. Im Gesundheitswesen ist Selbstbestimmung an Voraussetzungen geknüpft: Es gelten nur diejenigen als selbstbestimmt, die in den Augen von Experten als kompetent genug gelten, eigene Entscheidungen in Sachen Gesundheit zu treffen. Ziel der *Patientensouveränität* ist nämlich nicht die Emanzipation von ärztlichem Paternalismus, sondern die Anpassung von Patient:innen an die Erfordernisse des Gesundheitssystems. Der Sachverständigenrat Gesundheit nennt das im Gutachten von 2000/2001 „Optimierung des Nutzerverhaltens durch Kompetenz und Partizipation“. Was Optimierung des Nutzerverhaltens meint, erklärt der einleitende Satz:

*„Der Rat erkennt in Kompetenz und Partizipation die Schlüsselqualitäten des Nutzers, die einen wesentlichen Einfluss auf Prozess- und Ergebnisqualität der Leistungen und Wirtschaftlichkeit des gesamten Systems ausüben“ (SVR Gesundheit 2000/20001, 40).*

Pointiert zusammengefasst: Patient:innen sollen aktiv eingebunden werden, damit das System besser läuft. Hintergrund dafür ist u. a. die sogenannte Ökonomisierung des Gesundheitssystems, die dazu geführt hat, dass Patient:innen nicht mehr als „Leidende“, sondern wie auf jedem Markt als nachfragende Konsument:innen verstanden werden. Die Empfehlungen des Sachverständigenrates lauten daher, die „eigenständige Entscheidung des Patienten“ zu fördern – aber immer nur im Zusammenhang mit Erziehungsmaßnahmen: Ausdrücklich empfiehlt der Rat „Ausbau und Optimierung der vorhandenen Ansätze der Krankenkassen zur Versicherteninformation, Aufklärung, Beratung und Schulung“ (SVR Gesundheit 2003, 152). Patient:innen sollen für ihre neue Rolle also umfassend präpariert werden, damit sie von ihrer Freiheit den richtigen, nämlich systemkompatiblen Gebrauch machen. Ein Bertelsmann-Gutachten macht die Mittel-Zweck-Relation zwischen Schulung bzw. Information und *Verhalten* noch deutlicher:

*„Die Qualitätssicherung für Informationen (muss) sich nicht nur um die Angebote kümmern, sondern auch darum, ob, wie und welche Informationen Verhalten modifizieren. Die gewonnenen Erkenntnisse müssen dann in einer zeitgemäßen Konzeption von Gesundheitsbildung berücksichtigt werden“ (Bertelsmann/Universität Bremen 2006, 52).*

Es wird deutlich, dass Information heute im Gesundheitswesen als Mittel zur Verhaltenssteuerung dient – und nicht etwa dazu, dass sich Menschen ein eigenes Urteil bilden. Auch hier hat die Corona-Krise einen bestehenden Konflikt verschärft, nämlich die Auseinandersetzung um die Frage, was glaubwürdige und gute Information ist, aus welchen Quellen sie kommt und welchen Status abweichende Ansichten und Kritik haben. Im Internet und in den sozialen Medien ist mit Beginn der Corona-Krise

ein regelrechter *Informationskrieg* entbrannt. Die WHO hat im März 2020 die Pandemie ausgerufen, und drei Monate später erklärte sie die „Infodemie“ zum nächsten großen Gesundheitsproblem, also die „unüberschaubare Menge an Informationen“ (WHO 2020) zum Thema Corona. Sie forderte Staaten und Organisationen dazu auf, „ein unkontrolliertes Wuchern von Desinformation und Fehlinformation zu verhindern“. Seither löschen Digitalkonzerne wie Google oder Facebook diejenigen Kanäle, Seiten und Videos, deren Inhalte nicht zu behördlich genehmigten Narrativen passen. Selbst das *British Medical Journal*, eine der renommiertesten internationalen medizinischen Fachzeitschriften, wurde bereits Opfer von Facebooks „Fakten-Checkern“ (BMJ 2021, 375).

## Die alltägliche Überwachung im Namen der Gesundheit

### Die Umkehr der Unschuldsvermutung

In der Corona-Krise wurde nicht nur das Internet und die Informationsverbreitung einer neuartigen Form von Kontrolle und Überwachung unterworfen, sondern auch das Alltagshandeln der Bürger:innen. Noch nie waren die Erwartungen an den Einzelnen höher, Gesundheitsrisiken im Alltag zu kontrollieren. Warn-Apps und digitale Impfpässe haben eine digitale Infrastruktur geschaffen, die dazu verpflichtet, bei alltäglichen Einrichtungen wie Einkaufen und Busfahren immer wieder nachzuweisen, kein „Gefährder“ zu sein. Alle Menschen, auch die kerngesunden, gelten als potenzielles Risiko und sind nicht mehr Träger aller Bürgerrechte, solange sie sich nicht als frisch getestet, kürzlich genesen oder geimpft ausweisen können. Die rechtsstaatliche Unschuldsvermutung wird dadurch umgekehrt, nach der jeder Mensch als unbescholten gilt und Grundrechtsträger ist, solange nicht das Gegenteil bewiesen ist. Diese Verkehrung der rechtsstaatlichen Unschuldsvermutung ist keinesfalls neu, sie hat sich durch die Corona-Krise lediglich zugespitzt. Eine Gesellschaft, die sich dem Ziel der Prävention verschrieben hat – Gesundheits- und Kriminalitätsprävention sind nur zwei markante Bereiche – verallgemeinert den Verdacht. Wenn Vorbeugung das Ziel von Gesundheitspolitik oder Justiz wird, muss nicht mehr Schuld, sondern Unschuld bewiesen werden. Wenn beispielsweise Eltern ihr Kind nicht zu den vorgesehenen Vorsorgeuntersuchungen beim Kinderarzt vorstellen und hierdurch nachweisen, dass sie es nicht misshandeln, wird das Jugendamt umgehend alarmiert, das zu einem Kontrollbesuch anrückt.

*„Weil Risiken nur probabilistisch erfassbar sind, generalisiert der präventive Blick den Verdacht und sucht Indizien aufzuspüren, die auf künftige Übel hindeuten und an denen die vorbeugenden Maßnahmen ansetzen können“ (Bröckling 2004, 211-212).*

### Von der klinischen Medizin zur Überwachungsmedizin

Durch den Fokus auf Prävention und die Identifizierung von Risikofaktoren ist Überwachung in der heutigen Medizin bereits angelegt. Der Medizinsoziologe David Armstrong analysierte schon in den 1990-er Jahren einen tief greifenden Umbruch im medizinischen Denken, den er als Übergang von der klinischen





Medizin zur *Überwachungsmedizin* beschrieb. Die Überwachungsmedizin orientiert sich nicht mehr am Körper des Patienten wie die klinische Medizin, sondern an statistischen Wahrscheinlichkeiten. Die Unterscheidung zwischen dem Gesunden und Pathologischen, welche bis dahin das ärztliche Denken und Handeln bestimmte, löst sich auf. Nicht mehr nur die Kranken sind Zielscheibe medizinischer Kontrolle und Behandlung, sondern vor allem die gesunde Bevölkerung: „Surveillance Medicine requires the dissolution of the distinct clinical categories of healthy and ill as it attempts to bring everyone within its network of visibility“ (Armstrong 1995, 395). Ziel der Überwachungsmedizin ist nicht, eine abhanden gekommene Gesundheit wiederherzustellen, sondern sich der Zukunft zu bemächtigen. „Surveillance Medicine [...] attempt[s] to transform the future by changing the health attitudes and health behaviours of the present“ (Armstrong 1995, 402).

### Ziel: Die Kontrolle der Wahrscheinlichkeiten und der Zukunft

Ziel der Überwachungsmedizin ist es also, wie der Philosoph Michel Foucault für die Biopolitik im Allgemeinen formulierte, die „Wahrscheinlichkeit zu kontrollieren“ (Foucault 1999, 288). Um den Einzelnen geht es dabei gar nicht – die Patientin als Wesen aus Fleisch und Blut kommt gar nicht mehr vor. Voraussetzung für die Kalkulation statistischer Gesetzmäßigkeiten ist es, den Menschen in der Masse aufzulösen. Der Tod, die Geburt, die Erkrankung und der Unfall gerinnen erst auf der Ebene der Masse zur berechenbaren Regelmäßigkeit, also zur Mortalität, Geburtenrate, Morbidität oder zum Unfallrisiko. Für den Einzelnen bleiben sie unvorhersehbarer Zufall, Schicksalsschlag oder einzigartige Lebensgeschichte.

*„Es sind zufällige und unvorhersehbare Phänomene, wenn man sie individuell für sich nimmt, die jedoch auf kollektiver Ebene Konstanten aufweisen, die ausfindig zu machen leicht oder doch immerhin möglich ist“ (Foucault 1999, 284).*

Statistische Wahrscheinlichkeiten sagen also per definitionem nichts über den Einzelfall, sie beziffern lediglich zukünftige Häufigkeiten in Populationen. Dennoch: Die Wahrscheinlichkeiten können nicht ohne Individuen gesteuert werden. Die medizinischen „Sicherheitstechnologien“, wie Foucault sie nennt, zielen daher durchaus auch auf den Einzelnen, allerdings nicht als Individuum, sondern als Element von berechenbaren und regulierbaren Kollektiven.



**Silja Samerski** ist Biologin und Sozialwissenschaftlerin und erforscht die sozialen und kulturellen Auswirkungen der Technisierung im Gesundheitswesen. Im Mittelpunkt ihrer Arbeit steht die Frage, welche neuen Selbstverständlichkeiten z. B. Gentests in der Schwangerschaft oder Risikovorhersagen in Gesundheits-Apps vermitteln. Sie leitet das Forschungsprojekt StePOn, das soziotechnische Praktiken der Objektivierung am Beispiel von Gesundheits-Apps untersucht. Seit 2018 ist sie Professorin für Soziale Arbeit mit dem Schwerpunkt Gesundheit an der Hochschule Emden/Leer.

Die Steuerung der Einzelnen als Elemente statistischer Populationen lässt sich durch die Datafizierung und Digitalisierung als individuelles Gesundheitsmanagement darstellen. Durch Sensoren, KI, Big Data und Gesundheits-Apps wird die Überwachungsmedizin zugleich übermächtig und alltäglich. Die Möglichkeiten, Gesundheitsrisiken zu konstruieren und darüber das individuelle Verhalten zu steuern, weiten sich in ungeahntem Maße aus. Ganze Datenmeere können nun nach gesundheitsbezogenen Mustern und Korrelationen durchforstet werden, um Risikofaktoren und potenzielle Vorhersagen zu produzieren. Nicht nur die klassischen Gesundheitsdaten, sondern auch Daten aus Sozialen Netzwerken, Google-Suchen, Fitness- und Stimmungs-Tracking, Mobilitätsaufzeichnungen etc. dienen dazu, immer feinkörnigere Datendoppel von Menschen zu erstellen, von denen computergestützt alle möglichen Gesundheits- und Krankheitswahrscheinlichkeiten abgeleitet werden können. Auf dieser Grundlage werden dann auf Gesundheits- und Lifestyle-Apps Frühwarnsysteme installiert, die Nutzer:innen – vermeintlich persönlich – die nächste Depression oder eine mögliche Herz-Kreislauferkrankung vorhersagen, verbunden mit der Aufforderung, diese rein statistische Möglichkeit durch entsprechendes Risikomanagement zu verhindern. Doch nicht nur das Management von Risiken, sondern auch die Optimierung von kalkulierbaren Gesundheitschancen ist das Ziel der Überwachung: Das weltweit agierende Unternehmen *Dacadoo* bietet eine Gesundheits-Plattform an, die zum umfassenden Gesundheits- und Lebensstil-Tracking einlädt und daraus einen dynamischen „Gesundheits-Score“ kalkuliert, eine Zahl zwischen 0 und 1000. Den Score vergleicht das Unternehmen mit einem Aktienkurs und wirbt damit, dass er sowohl über die gegenwärtige als auch über die zukünftige Gesundheit Auskunft gibt. Zahlreiche Gesundheitstipps leiten dabei an, diesen Score fortwährend zu halten und zu optimieren.

### Überwachung im Alltag: Von der Erfassung zur Selbstermächtigung?

Überwachung, Profiling und Predictive Analytics bzw. computergestützte Risikokalkulation, im Gesundheitsbereich eingesetzt, sind in anderen sozialen Bereichen bereits alltäglich: In mehreren deutschen Städten arbeitet die Polizei mit der Software *precobs*, die auf der Grundlage von Polizeidaten die Wahrscheinlichkeit kalkuliert, dass in den nächsten drei bis sieben Tagen in bestimmten Straßenzügen eingebrochen wird. Markiert das Programm eine Gegend rot, verstärkt die Polizei dort ihre Präsenz. „Die Polizei überwacht die Zukunft“, so betitelt die Süddeutsche

**Silja Samerski**



Zeitung ihre Reihe zum Thema *predictive policing*. In anderen Ländern identifiziert die Polizei nicht nur risikoträchtige Straßenzüge, sondern auch risikoträchtige Personen: In den USA werden neben Polizeidaten auch Daten aus sozialen Netzwerken und Überwachungstechnologien in die Programme zur Risikokalkulation eingespeist. Städte wie Oklahoma City sind bereits mit einem dichten Netz aus Überwachungskameras und Überwachungssensoren überspannt. Das europäische Forschungsprojekt INDECT, 2014 abgeschlossen, strebte eine ähnlich umfassende Überwachung zur Erfassung „abnormalen Verhaltens“ an. Der Verdacht wird universalisiert; niemand ist davor gefeit, aufgrund bestimmter Merkmale als Risikoträger, also als potenzieller Krimineller oder Terrorist zu gelten.

Während digitale Überwachung und Profiling zugunsten öffentlicher Sicherheit vielfach als „Überwachungsstaat“ und tief greifender Eingriff in die Persönlichkeitsrechte kritisiert worden sind (z. B. Lyon 2014), werden die gleichen Techniken im Gesundheitsbereich als Zuwachs an Selbstbestimmung und Eigenverantwortung propagiert. Es gilt als Akt der Selbstermächtigung, bei einem *Mood-Tracker* oder bei einer Gesundheitsplattform ein Profil anzulegen und seine Gesundheit algorithmisch bewerten und vorhersagen zu lassen. Aus Techniken der Erfassung und Überwachung, so stellt der Kulturwissenschaftler Andreas Bernard fest, sind offenbar Vehikel der Selbstermächtigung geworden. Bis vor wenigen Jahrzehnten war das Erstellen von Profilen als „Raster der Menschenbeschreibung“ (Bernard 2017, 11) vor allem eine erkennungsdienstliche Praxis, eine Technik der Kriminologie, um „Serienmörder oder Wahnsinnige“ (Bernard 2017, 11) dingfest zu machen. Heute machen Menschen sich selbst und ihre Gesundheit freiwillig auf die gleiche Weise „dingfest“ – in der Hoffnung auf Selbsterkenntnis und Verfügung über die Zukunft.

### Das Selbst als Aktienpaket

Das Aufkommen der Überwachungsmedizin hält der Medizinsoziologie David Armstrong deshalb für einschneidend, weil die „Überwachungsmaschinerie“ Menschen ein grundlegend neues Selbstverständnis zuweist: Ein Selbstverständnis, das er „Risiko-Identität“ nennt (Armstrong 1995, 405). Diese neue *Identität* steht im Schatten einer risikoträchtigen Zukunft. Sie ist nicht mehr, wie zu Zeiten der klinischen Medizin, vom konkreten Körper abgeleitet, sondern von statistischen Kollektiven und Möglichkeitsräumen. „Surveillance analyses a four-dimensional space in which a temporal axis is joined to the living density of corporal volume“ (Armstrong 1995, 402). Menschen, die ihre Gesundheit berechnen und bewerten lassen, sehen sich nicht mehr als konkrete Person mit einzigartiger Biografie und offener Zukunft, sondern als Verkörperung von Möglichkeiten und Risiken. Ihr Dasein wurzelt nicht mehr in erlebter Vergangenheit und Gegenwart, sondern ist von einer statistisch vorweggenommenen Zukunft abgeleitet. Durch diese Umdeutung scheint es plausibel, Gesetzmäßigkeiten von statistischen Kohorten und Wahrscheinlichkeitsverteilungen auf sich selbst anzuwenden. Menschen werden geradezu körperlich kompatibel mit Populations-bezogenen Risikoberechnungen und Präventionsstrategien. Eine solche *Risiko-Identität* macht den eigenen Leib unsicher und prekär, da in ihm – z. B. in Form von schlummernden Krankheitserregern, unbemerkten Krebszellen, erhöhten Cholesterin-Werten oder genetischen Krankheitsanlagen eine be-

drohliche Zukunft stecken könnte (Samerski 2009). Gesundheit, so suggeriert der datafizierte, risikobehaftete Körper, ist ständig bedroht. Die Frage nach der Gesundheit mutiert damit zu einer Frage der *inneren Sicherheit* und erzeugt das Bedürfnis nach Überwachung und Risikominimierung.

In den neuen digitalen Gesundheitspraktiken fallen die biopolitische Regulierung von Wahrscheinlichkeiten und persönliche Gesundheitspflege sowie Überwachung von Außen und Selbstüberwachung weitgehend zusammen. Die Praktiken bringen einen risikobehafteten, datafizierten Körper hervor, der in beunruhigender Weise der Wirtschafts- und Leistungs-ideologie des 21. Jahrhunderts entspricht. Die Selbstwahrnehmung, die hier vermittelt wird, ist kompatibel mit den Anforderungen und Denkschemata in der Unternehmensführung und des Managements: „People are, so to speak, coming to see themselves as mini-corporations, collections as assets that each person must continually invest in, nurture, manage, and develop“ (Martin 1994, 77). Wenn Selbstbestimmung noch bedeuten soll, „sich seines Verstandes ohne Leitung eines anderen zu bedienen“, wie Immanuel Kant vor rund 250 Jahren postulierte (Kant 1781, 35), dann ist es nötig, sich von den Zumutungen digitaler Risikovorhersagen und Optimierungsangebote zu befreien.

### Referenzen

- Armstrong, David (1995) The Rise of Surveillance Medicine. In: *Sociology of Health and Illness*, 17 (3): 393-404.
- Bernard, Andreas (2017) Komplizen des Erkennungsdienstes. Das Selbst in der digitalen Kultur. Frankfurt a. M.
- British Medical Journal (2021) Open Letter from The BMJ to Mark Zuckerberg. Online: <https://www.bmj.com/content/375/bmj.n2635/rr-80>
- Bröckling, Ulrich (2004) Prävention. In: Bröckling, U., Krasmann S., Lemke, T., (Hrsg.) *Glossar der Gegenwart*. Frankfurt am Main.
- Deutscher Ethikrat (2017) Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung. Berlin.
- Foucault, Michel (1999) In Verteidigung der Gesellschaft. Vorlesungen am Collège de France (1975-1976), Frankfurt a. M.
- Lyon D. (2014) Surveillance, Snowden, and big data: capacities, consequences, critique. *Big Data & Society*. 2014;1(2) <https://doi.org/10.1177/2053951714541861>.
- Martin, Emily (1994) *Flexible Bodies. Tracking Immunity in American Culture – from the Days of Polio to the Age of AIDS*. Boston: Beacon Press.
- SVR (Sachverständigenrat) Gesundheit (2000/2001). Bedarfsgerechtigkeit und Wirtschaftlichkeit, Kurzfassung
- SVR Gesundheit (2003) Finanzierung, Nutzerorientierung, Qualität.
- Bertelsmann Stiftung/Universität Bremen (2006), Anreize zur Verhaltenssteuerung im Gesundheitswesen. Effekte bei Versicherten und Leistungsanbietern.
- SVR Gesundheit (2021) Digitalisierung für Gesundheit. Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems. Online: [https://www.svr-gesundheit.de/fileadmin/Gutachten/Gutachten\\_2021/SVR\\_Gutachten\\_2021.pdf](https://www.svr-gesundheit.de/fileadmin/Gutachten/Gutachten_2021/SVR_Gutachten_2021.pdf)
- Theyras, Kristel (2021) How Digital ID Can Help Citizens Access Government Services from Anywhere. Online: [https://dis-blog.thalesgroup.com/identity-biometric-solutions/2021/07/27/how-digital-id-can-help-citizens-access-government-services-from-anywhere/?utm\\_source=twitter&utm\\_medium=Hootsuite&utm\\_term=&utm\\_content=&utm\\_campaign=DIS-Digital-Identity](https://dis-blog.thalesgroup.com/identity-biometric-solutions/2021/07/27/how-digital-id-can-help-citizens-access-government-services-from-anywhere/?utm_source=twitter&utm_medium=Hootsuite&utm_term=&utm_content=&utm_campaign=DIS-Digital-Identity)



## Die soziale Konstruktion von Algorithmen

### Interpretationen und Praktiken algorithmischen Managements

Algorithmen sind allgegenwärtig, obwohl sie keineswegs eine neue Erscheinung sind. In Folge gesteigerter Rechenkapazitäten ist ihre Leistungsfähigkeit in jüngerer Zeit markant gestiegen und mit der Allgegenwärtigkeit computergestützter mediatisierter Umgebungen auch ihre Relevanz. Als Technologien, denen Herrschaft inhärent ist, steuern und überwachen sie Menschen und (re)produzieren soziale Ungleichheiten (Eubanks 2018; Zuboff 2018). In den Debatten liegt der Fokus aber meist auf Konsum-Algorithmen, die in sozialen Medien, Musikangeboten, Suchmaschinen oder dem Online-Einzelhandel versuchen, die Betroffenen zum Konsum von Produkten, Informationen oder sozialen Beziehungen anzuregen. Weniger im Blick ist, dass Algorithmen zunehmend auch bestimmen wie wir arbeiten (Heiland 2018). Algorithmisches Management verbreitet sich. Damit wenden Unternehmen, in denen bereits betriebliche Herrschaft existiert, Algorithmen an. Das Management bestimmt, wer, wann, wo und wie zu arbeiten hat, und Algorithmen unterstützen diese Herrschaft. Entsprechend werden algorithmisch gesteuerte Arbeitskontexte als umfassend kontrolliert beschrieben, in denen die Allmacht der Algorithmen mit ihrer „Kombination von totaler Überwachung und Fernsteuerung“ (Zuboff 2018, 390) den Arbeitenden keine autonomen Spielräume mehr lassen. Mit Marx (1962, 446) kann man fragen, ob „nicht der Arbeiter die Arbeitsbedingungen, sondern umgekehrt die Arbeitsbedingung den Arbeiter anwendet“.

Demgegenüber steht eine soziologische Perspektive, die davon ausgeht, dass Technologien sowie deren vermeintlich objektive Fakten und Prozesse zu einem gewissen Maß sozial konstruiert sind.

### Algorithmisches Management

Seit Arbeit als Lohnarbeit verrichtet wird und abhängige Beschäftigung im frühen Kapitalismus die Norm wurde, stellt sich die Frage, wie sichergestellt wird, dass Arbeiter:innen auch tatsächlich arbeiten. Henry Ford soll sich über die Tatsache beschwert haben, dass jedes Mal, wenn er ein neues paar Hände in seiner Produktion benötige, mit diesen ein neues Gehirn einhergehe. Die Besonderheit der Ware Arbeitskraft ist, dass sie unweigerlich an Menschen gebunden ist. Menschen sind keine Maschinen, und haben eigene Interessen, bringen Eigensinn mit und sind nach gewisser Zeit erschöpft, sodass sie ihre Arbeitskraft reproduzieren müssen. Ein Arbeitsvertrag hält nur fest, wann und grob zu welchen Inhalten die Arbeitenden eingesetzt werden. Das Management eines Unternehmens muss die Arbeitsfähigkeit der Angestellten in Arbeitsleistung transformieren. Zu diesem Zweck hat es verschiedene Kontrolltechniken entwickelt. Vorgesetzte können die Arbeitenden während der gesamten Arbeit beobachten, ein enges Korsett an Vorschriften festlegen, oder die Arbeit kann subjektiviert werden, sodass die Beschäftigten aus intrinsischem Interesse ihre Arbeitsleistung erbringen. Eine neue Kontrollform ist algorithmisches Management, das erlaubt Arbeitsprozesse automatisiert zu koordinieren und zu kontrollieren. Auf Basis aufgezeichneter Daten weist es automatisch Aufgaben zu, überwacht deren Umsetzung und evaluiert die Leistung der Arbeitenden. Taylor (2007, 45) merkt 1914 noch an, dass „die allermeisten Maschinenfabriken zu wenig Aufsichtsorgane [haben], um wirtschaftlich zu arbeiten“, heute ist das keine Her-

ausforderung mehr. Ob im Büro, im Homeoffice oder unterwegs lassen sich unterschiedliche Arbeitsprozess kleinteilig beobachten und steuern. Algorithmisches Management findet besonders im Bereich gering qualifizierter Tätigkeiten statt, zunehmend aber auch in anderen Arbeitsformen (Kellogg et al. 2020).

Grundlage algorithmischen Managements ist die Verdattung der sozialen Welt. Komplexe soziale Beziehungen und Individuen werden dematerialisiert, als reduzierte Datenstruktur modelliert und damit in *numerische Repräsentationen* transformiert. Auf dieser Basis geben Algorithmen nach programmierten Entscheidungsbäumen vor, was die Beschäftigten umzusetzen haben. So bestimmen sie entweder konkrete Handlungen der Arbeiter:innen, oder sie legen enge Korridore fest, in denen die Beschäftigten autonom agieren können. Ähnliches zeigt sich bereits bei früheren Arbeitstechnologien: „Einem Arbeiter, der eine moderne Maschine bedient, wird der Gedanke gar nicht kommen, der sinnfälligen Gesetzmäßigkeit dieser Maschine willkürlich zuwider zu handeln“ (Popitz et al. 1976, 211). In ihrer digitalen Form ist die Kontrolle von Arbeit umfassender und unausweichlicher. In Software programmierte soziale Verhältnisse sind nicht verhandelbar und üben einen besonderen Druck aus: „Code is law“ (Lessig, 2001).

Verdattung und algorithmische Entscheidungen reproduzieren und beeinflussen die sozialen Verhältnisse spezifisch. Anders formuliert ist Algorithmen Herrschaft unweigerlich inhärent, im Arbeitskontext die betriebliche Herrschaft der Unternehmensleitung. Algorithmisches Management agiert als ein verlängerter Arm der Vor-



Heiner Heiland

Heiner Heiland ist wissenschaftlicher Mitarbeiter am Institut für Soziologie der Universität Göttingen. Er forscht zu Digitalisierung, Kontrolle und Widerstand in Arbeitsprozessen von Großunternehmen und der Plattformarbeit.





gesetzten, der es erlaubt, die Kontrolle über den Arbeitsprozess zu wahren und auszubauen. Diese Kontrolle wird durch die vermeintlich rein technologischen Mechanismen und deren unpersönliche Vermittlung als objektiv wahrgenommen. Eine Begutachtung der algorithmischen Entscheidungssysteme ist in der Regel unmöglich, sie sind als *black box* intransparent und lassen keine Reflektion oder Kritik der Entscheidungen zu. In dieser Perspektive etabliert algorithmisches Management ein umfassendes Kontrollregime in Arbeitskontexten, das die autonomen Handlungsspielräume der Arbeitenden eliminiert oder zumindest einschränkt. Diese verbreitete Ansicht ist nicht falsch, trägt aber zugleich die Züge eines Technikdeterminismus, der von den technologischen Gegebenheiten auf die tatsächlichen Praktiken schließt. Demgegenüber konstatiert ein techniksoziologischer Blick, dass die Praxis differenzierter ist.

### Die soziale Konstruktion von Algorithmen

In der Technikphilosophie und -soziologie ist es ein Gemeinplatz, dass auch Technik sozial konstruiert ist. Das Ausmaß des Sozialen in der Technik ist Gegenstand anhaltender Debatten. Einigkeit herrscht aber darüber, dass die Entwicklung von Technik kein automatischer und determinierter Prozess ist, an deren Ende das einzig möglich Zielprodukt steht. So zeigen zum Beispiel Pinch und Bijker (1987), dass der heutigen Form des Fahrrads zahlreiche andere Versionen vorangingen, deren Entwicklung von unterschiedlichen Diskursen geprägt wurden. Technik ist kontingent und könnte immer auch anders sein.

Auch Algorithmen sind konstruiert. Diese Konstruktion geschieht nicht in einem sozialen Vakuum. Sie lässt sich in vier Ebenen unterteilen, in die jeweils soziale Prozesse mit einfließen (siehe Abbildung 1). Zuerst wird ein Algorithmus geplant. Das Management eines Unternehmens kommuniziert Vorgaben (etwa die Kontrolle des Arbeitsprozesses). Auf der zweiten Ebene wird ein Algorithmus programmiert. Mit dem Ziel, in spezifischen Situationen eigenständige und automatische Entscheidungen zu treffen, wird Code geschrieben und in vorhandene Software implementiert. Drittens wird ein Algorithmus kuratiert. Menschen agieren als „data janitors“, die algorithmische Entscheidungen den Nutzenden vermitteln, Fehler korrigieren und in den Entscheidungsprozess eingreifen können. Viertens, und meist weniger berücksichtigt, konstruieren auch die Nutzenden die Algorithmen. Algorithmische Entscheidungen werden nur durch ihre Anwendung in der Praxis wirksam. Die Nutzenden setzen diese Vorgaben individuell um und bringen somit ihre persönlichen Interessen und Subjektivitäten ein.

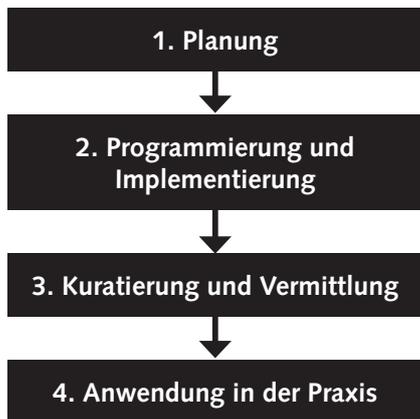


Abbildung 1: Vier Ebenen der Konstruktion von Algorithmen

Algorithmen sind auf allen vier Ebenen ihrer Konstruktion verschiedenen Interessen und Praktiken ausgesetzt. Das bedeutet nicht, dass diese Ebenen symmetrisch sind und gleichwertigen Einfluss auf die Resultate der Regelungsstrukturen haben. Technik allgemein und auch Algorithmen sind keine Dinge, sondern komplexe soziale Prozesse, die auch als solche analysiert werden müssen. Mit Blick auf ihre Konstruktion umfasst Technik unweigerlich Herrschaft. Das gilt umso mehr in Arbeitskontexten, in denen Management und Arbeiter:innen in einem strukturellen Gegensatz zueinander verortet sind. Technik ist eine „Verdinglichung gesellschaftlicher Interessen“ (Rammert 1983, 62). In algorithmisches Management sind explizite Interessen der Unternehmen eingeschrieben und bestimmen dessen Funktionsweisen. Resultate sind umfassende technologische Kontrollregime.

Doch Herrschaft ist eine soziale Beziehung. Sie wirkt nicht unilateral und muss sich in der Praxis etablieren. Darüber hinaus ist Technik mehr als eine einzige mögliche Anwendungsweise eingeschrieben. Es existiert eine *interpretative Flexibilität*, der zufolge Technik zwar meist eine dominante Nutzungsweise mit sich bringt, sie kann aber immer auch anders genutzt werden (Oudshoorn und Pinch 2003, 1–2). Beispielsweise nutzten amerikanische Farmer *Fords Model T* oft nicht, um von A nach B zu kommen, sondern als mobile Antriebsquelle für landwirtschaftliche Maschinen (Kline und Pinch 1996). Technologie entwickelt ihre Wirkung erst in der Praxis und kann mitunter durch die Nutzenden *redesigned* werden. Ohne Zweifel schränken digitale Strukturen abweichende Praktiken weit stärker ein als analoge – siehe beispielsweise den Kontrast zwischen einem technisch vglw. einfachen *Model T* und einem modernen mechatronischen Auto. *Users matter* trotzdem. So ist nicht gesagt, dass die durch Algorithmen vermittelten Anweisungen und Kontrollen ungefiltert umgesetzt werden (Heiland 2020a). Entscheidend sind die konkreten praktischen Interaktionen der Arbeiter:innen mit Algorithmen, und erst ein Blick auf diese Praxis erlaubt, die Effekte algorithmischen Managements realistisch einzuschätzen.

Menschliche Praxis ist nicht losgelöst von den Individuen und deren Sozialisationen, Erfahrungen und Annahmen über die Dinge, mit denen sie interagieren. Niemand wägt jede Situation, in der sie oder er sich befindet, immer neu ab, wir greifen auf allgemeine soziale Deutungsrahmen sowie individuelle Erfahrungen zurück. Um Informationen verarbeiten zu können, bedürfen Menschen kognitiver Strukturen (Bandura 1986), die es ihnen erlauben, die soziale Realität sinnhaft zu deuten. Diese kognitiven Schemata und mentalen Modelle bieten Orientierung und leiten individuelle Handlungen und Entscheidungen an – sei es um abzuschätzen, wann die Waschmaschine fertig ist, oder um die Entscheidungen von Algorithmen antizipieren und berücksichtigen zu können. Anders wären Menschen angesichts der Komplexität ihrer Umwelt überfordert und unfähig zu handeln. So nutzen Menschen im Straßenverkehr ihr Wissen über Schilder, Ampeln und Vorfahrtsregeln, verbinden es mit ihren Erfahrungen und agieren demgemäß. Größte Gefahr im Leben von Kindern in Deutschland ist der Straßenverkehr, gerade weil sie dieses Wissen und die dazugehörigen Erfahrungen und damit die notwendigen mentalen Modelle noch nicht haben.

In ihren Interaktionen mit Algorithmen entwickeln Arbeiter:innen mentale Modelle von deren Funktionsweise, um ihre Handlungen anzupassen und die Resultate in ihrem Sinne zu beeinflussen



(Payne 2003). Ähnlich ist bekannt, dass Computerspieler:innen ein mentales Abbild der Spielmechanismen entwickeln und diesem Modell ihre Handlungen anpassen. Entscheidend ist aber, dass Algorithmen, anders als ein *Model T*, keine Motorhaube haben, die sich von den Arbeiter:innen öffnen ließe und ihre Mechanismen darlegt, geschweige denn, dass Nutzer:innen den Code der Algorithmen verändern können. Algorithmen sind eine *black box*. Trotzdem entwickeln Arbeiter:innen Theorien über die Funktionsweise von Algorithmen, die ihre Handlungen anleiten und damit auch das Ergebnis algorithmischer Entscheidungen bestimmen.

Vorreiter bei Entwicklung und Anwendung algorithmischen Managements sind die Plattformen (Heiland 2018; Heiland 2020b). Vor allem wenn diese meist kleinteilige Arbeitsaufträge vermitteln, müssen sie räumlich verteilte Arbeiter:innen organisieren und Arbeitsprozesse auf Distanz automatisiert koordinieren und kontrollieren. Bei Plattformen zeigt sich besonders, dass die soziale Konstruktion der Algorithmen vonseiten der Nutzer:innen die Effekte bestimmt. So ist bekannt, dass *Uber*-Fahrer:innen sich in Online-Foren über die Algorithmen austauschen und ihre Strategien entsprechend anpassen (Reid Musson et al. 2020; Rosenblat 2018) oder dass *YouTube*-Vlogger:innen „algorithmic gossip“ betreiben, um den Erfolg ihrer Videos zu beeinflussen (Bishop 2019). Auch in der plattformvermittelten Lieferung bestellter Mahlzeiten ist algorithmisches Management relevant (Heiland 2021a; Heiland 2021b). Hier zeigt sich, dass die Arbeiter:innen Theorien über die intransparenten Algorithmen entwickeln, die nur begrenzt mit deren tatsächlichen Funktionsweisen übereinstimmen. Auch wenn diese Interpretationen objektiv falsch sind, wirken sie handlungsleitend, denn „[i]f men define situations as real, they are real in their consequences“ (Thomas und Thomas 1928, 572). Resultat ist, dass nicht nur die eigentlichen Algorithmen, sondern auch deren Intransparenz den Arbeitsprozess steuern und zu einem vorausseilenden Gehorsam führen (Heiland 2022 in review; Heiland 2022).

## Fazit

Algorithmisches Management weitet die Kontrolle über Arbeitsprozesse aus und schränkt die Handlungsspielräume der Arbeitenden markant ein. Doch Algorithmen sind kein Ding, sondern entfalten ihre Wirksamkeit erst im Zusammenspiel mit Menschen, die ihre Anweisungen umsetzen. Um die konkreten Effekte algorithmischen Managements zu bestimmen, müssen daher nicht nur die Funktionsweise der Algorithmen erforscht werden, sondern ergänzend auch die Annahmen der Arbeiter:innen und in welcher Form diese handlungsleitend wirken. Erst durch eine solche praxisorientierte Perspektive ist ein realistischer Blick auf die tatsächlichen Auswirkungen sowie etwaige widerständige Praktiken der Arbeiter:innen möglich.

## Referenzen

- Bandura, Albert (1986) *Social foundations of thought and action. A social cognitive theory*. Englewood Cliffs, NJ, Prentice-Hall.
- Bishop, Sophie (2019) Managing visibility on YouTube through algorithmic gossip. *New Media & Society* 21 (11-12), 2589–2606. <https://doi.org/10.1177/1461444819854731>.
- Eubanks, Virginia (2018) *Automating inequality. How high-tech tools profile*

- le, police, and punish the poor. New York, St. Martin's Press.
- Heiland, Heiner (2018) Algorithmus = Logik + Kontrolle. Algorithmisches Management und die Kontrolle der einfachen Arbeit. In: Daniel Houben/Bianca Prietl (Hg.). *Datengesellschaft. Einsichten in die Datafizierung des Sozialen*. Bielefeld, transcript, 233–252.
- Heiland, Heiner (2020a) Die Praxis der Plattformarbeit. Von der Relevanz ethnographischer Analysen digitaler Arbeitskulturen. *Berliner Blätter* (82), 17–28. <https://doi.org/10.18452/22133>.
- Heiland, Heiner (2020b) Workers' Voice in Platform Labour. An Overview. WSI-Study.
- Heiland, Heiner (2021a) Controlling Space, Controlling Labour? Contested Space in Food Delivery Gig Work. *New Technology, Work and Employment* 36 (1), 1–16. <https://doi.org/10.1111/ntwe.12183>.
- Heiland, Heiner (2021b) Neither Timeless, nor Placeless. Control of Food Delivery Gig Work via place-based Working Time Regimes. *Human Relations*. <https://doi.org/10.1177/00187267211025283>.
- Heiland, Heiner (2022) Black Box Power. Zones of Uncertainty in Algorithmic Management. In: Emiliana Armano/Marco Briziarelli/Elisabetta Risi (Hg.). *Digital Platforms and Algorithmic Subjectivities*. Westminster, Westminster University Press.
- Heiland, Heiner (2022 in review) The Social Construction of Algorithms. Influence of and Influence on Algorithmic Management.
- Kellogg, Katherine C, Valentine, Melissa A, Christin, Angéle (2020) Algorithms at Work: The New Contested Terrain of Control. *Academy of Management Annals* 14 (1), 366–410. <https://doi.org/10.5465/annals.2018.0174>.
- Kline, Ronald, Pinch, Trevor (1996) Users as Agents of Technological Change: The Social Construction of the Automobile in the Rural United States. *Technology and Culture* 37 (4), 763. <https://doi.org/10.2307/3107097>.
- Lessig, Lawrence (2001) *Code und andere Gesetze des Cyberspace*. Berlin, Berlin-Verlag.
- Marx, Karl (1962) *Das Kapital. Erster Band*. In: Karl Marx und Friedrich Engels Werke. Berlin, Dietz.
- Oudshoorn, Nelly, Pinch, Trevor J (2003) Introduction. In: Nelly Oudshoorn/Trevor J. Pinch (Hg.). *How users matter. The co-construction of users and technologies*. Cambridge, Mass, MIT Press, 1–25.
- Payne, Stephen J (2003) Users' Mental Models: The Very Ideas. In: HCI Models, Theories, and Frameworks. Elsevier, 135–156.
- Pinch, Trevor J, Bijker, Wiebe E (1987) The Social Construction of Facts and Artifacts. Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. In: Wiebe E. Bijker, Thomas P. Hughes, Trevor J. Pinch Hg. (1987) *The social construction of technological systems. New directions in the sociology and history of technology*. Cambridge, MIT Press, 17–50.
- Popitz, Heinrich, Bahrndt, Hans P, Jüres, Ernst A, Kesting, Hanno (1976) *Technik und Industriearbeit. Soziologische Untersuchungen in der Hüttenindustrie*. Tübingen, Mohr.
- Rammert, Werner (1983) Technisierung der Arbeit als gesellschaftlich-historisches Projekt. In: Wolfgang Lütke/Werner Rammert/G. Wachtler (Hg.). *Einführung in die Arbeits- und Industriosozologie*. Frankfurt, Campus, 62-75.
- Reid-Musson, Emily/MacEachen, Ellen/Bartel, Emma (2020) 'Don't take a pool': Worker misbehaviour in on-demand ride-hail carpooling. *New Technology, Work and Employment* 35 (2), 145–161. <https://doi.org/10.1111/ntwe.12159>.
- Rosenblat, Alex (2018) *Uberland. How Algorithms Are Rewriting the Rules of Work*. Berkeley, University of California Press.
- Taylor, Frederick Winslow (2007) *Die Betriebsleitung insbesondere der Werkstätten*. 3. Aufl. Berlin, Springer.
- Thomas, William I, Thomas, Dorothy S (1928) *The Child in America. Behavior Problems and Programs*. New York, Alfred Knopf.
- Zuboff, Shoshana (2018) *Das Zeitalter des Überwachungskapitalismus*. Frankfurt/New York, Campus.



## Verleihung des Weizenbaum-Studienpreises 2021

Auch in diesem Jahr verleihen wir wieder den Weizenbaum-Studienpreis, gewidmet Professor Joseph Weizenbaum, der die Gründung des FfF gefördert hat, dem wir 1998 einen Ehrenpreis des FfF für seinen Einsatz für Verantwortung in der Informatik verliehen haben und der dessen langjähriges Vorstandsmitglied war.

Zwei Zitate, die wir Hans-Jörg Kreowski verdanken, eignen sich als Leitbild unseres Weizenbaum-Studienpreises. Das erste Zitat betont die Verantwortung, die mit (technischem) Fortschritt und Entwicklung einhergeht:

*Naturwissenschaftler und Techniker tragen aufgrund ihrer Macht eine besonders schwere Verantwortung, vor der sie sich nicht hinter einer Fassade von Schlagwörtern wie dem der technischen Zwangsläufigkeit drücken können.*

Das zweite Zitat lautet wie folgt und kann auch als Kommentar zum Klimawandel gelesen werden:

*Ich glaube, eine Gesellschaft, die fähig wäre, eine deutliche und klare Entscheidung in Richtung Verzicht zu treffen, hätte die Fallen vermieden, in die wir getappt sind. Solch eine Gesellschaft könnte sich auch modernste Technik leisten. Aber zu solch einer Entscheidung waren wir nie fähig.*

Die prämierten Arbeiten decken ein breites Feld ab; drei Stichworte stehen dabei jedoch im Vordergrund:

- Digitalisierung,
- Vertrauen und
- Macht.

Wir vertrauen den Informationen, die uns das Internet bietet, wir vertrauen der Expertise, die uns von Services zu Verfügung gestellt wird, den Suchmaschinen, den Einschätzungen anderer Benutzer:innen – die wir nicht einmal kennen. Manche vertrauen blind irgendwelchen Blogposts oder Social-Media-Beiträgen, auch wenn es zahlreiche wissenschaftliche Erkenntnisse gibt, die gegenteilige Aussagen stützen.

Dabei stehen die technischen Plattformen, auf denen man die Inhalte finden kann, in einer Machtposition. Denn sie beeinflussen, was wir lesen (können) und was uns als erstes vorgeschlagen wird.

Bei so eingesetzten Empfehlungsalgorithmen kommt teilweise Künstliche Intelligenz ins Spiel. Von manchen wird sie als Allheilmittel angesehen, durch Joseph Weizenbaum wurde sie stets kritisch betrachtet – den aktuellen Boom hat er nicht mehr miterlebt. Und dieses Mittel kommt nicht nur im alltäglichen Internet zu Einsatz – nein, auch Institutionen wie Behörden nutzen es beispielsweise zur Identifizierung von Personen.

All diese Entwicklungen fassen wir unter den Begriff der „Digitalisierung“. Doch diese ist nicht so neu, wie manche Glauben machen wollen, sondern eine exponentielle Entwicklung, die in-



Weizenbaum  
Studienpreis

zwischen in die Phase zunehmender Beschleunigung eingetreten ist. Sie begann bereits in den 1950-er Jahren, in unterschiedlichen Gesellschaftssystemen, und immer wirken die sozialen Rahmenbedingungen darauf ein.

Der Unternehmensgründer und Investor Azeem Azhar sagte kürzlich in einem Interview: „Technology is too important to be left to technologists.“ Dem stimmen wir zu. Für uns Informatikerinnen und Informatiker ist es die gesellschaftliche Aufgabe, technische Systeme auch von ihren ethischen, sozialen und rechtsstaatlichen Anforderungen her zu denken, um eine Technik zu verhindern, die zum Selbstzweck wird und schädliche Nutzung als „Sachzwang“ etabliert. Mit unserem Studienpreis wollen wir Arbeiten auszeichnen, die dieser Aufgabe gerecht werden.

Worauf haben wir bei den Arbeiten geachtet? Unsere Kriterien sind:

- Interdisziplinarität, inhaltliche Verbindung von Informatik und gesellschaftlich relevanten Themen,
- Kreativität und Originalität der Arbeit,
- Neuartigkeit und Aktualität der Ergebnisse,
- Inhaltliche Korrektheit und Vollständigkeit, Formale Korrektheit und Lesbarkeit,
- Umfang der Berücksichtigung einschlägiger Literatur
- und, besonders wichtig, kritischer Umgang mit dem Thema.

Wir bedanken uns herzlich für die große Zahl an Arbeiten, die in diesem Jahr bei uns eingereicht wurde. Eine Jury, besetzt mit

- Professorin *Britta Schinzel* aus Freiburg,
- Professorin *Christina Claß* aus Jena,
- Professor *Jochen Koubek* aus Bayreuth,
- Professor *Dietrich Meyer-Ebrecht* aus Aachen,
- *Rainer Rehak* aus Berlin,
- *Christian Ricardo Kühne* aus Berlin,
- *Tina Lenk* aus Chemnitz und *Felix Kettenbeil* aus Göttingen, als Vertreterin und Vertreter der Konferenz der Informatik-Fachschaften
- *Stefan Hügel* aus Frankfurt am Main

hat aus den Einreichungen für den Studienpreis 2021 vier Arbeiten ausgewählt, die wir heute hier prämiieren werden. Wir haben einen ersten, einen zweiten und zwei dritte Preise vergeben:

- **Hendrik Heuer** für seine Arbeit *Users & Machine-Learning-Based Curation Systems*,



- **Helene Hahn** für ihre Arbeit *Digital identification systems and the right to privacy in the asylum context: An analysis of implementations in Germany*,
- **Silke Meiser** für ihre Arbeit *Trust me! Vorschlag zum Umgang mit der Vertrauensfrage im digitalen Zeitalter*,
- **Martin Schmitt** für seine Arbeit *Die Digitalisierung der Kreditwirtschaft. Computereinsatz in den Sparkassen der Bundesrepublik und der DDR, 1957-1991*.

Wir bedanken uns herzlich bei allen Teilnehmerinnen und Teilnehmern für die eingereichten Arbeiten und gratulieren den Preisträgerinnen und Preisträgern. Die Laudationes wurden von Stefan Hügel vorbereitet und von Rainer Rehak und Stefan Hügel vorgetragen. Näheres zum Weizenbaum-Studienpreis ist unter <https://www.fiff.de/studienpreis> zu finden.



## Weizenbaum-Studienpreis – Laudatio für den ersten Preis

# Hendrik Heuer: Users & Machine-Learning-Based Curation Systems

## Dissertation an der Universität Bremen

Immer mehr verlagern sich unsere Informationsquellen von den „klassischen“ Medien – Presse, Rundfunk, (lineares) Fernsehen – zu Informationsangeboten im Internet, vor allem in den sozialen Medien. Betreiber sind große Konzerne – gerne als GAFAM abgekürzt –, die in der Regel nicht allein nach der bestmöglichen Informiertheit ihrer Nutzer:innen streben, sondern, wie jüngst die Facebook-Whistleblowerin Frances Haugen eindrucksvoll belegte, vor allem wirtschaftliche Interessen verfolgen.

Welche Informationen den Nutzerinnen und Nutzern auf welche Weise präsentiert werden, kann dabei einen erheblichen Einfluss auf die öffentliche Meinung haben. Politikerinnen und Politiker wie Donald Trump setzen dieses Mittel gezielt ein, um die Öffentlichkeit zu beeinflussen. Auch in Europa werden solche Entwicklungen immer deutlicher erkennbar, etwa durch die Aktivitäten von Mitgliedern vor allem rechtspopulistischer Parteien. Damit kommt den Betreibern der Plattformen eine erhebliche Verantwortung zu. Shoshana Zuboff schreibt in ihrem bekannten Buch vom „Überwachungskapitalismus“:

*„Durch die erfolgreiche Durchsetzung des Anspruchs auf Freiheit und Wissen sowie auf seine strukturelle Unabhängigkeit vom Menschen – weder als Angestellte noch als Kundschaft – manövriert uns der Überwachungskapitalismus heute mittels der radikalen Indifferenz, die diese Ansprüche sowohl bedingen als auch ermöglichen und aufrechterhalten, einer Gesellschaft entgegen, in der der Kapitalismus nicht länger als Mittel inklusiver politischer und ökonomischer Institutionen funktioniert. Stattdessen müssen wir den Überwachungskapitalismus als das anerkennen, was er ist: eine zutiefst antidemokratische soziale Kraft.“*

Gleichzeitig erleben wir gerade eine beschleunigte Entwicklung der Künstlichen Intelligenz und des Machine Learning. Folgerichtig wird beides von der Sozial-Media-Industrie verbunden und kombiniert. So wird entsprechend trainierte, vermeintlich unbestechliche und neutrale Künstliche Intelligenz für die Kuratierung von Informationsangeboten in sozialen Netzen eingesetzt. Das erscheint naheliegend – doch sollten Chancen und Risiken zunächst kritisch untersucht werden, und dabei auch: Chancen für wen, Risiken für wen?

Diese Untersuchung hat Hendrik Heuer unternommen. Der erste Preis des diesjährigen Weizenbaum-Studienpreises geht deswegen an seine Dissertation *Users & Machine Learning-Based Curation Systems*, in der er die besonderen Herausforderungen untersucht, die sich durch automatisierte Kurationsysteme ergeben, die mittels Machine Learning trainiert werden.

Indem er den Fokus dabei auf die Menschen legt, die mit diesen Systemen zu tun haben, gelingt ihm eine originelle Herangehensweise, weitab rein rechnerischer Überlegungen. Vielmehr führt er in 10 Kapiteln teils aufwändige Studien mit einer beeindruckenden Methodenvielfalt durch, von qualitativen Interviews über quantitativ ausgewerteten Fragebögen bis zu automatisierten Evaluationsverfahren.

Als Ergebnis dokumentiert er verschiedene Aspekte journalistischer Praxis, von Youtube-Empfehlungen aus Anwender-Sicht, der Verlässlichkeit von Nachrichtenempfehlungen bis zu Erklärungsformen und Prüfverfahren.

Ein wesentliches Ergebnis seiner Arbeit ist, dass diese Systeme einerseits von Praktikerinnen und Praktikern deutlich kritischer wahrgenommen werden als ihre Wirkung vermuten lässt, aber dass es andererseits bei Nutzerinnen und Nutzern eine Lücke gibt zwischen den möglichen und den gewünschten Erklärungen für die Präsentation konkreter Inhalte, eine Lücke, die er den *explanatory gap* nennt.

Die Darstellung erfolgt entlang von fünf Forschungsfragen, die in den Kernkapiteln der Arbeit diskutiert und exemplarisch beantwortet werden:

1. Wie wird Machine Learning von Praktikerinnen und Praktikern verstanden, die ein Kurationsystem trainieren?
2. Welche Annahmen treffen Nutzer eines ML-basierten Kurationsystems, in das sie keine Einblicke haben und das sie nur als Black Box betrachten können?
3. Wie zuverlässig sind die Eingabedaten, mit denen Menschen ein ML-basiertes Kurationsystem trainieren? Und wie hängt diese Zuverlässigkeit mit dem beschränkten Verständnis dieser Systeme zusammen?



4. Wie kann die Funktionsweise dieser Systeme erklärt werden? Hier führt die Erklärungslücke dazu, dass wesentliche Aspekte nicht berücksichtigt, weil nicht verstanden oder von Nutzer:innen und Nutzern in ihrer Bedeutung falsch eingeschätzt werden.

5. Wie kann die Qualität von Kurationsystemen geprüft werden? Vorgestellt wird ein halbautomatisiertes Prüfverfahren, das die Zuverlässigkeit von Vorschlägen zu bewerten hilft.

Zentral für die Entscheidung der Jury war die konsequente Einordnung von Machine-Learning-basierten Kurationsystemen in gesellschaftliche Kontexte, die eben nicht nur aus technischer Sicht, sondern vor allem in ihrem Zusammenhang mit den Menschen, die sie nutzen, und dem gesellschaftlichen Kontext zu betrachten sind. Eine Kernaussage ist, dass Machine-Learning-Systeme auch hier sozio-technische Systeme sind, die falsch oder

unzureichend trainiert werden können, wenn es hier überhaupt ein „richtig“ gibt. Dadurch ergibt sich eine Erweiterung der Perspektive von den Algorithmen hin zu den Daten, die nicht nur von der Maschine, sondern auch von den Menschen ausgewählt und interpretiert werden.

Wir gratulieren ihm zu einer hervorragenden, originellen und gründlichen Arbeit über ein gesellschaftlich hochrelevantes Thema. Es hat eine kritische Begleitung dringend nötig, wofür hier ein wichtiger Baustein gelegt wurde. Wir verstehen den Preis auch als Empfehlung, welche Arbeit wir in diesem Jahr als besonders lesenswert erachten. Dies ist bei dieser Arbeit ohne Zweifel der Fall.

**Herzlichen Glückwunsch, Hendrik Heuer, zum Weizenbaum-Studienpreis 2021.**



Hendrik Heuer

## Warum YouTubes KI gefährlich ist und was wir dagegen tun können

### Zusammenfassung der Dissertation „Users & Machine Learning-based Curation Systems“



1. Preis

*Fake News, Verschwörungstheorien und Filterblasen sind gravierende gesellschaftliche Probleme. YouTube wird immer wieder eine Mitschuld an diesen Problemen gegeben. Mehr als zwei Milliarden Menschen nutzen YouTube jeden Monat und 70 % der dort konsumierten Videos werden von einem KI-System vorgeschlagen. Meine Dissertation untersucht, warum die Künstliche Intelligenz (KI) auf YouTube gefährlich ist und was man dagegen tun kann. Die Arbeit liefert die Grundlage für ein ganzheitliches Verständnis der Systeme, die Videos und Nachrichten empfehlen. Dazu kombiniere ich ein technisches Verständnis mit Einblicken in die Perspektiven der Nutzer:innen, der Entwickler:innen sowie die Perspektive jener, die Daten für solche Systeme liefern. Die Untersuchung zeigt, dass Erklärungen von KI-Systemen für Menschen nicht verständlich sind. Als Alternative dazu beschreibt die Arbeit Untersuchungsverfahren, die sicherstellen können, dass KI-Systeme im Interesse der Öffentlichkeit funktionieren.*

KI ist ein wichtiges Teilgebiet der Informatik. Sie ermöglicht es Computern, Aufgaben zu erledigen, die normalerweise menschliche Intelligenz erfordern. Ein wichtiger Ansatz, der für viele der jüngsten Durchbrüche in der künstlichen Intelligenz verantwortlich ist, ist das so genannte Maschinelle Lernen. Anders als Logik-basierte KI-Ansätze versucht man beim Maschinellen Lernen, mittels statistischer Verfahren aus Daten zu lernen. Dank der Techniken des Maschinellen Lernens ist es mittlerweile möglich, Sätze von einer Sprache in eine andere zu übersetzen, Personen und Objekte in Bildern zu erkennen oder Autos autonom fahren zu lassen. Plattformen wie YouTube nutzen die Techniken des Maschinellen Lernens, um automatisiert Videos auszuwählen, die für Nutzer:innen besonders interessant sind. Im Jahr 2019 wurden durchschnittlich 500 Stunden an Inhalten pro Minute bei YouTube hochgeladen. Auf den Tag gerechnet sind das 82,2 Jahre Videomaterial. Für ein Team menschlicher Expert:innen wäre es unmöglich, diese von Nutzer:innen hochgeladenen Inhalte zu überprüfen und zu kategorisieren. Social Media-Plattformen setzen daher KI-Techniken wie Maschinelles Lernen ein, um Videos zu kategorisieren und zu empfehlen. Solche Empfehlungssysteme sind sehr erfolgreich. 70 % der Videos, die die zwei Milliarden Menschen gucken, die YouTube jeden Monat nutzen, werden von diesem KI-System ausgewählt.



Hendrik Heuer beim Vorstellen seiner Dissertation

YouTube wurde von Journalist:innen immer wieder beschuldigt, Fake News und Verschwörungstheorien zu verbreiten. Ein wichtiges Beispiel für diesen Vorwurf sind die rechtsradikalen Ausschreitungen in Chemnitz im Jahr 2018. Bei einer Auseinandersetzung im Rahmen des Chemnitzer Stadtfestes wurde ein Mann durch Messerstiche tödlich und zwei weitere Personen wurden schwer verletzt. Rechte und rechtsextreme Gruppen instrumentalisierten den Vorfall mit Blick auf die vermeintliche Herkunft des Täters und riefen zu Aufmärschen auf. Einem Bericht der



New York Times zufolge schlossen sich viele Bürger:innen den rechten Aufmärschen an, nachdem sie sich auf YouTube über die Geschehnisse informiert und vom ML-basierten Empfehlungssystem immer rechtsradikalere Videos empfohlen bekommen haben. Meine Doktorarbeit ist in mehrfacher Hinsicht durch diese Vorfälle und den politischen Schock motiviert, den sie ausgelöst haben. Die Vorfälle zeigen, dass es wichtig ist zu verstehen, ob sich die Nutzer:innen der Tatsache bewusst sind, dass sie es mit Empfehlungssystemen zu tun haben. Deshalb wollte ich untersuchen, ob und wie gut Nutzer:innen verstehen, wie solche Systeme funktionieren. Es ist außerdem wichtig zu untersuchen, wie und ob solche Systeme kontrolliert werden können.

Die Arbeit ist insbesondere deshalb relevant, da repräsentative Umfragen zeigen, dass mehr als 80 % der Menschen weltweit ihre Nachrichten online konsumieren. Soziale Medien werden von mehr als der Hälfte der Menschen als Nachrichtenquelle genannt. YouTube wird von jeder vierten Person weltweit genutzt, um Nachrichten zu schauen. Ein sozio-technisches Verständnis derartiger Systeme ist deshalb von gesamtgesellschaftlicher Bedeutung. Unternehmen wie Google, Facebook, Twitter, LinkedIn, Netflix, Amazon, Microsoft, Spotify und viele andere setzen derartige Systeme auf vielfältige Weise ein. Meine Ergebnisse stellen einen wichtigen Beitrag zur Erklärung dieser KI-Systeme dar.

## ML-basierte Empfehlungssysteme

Automatisierung ist ein Kernversprechen der künstlichen Intelligenz. Insofern stellt sich die Frage: Wenn Automatisierung das Ziel ist, warum müssen Nutzer:innen ML-basierte Empfehlungssysteme verstehen? Die erste Antwort auf diese Frage steht im Zusammenhang mit den Herausforderungen, die mit der Anwendung von Maschinellem Lernen verbunden sind. Wie in der Arbeit dokumentiert, neigen Maschinelle Lernsysteme dazu, zu unerwarteten Zeitpunkten und bei unvorhersehbaren Eingaben Fehler zu machen. Deshalb müssen Nutzer:innen Situationen erkennen können, in denen ein System nicht das gewünschte Ergebnis liefert. Die zweite Antwort bezieht sich auf den Anwendungsfall. Die Empfehlungen auf YouTube beeinflussen den Medienkonsum der Nutzer:innen. Deshalb müssen Nutzer:innen wissen, dass sie es mit einem KI-System zu tun haben, das aktiv versucht, ihre Empfehlungen zu personalisieren. Personalisierung heißt, dass die Empfehlungen genau auf die Vorlieben und Interessen der Nutzenden zugeschnitten werden.

Empfehlungssysteme für Nachrichten und Videos sind eine Weiterentwicklung von Empfehlungssystemen, wie sie auch für Produkte auf Amazon oder für Musik auf Spotify genutzt werden. Im Hinblick auf Musikempfehlungen kann es für eine Nutzerin oder einen Nutzer wünschenswert sein, wenn er oder sie Musik empfohlen bekommt, die genau der Musik entspricht, die sie bereits gehört haben. Im Musikkontext kann es positiv sein, dass jemandem, der Bob Dylan mag, zunehmend Folkmusik empfohlen wird. Dieses Szenario wird in der Fachliteratur auch Filterblase genannt. In Hinblick auf Nachrichten kann dies allerdings hochgradig problematisch sein. Nehmen wir folgendes Beispiel zur Illustration. Ein Nutzer könnte zufällig ein Video über einen Verbrecher mit Migrationshintergrund sehen. Das Empfehlungssystem könnte daraufhin weitere Videos über Verbrecher:innen

mit Migrationshintergrund empfehlen. Genauso wie das System jemandem, der gerne Bob Dylan hört, weitere Lieder von Bob Dylan empfehlen würde. Während dies bei Musik positiv und gewollt sein kann, ist dies in Hinblick auf Nachrichten ein ernstzunehmendes Problem. Der Nutzer könnte fälschlicherweise glauben, dass ein Empfehlungssystem eine „objektive Realität“ repräsentiert und dass Menschen mit Migrationshintergrund häufiger Verbrechen begehen. Dabei sind die Videos, die YouTube empfiehlt, nur das Ergebnis einer Koproduktion zwischen den Handlungen der Nutzer:innen und der Fähigkeit des Empfehlungssystems, Interessen zu bedienen.

Die Doktorarbeit im Forschungsfeld Mensch-Maschine-Interaktion zeigt, dass ein Empfehlungssystem mehr als ein Algorithmus ist. Die Arbeit untersucht Empfehlungssysteme als sozio-technische Systeme, die immer von und mit Nutzer:innen in bestimmten Kontexten verstanden und untersucht werden müssen. Vom Grundprinzip her sind Empfehlungssysteme Spam-Filtern sehr ähnlich. Spam-Filter erhalten Eingaben wie den Absender, den Betreff und den Text einer E-Mail und generieren daraus eine Ausgabe. Die Ausgabe ist beispielsweise die Einschätzung, ob eine E-Mail als Spam eingestuft wird oder nicht. Ein Empfehlungssystem entscheidet, ob eine Nachricht für die Nutzer:innen interessant ist oder nicht. Allerdings ist bislang wenig darüber bekannt, worauf diese Einschätzung basiert und inwiefern Nutzer:innen verstehen, warum sie bestimmte Empfehlungen bekommen. Meine Dissertation befasst sich deshalb mit dem Verständnis von ML-basierten Empfehlungssystemen. Startpunkt ist dabei, wie Expert:innen Machine Learning verstehen. Dazu wurden mehr als vierzig Anleitungen analysiert, in denen ML erklärt wird. Die Dissertation zeichnet sich hier besonders dadurch aus, dass ich Nutzer:innen mittleren Alters ohne technischen Hintergrund aus drei verschiedenen Ländern befragt habe. Neben Nutzer:innen aus Deutschland wurden auch Nutzer:innen aus Belgien und Costa Rica befragt. Dies ermöglicht ein Verständnis, das über die Kultur eines einzelnen Landes hinausgeht.

Basierend auf dem Verständnis von KI untersuche ich verschiedene Erklärungen, die die Funktionsweise von Empfehlungssystemen nachvollziehbar machen sollen. Ein zentrales Ergebnis dieser Untersuchung ist es, dass Erklärungen nur sehr wenig nützen. Keines der von mir entwickelten Werkzeuge konnte das Verständnis erhöhen. Ein wichtiger theoretischer Beitrag der Doktorarbeit ist die von mir erkannte „Erklärungslücke“ in Empfehlungssystemen. Als Alternative beschreibt und evaluiert die Arbeit Untersuchungsverfahren, mit denen solche Systeme dennoch kontrolliert werden können.

## ML-basierte Empfehlungssysteme verstehen

Der Beitrag meiner Doktorarbeit besteht darin, Machine Learning-basierte Empfehlungssysteme ganzheitlich sowohl in Hinblick auf ihre technische Funktionsweise als auch auf das Verständnis von Nutzer:innen zu beschreiben. Die beschriebenen theoretischen Grundlagen der Vorstellung von Nutzer:innen ermöglichen ein differenzierteres Verständnis von ML-basierten Empfehlungssystemen und ihren verschiedenen Komponenten. So können Expert:innen und Laien die verschiedenen Aspekte besser verstehen, die für die Untersuchung komplexer sozio-technischer ML-Systeme relevant sind. Basierend auf diesen



theoretischen Grundlagen gestalte und evaluiere ich konkrete Empfehlungen für die Erklärung derartiger Systeme. Die Doktorarbeit zeigt deutlich, dass selbst verhältnismäßig einfache Erklärungen für Nutzer:innen nicht hilfreich und verständlich sind. Als Alternative zu diesen für Nutzer:innen nicht verständlichen Erklärungen beschreibe ich systematische Untersuchungsverfahren mittels Bots. Bots sind Programme, die Nutzer:innen simulieren und Daten über das Verhalten eines Systems sammeln können. Die Arbeit zeigt, dass Expert:innen mittels solcher Verfahren ohne Zugang zum Quellcode eines Systems überprüfen können, ob das System politisch zunehmend radikalere Inhalte empfiehlt oder bestimmte Minderheiten systematisch benachteiligt, was insbesondere für den Fall in Chemnitz interessant ist.

Meine Dissertation liefert eine theoretische Grundlage dafür, zu verstehen, wie Nutzer:innen sich erklären, warum sie bestimmte Empfehlungen sehen. Die Ergebnisse zeigen, dass Nutzer:innen zwar annehmen, dass es ein System gibt, das ihre Empfehlung beeinflusst. Sie haben aber keine klare Vorstellung davon, warum sie die Empfehlungen sehen. Auch wenn ihnen Erklärungen zu einem ML-Modell präsentiert werden, verstehen sie das KI-System nicht besser, weil wenig darüber bekannt ist, wie die ML-basierten Empfehlungssysteme auf Plattformen wie YouTube funktionieren. Die Arbeit beschreibt, wie die Vorstellungen der Nutzer:innen genutzt werden können, um bessere und verständlichere Erklärungen für die Empfehlungen ML-basierter Systeme zu gestalten. Die Arbeit bietet außerdem wichtige Einblicke in das Verständnis der Expert:innen, die die Techniken des Maschinellen Lernens anwenden. Darüber hinaus offenbart die Arbeit wichtige Einschränkungen in der Fähigkeit von Nutzer:innen, qualitativ hochwertige Trainingsdaten für ML-basierte Systeme im Kontext von Fake News zu liefern.

### Empfehlungssysteme erklären und kontrollieren

Die Dissertation zeigt, dass verschiedene einfache, intuitive und interaktive Erklärungen selbst Journalist:innen nicht helfen, besser zu verstehen, warum ihnen bestimmte Nachrichten empfohlen werden. Meine Forschungsergebnisse beschreiben eine „Erklärungslücke“ zwischen dem, was zur Erklärung ML-basierter Empfehlungssysteme zur Verfügung steht, und dem, was Nutzer:innen zum Verständnis brauchen. Die Dissertation macht deutlich, dass die Entwicklung und Bewertung der Erklärungen ML-basierter Empfehlungssysteme komplex ist. Aus der Erklärungslücke lassen sich zwei Dinge ableiten: (1) die technischen Mittel zur Erklärung ML-basierter Systeme müssen verbessert werden, und (2) das Verständnis der Nutzer:innen für solche

Systeme muss verbessert werden. Meine Dissertation zeigt außerdem, wie entscheidend es ist, ML-Erklärungen in Studien zu evaluieren. Die Ergebnisse werfen die Frage auf, ob ML-basierte Entscheidungen überhaupt auf eine Weise erklärt werden können, die für Nutzer:innen zugänglich ist.

Die Erklärungslücke hat mich dazu motiviert, alternative Lösungen zu suchen, um ML-basierte Systeme transparent zu machen. Meine Forschung zeigt, dass eine gründliche Analyse der Empfehlungen mittels systematischer Untersuchungsverfahren sinnvoll ist. Dazu werden Videoempfehlungen systematisch heruntergeladen und analysiert. Sie lassen sich dann so anpassen, dass Videos aller Menschen – unabhängig von Ethnie, Geschlecht oder politischer Meinung – empfohlen werden. So haben auch Minderheiten eine Chance, auf YouTube wahrgenommen zu werden. Die Doktorarbeit zeigt, dass solche Verfahren die Unzulänglichkeit der Erklärungen überwinden und das gesellschaftliche Vertrauen in Empfehlungssysteme erhöhen können. Dieses Vertrauen ist notwendig angesichts des sozialen, politischen und wirtschaftlichen Einflusses, den ML-basierte Empfehlungssysteme auf das Leben von Milliarden von Menschen haben. Da die Bedeutung von solchen Empfehlungssystemen in Zukunft nur noch zunehmen wird, wird die Erklärung und Prüfung von ML-basierten Empfehlungssystemen noch wichtiger werden.

Die Doktorarbeit veranschaulicht, wie Untersuchungsverfahren genutzt werden können, um zu untersuchen, ob YouTube wirklich systematisch politisch radikalere Inhalte empfiehlt, wie von der New York Times im Fall Chemnitz angenommen. Die Arbeit untersucht die Empfehlungen, die YouTube für eine Vielzahl politisch relevanter Themen macht. Für die Fälle, die ich analysiere, werden die Empfehlungen nicht radikaler. Vielmehr empfiehlt YouTube systematisch populärere Inhalte, gemessen an den Aufrufen und den Likes der Videos. Gleichzeitig zeigt meine Untersuchung, dass YouTube Empfehlungssystem keinen Minderheitenschutz gewährleistet, wie ihn deutsche Gesetze wie der Rundfunkstaatsvertrag fordern. Insgesamt zeigt meine Arbeit, dass das Risiko von Filterblasen möglicherweise nicht die größte Gefahr darstellt. Vielmehr ist die mögliche Unterdrückung von Minderheitsmeinungen ein akuteres Problem für die demokratische Meinungsbildung. Die Ergebnisse der Arbeit illustrieren, wie die von mir vorgestellten Untersuchungsverfahren systematische Verzerrungen aufdecken können. Solche Verzerrungen können die politischen Überzeugungen und Handlungen von Menschen beeinflussen, was sich negativ auf das demokratische Gemeinwesen auswirken kann. Deshalb schließe ich die Arbeit mit einer Skizze einer Institution des öffentlichen Rechts, die

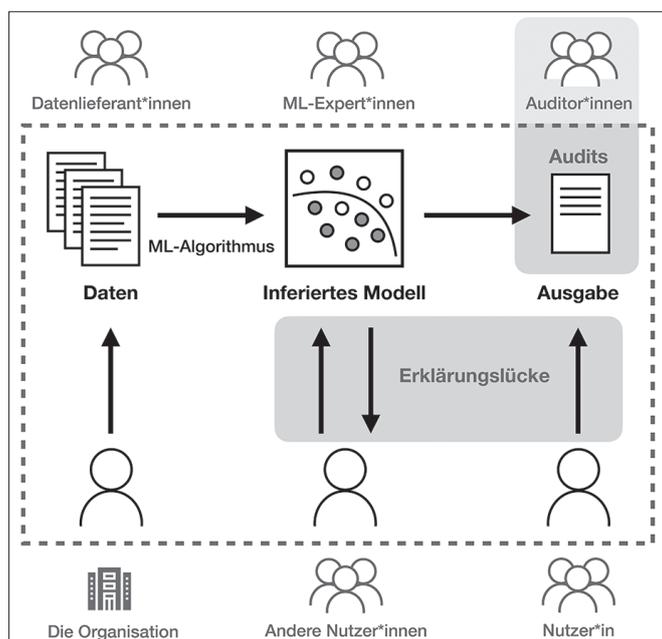
**Hendrik Heuer**



Foto Cosima Hanebeck

**Hendrik Heuer**, Dr.-Ing., ist wissenschaftlicher Mitarbeiter am Institut für Informationsmanagement Bremen (ifib) und Zentrum für Medien-, Kommunikations- und Informationsforschung (ZeMKI) an der Universität Bremen. Seine Forschungsschwerpunkte sind Mensch-Computer-Interaktion und Maschinelles Lernen. Derzeit arbeitet er an Möglichkeiten zur Bekämpfung von Desinformation. Darüber hinaus versucht er Texte für Menschen mit Behinderungen zugänglicher zu machen. Er hat Digitale Medien, Mensch-Computer-Interaktion und Maschinelles Lernen in Bremen, Buffalo, Stockholm, Helsinki und Amsterdam studiert.

analog zu TÜV und Stiftung Warentest sicherstellt, dass zentrale ML-basierte Empfehlungssysteme im Interesse des demokratischen Gemeinwohls agieren. Diese Institution soll Expert:innen zusammenbringen, die Anforderungen an ein ML-basiertes System sammeln. Durch die von mir beschriebenen Untersuchungsverfahren lässt sich feststellen, wo ein System den Anforderungen entspricht und wo nachgebessert werden muss.



Ein sozio-technisches Modell eines ML-basierten Kurationsystems. Das Modell stellt die in dieser Arbeit erkannten Akteur:innen und die Erklärungslücke und Audits dar. Das Icon für die Organisation stammt von Freepik und [www.flaticon.com](http://www.flaticon.com)

Die Abbildung bietet eine Übersicht über die Akteur:innen, die für die Untersuchung von ML-basierten Kurationsystemen relevant sind. Neben den Nutzer:innen, den Daten, dem ML-Algorithmus, dem inferierten Modell und der Ausgabe des ML-Systems werden in meiner Dissertation fünf weitere Akteur:innen beschrieben, die ML-basierte Kurationsysteme beeinflussen:

- die Organisation, die das System betreibt
- andere Nutzer:innen, z. B. in den sozialen Medien
- Datenlieferanten, die die Eingabe-Daten für das Training der ML-Systeme liefern
- ML-Praktiker:innen, die das ML-basierte System entwickeln und evaluieren
- Auditor:innen, die die Ausgabe von ML-basierten Systemen systematisch überprüfen.

Es ist wichtig, diese verschiedenen Akteure, ihre Verantwortlichkeiten und ihre Ziele zu untersuchen, um ihre Handlungsmacht (Agency) zu erkennen und um zu verstehen, wie ML-basierte Kurationsysteme erklärt und kontrolliert werden können und sollten.

## Fazit

Die Doktorarbeit bietet eine ganzheitliche sozio-technische Perspektive auf ML-basierte Empfehlungssysteme. Sie stellt theoretische Grundlagen zur Verfügung, um die Besonderheiten des Maschinellen Lernens kritisch zu reflektieren. Die Dissertation zeigt, dass *der Algorithmus*, der in der bisherigen Forschung eine wichtige Rolle spielt, nur Teil eines größeren sozio-technischen Systems ist. Zu diesem System gehört auch der Einfluss der Nutzer:innen, der Daten, des ML-Modells und der Benutzungsschnittstelle. Darüber hinaus spielt auch die Organisation eine wichtige Rolle, die das ML-basierte Empfehlungssystem betreibt. Meine Forschung zeigt, dass auch andere Nutzerinnen und Nutzer einer Social-Media-Seite sowie die Datenzulieferer, die Trainingsdaten für die KI bereitstellen, einen wichtigen Einfluss haben. Darüber hinaus untersucht die Arbeit die Rolle der ML-Expert:innen, die die Systeme trainieren. In der Dissertation erkläre ich im Detail, warum es wichtig ist, diese verschiedenen Akteure, ihre Verantwortlichkeiten und ihre Ziele zu verstehen. Ich biete außerdem konkrete Empfehlungen, wie ML-basierte Empfehlungssysteme erklärt und kontrolliert werden sollten.

Die Arbeit zeigt, warum YouTubes Möglichkeit zur Beeinflussung von Nutzer:innen eine Gefahr darstellt. Dies ist insbesondere für diejenigen wichtig, denen nicht bewusst ist, dass sie Empfehlungen bekommen. Es richtet sich aber auch an Nutzer:innen, die nicht verstehen, warum sie bestimmte Empfehlungen bekommen. Da sich Erklärungen der KI als nur bedingt hilfreich erwiesen haben, zeigt die Arbeit, wie derartige Systeme durch die systematische Analyse von Empfehlungen kontrolliert werden können. Meine Untersuchungen zeigen, dass die von mir beschriebenen Untersuchungsverfahren ein Weg sind, um Rechenschaftspflicht für Künstliche Intelligenz durchzusetzen. So kann sichergestellt werden, dass ML-basierte Systeme diskriminierungsfrei und zum Wohle aller arbeiten.

Die Arbeit wurde von Andreas Breiter (Universität Bremen) und Elena L. Glassman (Harvard University) betreut. Sie können die Arbeit über die Staats- und Universitätsbibliothek Bremen kostenlos als eBook herunterladen (Open Access): Heuer, H., 2020. Users & Machine Learning-Based Curation Systems (Universität Bremen). <https://media.suub.uni-bremen.de/handle/elib/4444>

## Referenzen

- Alvarado O, Heuer H, Vanden Abeele V, Breiter A, Verbert K (2020) Middle-Aged Video Consumers' Beliefs About Algorithmic Recommendations on YouTube. Proceedings of the ACM on Human-Computer Interaction, 4(CSCW2).
- Heuer H, Breiter A (2018) Trust in news on social media. Proceedings of the 10th Nordic conference on human-computer interaction (pp. 137-147).
- Heuer H, Hoch H, Breiter A, Theocharis Y (2021) Auditing the Biases Enacted by YouTube for Political Topics in Germany. Mensch und Computer 2021.
- Heuer H, Jarke J, Breiter A (2021) Machine learning in tutorials—Universal applicability, underinformed application, and other misconceptions. Big Data & Society.
- Heuer H (2021) The Explanatory Gap in Algorithmic News Curation. MIS-DOOM 2021.



## Helene Hahn: Digital identification systems and the right to privacy in the asylum context: An analysis of implementations in Germany

Masterarbeit an der Leuphana-Universität Lüneburg



Es kann viele Gründe geben, warum Menschen nach Deutschland kommen und bei uns Schutz suchen. Kriege, Menschenrechtsverletzungen, und ja, auch wirtschaftliche Gründe, bei Menschen, die zum Teil in bitterer Armut leben. Der beschleunigte Klimawandel und seine Folgen werden weitere Menschen zwingen, ihre Heimat zu verlassen und in andere Länder umzusiedeln.

Ob, wie und nach welchen Kriterien darüber entschieden wird, wer in Europa aufgenommen wird, ist eine menschenrechtliche, aber auch eine politische Frage. Das Bundesministerium des Innern, für Bau und Heimat beschreibt die Ziele seiner Migrationspolitik so:

*„Die Migrationspolitik der Bundesrepublik Deutschland dient der Steuerung, Kontrolle und Begrenzung des Zugangs von Ausländern in unser Land. Dabei sind die Aufnahme- und Integrationsfähigkeit unserer Gesellschaft sowie unsere wirtschaftlichen und arbeitsmarktpolitischen Interessen zu berücksichtigen. Zugleich dient die Migrationspolitik der Erfüllung unserer humanitären Verpflichtungen.“*

Wie auch immer wir diese Fragen entscheiden – eine Voraussetzung für die einschlägigen Verfahren in den Behörden ist es, die Identität der Menschen zu kennen, die ein Bleiberecht suchen. Liegen keine amtlichen Dokumente darüber vor, versucht das Bundesamt für Migration und Flüchtlinge (BAMF), die Identität auf anderem Wege festzustellen. Dazu wurde das IDM-S – *Integrated Identity Management – plausibility, data quality and security aspects* entwickelt. Dessen Ziele bestehen darin, die Qualität der Daten über Antragsstellerinnen und Antragsteller zu verbessern, ihre Informationen zu plausibilisieren und die Verschleierung der Identität zu erschweren. Bereitgestellte Werkzeuge umfassen Namenstranskription, Sprachbiometrie, Bildbiometrie und das Auslesen mobiler Datenträger. Dabei werden auch Methoden des Machine Learning und der sogenannten Künstlichen Intelligenz eingesetzt.

Ganz offensichtlich ergeben sich Fragen zum Persönlichkeitsrecht, zur individuellen Privatheit und zum gesellschaftlichen Datenschutz. Derartige Verwaltungsverfahren und Methoden bedürfen immer einer Legitimation – damit sind wir bei der Arbeit von Helene Hahn – *Digital identification systems and the right to privacy in the asylum context: An analysis of implementations in Germany*, die wir heute mit dem zweiten Preis des Weizenbaum-Studienpreises 2021 auszeichnen.

Die Arbeit setzt sich mit der Frage auseinander, wie das BAMF Methodik und Nutzung des Digitalen Identifikationssystems IDM-S als Teil einer neuen Ausrichtung der Governance im Asylkontext zu legitimieren sucht.



Laudator Rainer Rehak

Die Betreiber geben als Legitimation für den Einsatz des Verfahrens vier Aspekte an:

- Gesetzliche Regelungen und nationale Sicherheitsinteressen,
- Verschweigen delegitimierender Informationen und begrenzte Glaubwürdigkeit,
- Effizienz des Prozesses,
- hohes Innovationsniveau und Objektivität durch den mathematisch-technischen Ansatz.

In der Arbeit werden diese Aspekte einer kritischen Überprüfung unterzogen, mit den folgenden Ergebnissen und Feststellungen:

- Die entsprechenden Gesetze wurden zu schnell auf den Weg gebracht und es wurden dabei wichtige Verfahrensregeln, wie Fristen für Eingaben, nicht eingehalten.
- Auch bei der Umsetzung wurden bezüglich Datenschutz, Privatsphäre und Behandlung Asylsuchender nicht alle geltenden Gesetze beachtet.
- Es gab keine ausreichenden Abklärungen, ob es datenschutzfreundlichere Möglichkeiten gegeben hätte. Damit wurde ein weiteres Mal IT als ein Allheilmittel für Probleme betrachtet.
- Das System wurde sehr schnell umgesetzt unter Rückgriff auf externe Dienstleister. Vieles dabei geschah intransparent, die Implementation war teurer als geplant, aber es wurde als Erfolg verkauft.
- Nachdem das Projekt als Erfolg verkauft worden war, entstand offenbar ein Erfolgsdruck für den praktischen Einsatz. Ein Zurücktreten davon ist dadurch kaum mehr möglich.

- Es gibt begründete Zweifel an der Korrektheit der Ergebnisse bei der Nutzung von IDM-S.

Neben diesen Kritikpunkten am System sind auch Zweifel an den dazugehörigen Prozessen angebracht:

- Auch wenn viel in die Entwicklung investiert wurde, flossen offenbar zu wenig Ressourcen in die Ausbildung derer, die das Ergebnisse interpretieren und Entscheidungen nutzen sollen. Diese werden nicht ausreichend befähigt, Ergebnisse richtig einzuschätzen. Zwar wird behauptet, die Entscheidungen würde letztens der Mensch treffen, aber wenn diese die Ergebnisse nicht richtig einschätzen können und unter Zeitdruck stehen, steht die Qualität solcher Entscheidungen in Frage.
- Auch wenn die Ergebnisse der Analyse nur nach Bewilligung durch eine Rechtsanwält:in zu Rate gezogen werden dürfen, gibt es keine Regeln, die erfordern, dass dieser unabhängig ist und es nicht der/die Sachbearbeiter:in selbst sein darf.

In der immer noch aufgeheizten politischen Debatte behandelt die Arbeit ein Thema von hoher Aktualität und Bedeutung – In-diz dafür ist vielleicht auch, dass wir bereits zum zweiten Mal eine Arbeit auszeichnen, die sich mit dem Themenkomplex der Migration und der zu deren Steuerung eingesetzten IT-Systeme auseinandersetzt. Auch wenn die aktuell betrachtete Arbeit selbst kaum technisch auf das betrachtete System IDM-S selbst eingeht, beschreibt sie anhand dieses Beispiels sehr gut prototypische Probleme, die genau so auch bei anderen Systemen vorliegen und ist in diesem Sinne auch verallgemeinerbar. Gerade die detaillierte Dokumentation der Diskussionen und Prozesse stellen einen großen Beitrag und Wert der Arbeit dar. In der Einleitung stellt sie sehr überzeugend die Grundlagen zu politischer Legitimität, Privatheit und Governance vor. Die Arbeit beinhaltet darüber hinaus eine gute Quellenstudie und zahlreiche belegende Zitate der Akteure. Die Jury hat sich deswegen einhellig für die Auszeichnung entschieden.

**Herzlichen Glückwunsch, Helene Hahn, zum Weizenbaum-Studienpreis 2021.**



Helene Hahn

## Digitale Identifikationssysteme und das Recht auf Privatsphäre im Asyl-Kontext

### Eine Analyse der Umsetzungen im Bundesamt für Migration und Flüchtlinge



2. Preis

*Seit 2017 setzt das Bundesamt für Migration und Flüchtlinge verschiedene IT-Assistenzsysteme bei der Identitätsfeststellung von asylsuchenden Menschen ein. Das Integrierte Identitätsmanagement – Plausibilität, Datenqualität und Sicherheitsaspekte (IDM-S) analysiert u. a. die Namen sowie Dialekte und wertet mobile Datenträger aus. Der Einsatz derartiger technischer Systeme und wissenschaftlich fraglicher Analyse-Methoden, die tief in die Rechte betroffener Personen eingreifen, ist zutiefst umstritten.*

#### Einsatz technischer Systeme in vulnerablen Settings

Dass staatliche Behörden technische Systeme im Kontext von Migration und Asyl einsetzen, lässt sich an verschiedenen Entwicklungen in der EU beobachten. So setzt etwa Norwegen auf das Screening von Social-Media-Profilen von asylsuchenden Menschen (Brekke und Staver, 2019) und die EU übt sich im *EU Horizon 2020* geförderten Projekt *iBorderCtrl* in der Entwicklung von computergestützten Avataren, die anhand von Gesichtszügen einer Person erkennen sollen, ob wahrheitsgemäße Angaben bei der Einreise gemacht werden oder nicht (Sánchez-Monedero und Dencik, 2020).

Aus politischer Sicht geht es darum, durch sogenannte *innovative Technologien* Kontrolle über Migration auszuüben, einen noch restriktiveren Grenzschutz sicherzustellen und Entscheidungen im Kontext von Asyl datenbasiert abzuleiten. Auch in Deutschland werden neue technikgestützte Entwicklungen im Bereich der Governance deutlich: Experimentell eingesetzte algorithmische Systeme begleiten die immer strengeren Asylverfahren und verschärften Asylantragsbedingungen, die durch viele neue Gesetze eingeführt wurden. Allein ab 2015 wurden in Deutschland durch die Asylpakete I und II über 20 Asylgesetze

oder ihre Anpassungen erlassen, darunter die Ausweitung des Ausländerzentralregisters und der Zugriffsbefugnisse auf sensible Daten asylsuchender Menschen durch staatliche Behörden, die Abschiebung ohne Ankündigung und die Residenzpflicht für Asylbewerber:innen (Grote, 2018).

Im Jahr 2015 stellten fast eine halbe Million Menschen einen Asylantrag in Deutschland, doppelt so viele wie im Vorjahr. Die Dauer der Asylverfahren betrug fast acht Monate (BAMF, 2016: 11). Das Bundesamt für Migration und Flüchtlinge (BAMF) geriet politisch und öffentlich unter Druck: Nach innen bemängelten Personalräte des BAMF die „Schnellschuss-Qualifizierung“ der Entscheider:innen in Asylverfahren und verwiesen auf „systematische Mängel“ in einem offenen Brief (Scheinost und Hüter, 2015: 1). Nach außen wurde das Bundesamt durch zahlreiche journalistische Recherchen als eine überforderte Behörde dargestellt (Jehle, 2016; Bock, 2015).

In diesem Kontext setzte das BAMF massiv auf Digitalisierung. Mit der Einführung des IDM-S sollten die Qualität der Asylentscheidungen erhöht und Verfahren beschleunigt werden (BAMF, 2017b). IDM-S basiert auf verschiedenen IT-Assistenzsystemen, darunter Namens-Transliteration und -analyse, Sprachbiometrie sowie der Auswertung mobiler Datenträger. Seit 2017 wer-



den diese Systeme im Rahmen der Identitätsfeststellung und -verifikation in Ankunftszentren und Außenstellen des BAMF eingesetzt. Jedes dieser drei Systeme analysiert personenbezogene Daten von asylsuchenden Menschen und erstellt Ergebnisberichte, die von Entscheider:innen des BAMF genutzt werden können. Die Analysen dieser Berichte sollen bei der Entscheidungsfindung – ob Asyl gewährt wird oder nicht – datenbasiert unterstützen (BAMF und BFM, 2017).

### Kritische Reflexion dringend notwendig

Das Experimentieren mit umstrittenen digitalen Identifikationsmethoden führt im Bereich Migration und Asyl zu einer zunehmenden Macht von staatlichen Behörden gegenüber besonders schutzbedürftigen Personen, deren Rechte und Freiheiten bedroht und eingeschränkt werden (Molnar, 2018a; Molnar, 2018b). Nicht selten verlieren Betroffene die Kontrolle und Entscheidungsmöglichkeiten über ihre sensiblen und persönlichen Daten (Kaurin, 2019). Zudem weisen solche Systeme durch technische Voreingenommenheit und die ihrer Anwender:innen Bias auf, die unrechtmäßige Praktiken verstärken können und politische Interessen umso mehr in den Vordergrund stellen (Latorero, Hiatt, Napolitano, Clericetti und Penagos, 2019).

Asylsuchende Menschen gehören durch ihre prekäre Lage *per se* zu vulnerablen Gruppen, die besonderen Schutzes bedürfen (ECTHR, 2011: Case of M.S.S v. Belgium and Greece, para. 251). Sie haben weniger Zugang zu solidem Menschenrechtsschutz und gleichzeitig weniger Ressourcen, um ihre Rechte zu verteidigen. Sprachbarrieren und unzureichende Kenntnisse lokaler Regierungssysteme benachteiligen sie zusätzlich, was zu Machtungleichgewichten vor allem gegenüber Behörden führt. Nicht selten haben asylsuchende Menschen durch ihre Fluchtgeschichte mit traumatischen Erlebnissen zu kämpfen, wenn sie etwa Folter und Menschenhandel ausgesetzt waren oder aufgrund ihres Geschlechts oder ihrer sexuellen Orientierung verfolgt werden. Umso wichtiger ist es, dass Staaten die Vulnerabilität individuell einschätzen und Maßnahmen in Asylverfahren besonders sensibel umsetzen. Technische Verfahren müssen daher genauso kritisch auf Eignung hinterfragt und evaluiert werden wie bereits etablierte, um u. a. Retraumatisierungen zu vermeiden.

Staaten und Regierungen tragen die primäre Verantwortung für die Einhaltung, Umsetzung und den Schutz von Menschenrechten, zu denen sie nach internationalen Standards verpflichtet sind. Die Entscheidung, digitale Identifikationssysteme in einem Land zu implementieren, kann ein Vorbild für andere Länder setzen und durch den Export solcher Systeme zu Menschenrechtsverletzungen auch außerhalb der eigenen Ländergrenzen führen. Darüber hinaus kann der unverhältnismäßige Fokus auf technologische Trends bei der Suche nach Lö-

sungen für komplexe soziale Probleme dafür sorgen, dass Alternativen außerhalb des digitalen Bereichs aus dem Blick geraten, die besser für bestehende Herausforderungen geeignet sind. Ein kritischer und umsichtiger Umgang mit der Entwicklung und dem Einsatz digitaler Systeme ist daher eine wesentliche Voraussetzung für gerechtes, demokratisches Staatshandeln und somit relevant für Entscheidungsträger:innen in der Politik. Angesichts der möglichen und realen Folgen für Betroffene muss es eine gelebte Option geben, risikobehaftete Systeme nicht zu implementieren.

### Die IT-Assistenzsysteme des BAMF als Teil von IDM-S

*TraLitA*, der *Transliterations-Assistent*, transkribiert Namen in die lateinische Schreibweise nach einheitlichen Vorgaben, um potenzielle Fehler bei der Transliteration zu vermeiden und Folgekorrekturen zu minimieren. An einem Computer geben Betroffene ihr Herkunftsland und ihren vollständigen Namen ein. Anschließend wird eine Analyse der Herkunftsregion auf der Grundlage des erfassten Namens durchgeführt. Das Ergebnis soll zeigen, wie häufig ein Name in einem oder mehreren Ländern vorkommt. Im Bericht der Analyse wird je nach Treffer beispielsweise festgehalten: „Der Name kommt im angegebenen Land [Syrien] [selten/sehr selten] vor. In [den Ländern/dem Land] [Libyen, Algerien und Marokko] kommt er hingegen häufiger vor.“ (BAMF, 2018a: 3.4) Die Namens-Transkription wird standardmäßig bei allen Personen mit arabischen Namen eingesetzt – unabhängig von vorhandenen Identitätsdokumenten.

*DIAS*, der *Dialektbestimmungs-Assistent* oder Sprachbiometrie gleicht Sprechproben mit einem zugrunde liegenden Sprachmodell ab. Er ordnet den Dialekt der betroffenen Person einer bestimmten Region zu. Derzeit wird das System dann eingesetzt, wenn Personen einen der fünf arabischen Großdialekte

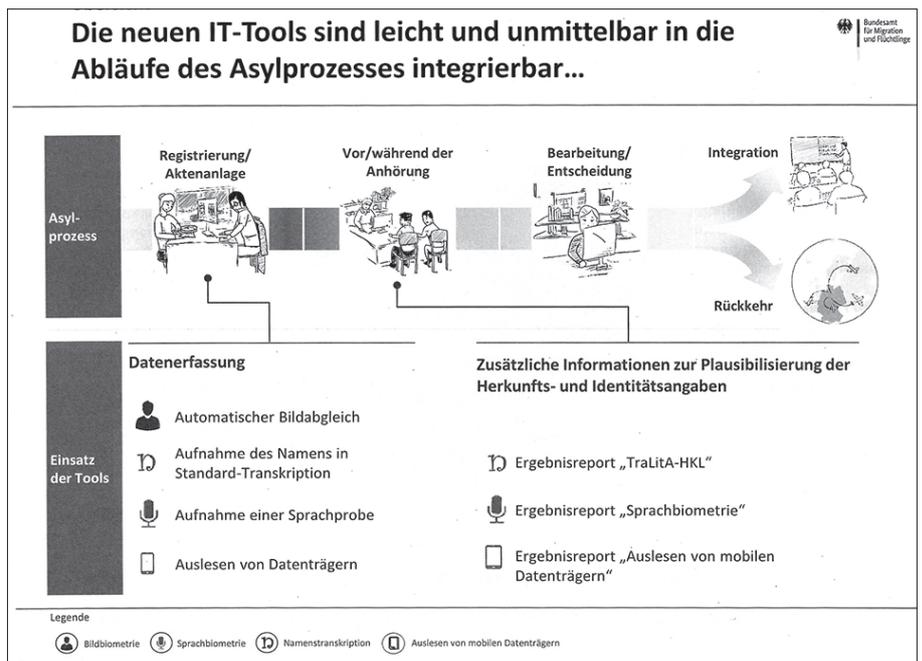


Abbildung 1: Einbettung von IDM-S im Asylverfahren. Quelle: BAMF, 2017a: Integriertes Identitätsmanagement – Plausibilisieren, Datenqualität und Sicherheitsaspekte. Einführung in die neuen IT-Tools



sprechen: Maghrebinisch, Ägyptisch, Irakisch, Levantinisch und Golf (BAMF, 2018b: 3.2). Beim Einsatz der Sprachbiometrie werden Asylbewerber:innen dazu aufgefordert, am Telefon ein oder mehrere bereitgestellte Bilder in ihrer Muttersprache zu beschreiben (BAMF, 2017a). Diese Beschreibungen werden aufgezeichnet und nach ungefähr zwei Minuten beendet. Aus dieser biometrischen Sprachprobe werden Wahrscheinlichkeiten für die gesprochenen Dialekte berechnet und im Ergebnisbericht festgehalten (BAMF, 2017a; BAMF, 2019a: 14). Die Sprachbiometrie wird eingesetzt, wenn Betroffene keinen gültigen Pass vorlegen können oder es Zweifel an ihrer Identität gibt (BAMF, 2018a: 3).

*AmD, Auslesen von mobilen Datenträgern*, soll die Identität und Herkunft von Asylbewerber:innen plausibilisieren. Das Bundesamt unterscheidet drei Stufen: das Auslesen mobiler Datenträger, die automatische Auswertung der Gerätedaten und die abschließende Verwendung der Ergebnisse in der Anhörung durch Entscheider:innen. Derzeit werden Smartphones, Featurephones und Tablets ausgelesen. In der Anwendung erfassen BAMF-Mitarbeitende generelle Informationen des Datenträgers wie das Kaufdatum und Land, in dem das Gerät erworben wurde. Dann müssen Asylbewerber:innen ihre Geräte entsperren. Das Auslesen erfolgt im Beisein der betroffenen Person an einem spezialisierten Computer, an den die Geräte angeschlossen werden. Extrahierte Daten werden automatisch analysiert. Im Gegensatz zu den anderen IDM-S-Systemen steht der Ergebnisbericht den Entscheidungsträger:innen nicht sofort zur Verfügung, sondern erst nach Freigabe durch einen Volljuristen. Das Auslesen der mobilen Datenträger kommt zum Einsatz, wenn Betroffene keinen gültigen Pass vorlegen können oder ihre Identität nicht zweifelsfrei geklärt werden kann (BAMF, 2018a: 3.1).

Die drei Systeme werden mit der Registrierung und Aktenanlage im Asylprozess eingesetzt, spätestens jedoch zur Anhörung. Dort sollen die Ergebnisse Hinweise zur Identität und Herkunft der asylsuchenden Menschen geben.

## Unrechtmäßige Eingriffe in die Privatsphäre

Von den drei IDM-S-Systemen wurde die Datenträger-Auswertung am heftigsten kritisiert, da sie massiv in die Privatsphäre von Schutzbedürftigen eingreift. Mit den Stimmen von CDU/CSU und der SPD wurde 2017 das *Gesetz zur besseren Durchsetzung der Ausreisepflicht* beschlossen, das die rechtliche Grundlage für die umstrittene Maßnahme im BAMF einführte (Deutscher Bundestag, 2020a: ID 18-80058). Der tiefe Eingriff in die Privatsphäre wurde nicht zuletzt von der damaligen Bundesdatenschutzbeauftragten, Andrea Voßhoff (2017), als nicht verfassungskonform ausgelegt.

Die Regierung hielt hartnäckig an der Methode fest. In der öffentlichen Anhörung war das BAMF, vertreten durch den ehemaligen IT-Chef und heutigen Bundes-CIO, Markus Richter, bemüht zu demonstrieren, dass die Maßnahme mit geltendem Recht vereinbar sei: Die Datenträger-Auswertung werde lediglich als „äußerstes Mittel“ (Richter, in Deutscher Bundestag, 2017: 20) eingesetzt, wenn alle anderen Wege der Identitätsprüfung ausgeschöpft seien, und nur in „Einzelfällen“ (Deutscher Bundestag, 2020b: 35). Man greife auf „ein ganz begrenztes Datenfeld“ zu (Richter, in Deutscher Bundestag, 2017: 39).

Die internen Dokumente des BAMF zeichnen jedoch ein anderes Bild. Demnach werden folgende Daten erfasst und analysiert: Metadaten der Bilder, Nachrichten, Telefonlisten (BAMF, 2018c); Geo-Informationen von Bildern, Apps, Login-Information zu Social Media, Informationen über gesprochene Sprachen in beispielsweise Browser-Historie, Mails und Chatnachrichten (Richter, in Deutscher Bundestag, 2017: 103). Statistiken zeigen, dass allein 2019 über 10 000 Geräte auslesen wurden, die Regierung ging sogar davon aus, dass 50–60 % aller Asylsuchenden keinen Pass besitzen und damit potenziell von der Maßnahme betroffen wären (Deutscher Bundestag, 2020b: 33; Bundesregierung, 2017: 15) – das sind keine *Einzelfälle*.

Gegen die Datenträger-Auswertung des BAMFs hat die Gesellschaft für Freiheitsrechte drei Klagen vor Verwaltungsgerichten eingereicht. In Berlin stellte das Gericht 2021 bereits fest, dass das BAMF das Handy einer geflüchteten Person zu Unrecht ausgelesen hatte. Das Urteil sendet ein wichtiges Signal für den Schutz der Rechte asylsuchender Menschen. Weitere Entscheidungen stehen noch aus (Zillekens, 2021).

Auch wenn die Datenträger-Auswertung aus Sicht der Privatsphäre die tiefgreifendste Maßnahme darstellt, zeigen auch die anderen beiden Systeme Mängel bei der Vereinbarkeit mit datenschutzrechtlichen Anforderungen. So werden asylsuchende Menschen nicht sinnvoll über die Erhebung und Datenverarbeitung ihrer personenbezogenen Daten informiert. Bei der Sprachbiometrie müssen Betroffene zwar formal ihre Unterschrift auf ein Formular setzen, jedoch findet keine adäquate Unterrichtung statt (BAMF, 2020c). Im Falle der Namens-Transliteration wird Betroffenen keinerlei schriftliche Information zur Analyse ihrer Namen in Bezug auf eine Herkunftsregion gegeben (BAMF, 2020b). Es ist daher fraglich, inwieweit sie über die Verwendung ihrer Daten über die Transliterations-Funktion hinaus aufgeklärt werden.

## Fehlende Transparenz und unabhängige Evaluation

Die Entwicklung und Umsetzung von IDM-S im BAMF wurde in der Kommunikation nach außen stark restriktiv gehandhabt und kontrolliert. Es wurde weitestgehend vermieden, proaktiv, kontinuierlich und dialogorientiert Information über die Namensanalyse, Sprachbiometrie und Datenträger-Auswertung bereitzustellen. Presse- und Informationsfreiheitsanfragen an das BAMF wurden verzögert, lückenhaft und verkürzt beantwortet. Detaillierte Angaben zu den Funktionalitäten, Kosten-Nutzen-Abwägungen, Testergebnissen sowie Kooperationspartnern nach Informationsfreiheitsgesetz (IFG) wurden abgelehnt (BAMF, 2020a; BAMF, 2019b; BAMF, 2019c; BAMF, 2019d). Es ist nach wie vor unklar, wie das zugrunde liegende Datenmodell der drei Systeme genau aussieht, wie die Daten mit diesen Grundmodellen abgeglichen und die Analyse-Ergebnisse gewichtet werden. Eine unabhängige Evaluation der Systeme fand nicht statt (BAMF, 2020a: 4; Deutscher Bundestag, 2018a: 14).

Für die Dokumentation der IDM-S-Systeme erfasst das BAMF kaum aussagekräftige Statistiken. So wird nur erhoben, wie oft die Systeme eingesetzt wurden und ob die Ergebnisse mit den Angaben der Asylsuchenden übereinstimmen (BAMF, 2018a: 3.2 – 3.4; BAMF, 2017a). In der Praxis kommt es jedoch häu-



fig vor, dass die IDM-S-Systeme vielfach eingesetzt werden, es aber keine stringente Einschätzung dazu gibt, inwieweit die Ergebnisse die Aussagen der Asylsuchenden stützen oder nicht (Deutscher Bundestag, 2018b: 31; Deutscher Bundestag, 2018a: 12; Deutscher Bundestag, 2019a: 28-29). Lückenhafte Statistiken erschweren es damit, die Effektivität dieser Systeme zu bewerten.

Gravierend ist auch, dass (un)beabsichtigte Auswirkungen auf asylsuchende Menschen, die die Identitätsfeststellung mittels IDM-S durchlaufen, gar nicht erhoben werden. Insbesondere wird nicht bewertet, ob die Ergebnisse der Systeme Asylentscheidungen negativ beeinflussen (Deutscher Bundestag, 2018a: 13; Deutscher Bundestag, 2018c: 7; Deutscher Bundestag, 2019b: 14; Deutscher Bundestag, 2020b: 35). Diese Perspektive wird ignoriert, obwohl bekannte Fälle bestätigen, dass die Ergebnisse von IDM-S zu Fehleinschätzungen und zu ungerechten Asylentscheidungen führen können (Biselli und Beckmann, 2020; Biselli, 2018). Es scheint, dass das Bundesamt Fälle, die nicht in die allgemeine Erfolgsgeschichte dieser *innovativen Technologien* passen, reale Folgen für Betroffene ausblendet und nicht ernst genug nimmt.

### Trügerische Versprechen der Effizienz

Das BAMF verweist in Argumentationen auf die Nützlichkeit und die Vorteile von IDM-S vor allem für die internen Abläufe: Der Einsatz der Systeme führe dazu, dass Asylverfahren effizienter und schneller abgewickelt werden und Kosten reduziert würden (BAMF und BFM, 2017). Die Realität zeigt jedoch, dass die IDM-S-Komponenten zu großen Teilen ineffizient sind und oft zu keinen brauchbaren Ergebnissen führen.

Das Erfolgs-Narrativ über TraLitA bezieht sich vor allem auf die Transliterations-Funktion, über die Namensanalyse spricht das BAMF selten. Die Ergebnisse der Namensanalysen sind aber nach Statistiken aus 2018 wenig aussagekräftig: Von den erfassten 1.443 Einsätzen von TraLitA war die Mehrheit der Hinweise (39 %) nicht verifizierbar (Deutscher Bundestag, 2018a: 24). Grundsätzlich ist es höchst fraglich, wie Namen, die beispielsweise kulturell, religiös beeinflusst oder nach Vorlieben vergeben werden, eindeutig Herkunftsländern zugeordnet werden können.

Von den drei untersuchten IDM-S-Systemen weist die Sprachbiometrie die höhere, wenn auch lediglich durchschnittliche Erfolgsquote von 85 % für alle enthaltenen Sprachmodelle auf (Deutscher Bundestag, 2018a: 13). Für Arabisch-Levantinisch

erreicht die Quote laut eigenen Angaben der Behörde 90 %, allerdings wird die Verteilung der Fehlerquote der anderen Dialekte nicht bekannt gegeben. Diese Informationen unterliegen der Geheimhaltung, um Täuschungsversuche in Asylverfahren zu unterbinden (Deutscher Bundestag, 2018a: 15).

Die Datenträger-Auswertung ist bei weitem das teuerste und ineffizienteste System im Portfolio: Ging die Bundesregierung beim Gesetzesbeschluss für diese Maßnahme noch von Kosten über 3.200.000 Euro aus, so wurden 2018 bereits 11 Millionen an Steuergeldern ausgegeben (Deutscher Bundestag, 2018a: 14-25; Deutscher Bundestag, 2018b: 32). Statistiken aus 2019 zeigen, dass von den 10.116 ausgelesenen Datenträgern lediglich 3.436 der Ergebnisse von Entscheider:innen genutzt wurden. Von diesen genutzten Fällen war die Mehrheit unbrauchbar (Deutscher Bundestag, 2020b: 35). Aus dieser tatsächlichen Ineffizienz werden keine Konsequenzen gezogen: „Das Auslesen mobiler Datenträger stellt momentan das wichtigste Instrument zur Identitätsüberprüfung dar“ (BAMF, 2020d: 2).

### Fazit

Mit dem Einsatz von neuartigen algorithmischen Systemen im Behördenkontext wird oft ein modernes Regierungshandeln verbunden. Allerdings zeigt gerade das Beispiel des Bundesamts für Migration und Flüchtlinge, wie konträr der Einsatz solcher Systeme zu demokratischen Prinzipien, behördlicher Verantwortung und individuellen Rechten von Betroffenen sein kann. Umso dringender und wichtiger ist es, Legitimität und *raison d'être* solcher technischen Systeme im politischen Kontext zu prüfen. Für eine Detailanalyse der drei vorgestellten IDM-S-Systeme und die Versuche des BAMF, diese zu legitimieren, sei interessierten Leser:innen die veröffentlichte Masterarbeit empfohlen (Hahn, 2021).

### Referenzen

- BAMF. 2016. Das Bundesamt in Zahlen: Asyl, Migration und Integration. Available at: [https://www.bamf.de/SharedDocs/Anlagen/DE/Statistik/BundesamtinZahlen/bundesamt-in-zahlen-2015.pdf?\\_\\_blob=publicationFile&v=16](https://www.bamf.de/SharedDocs/Anlagen/DE/Statistik/BundesamtinZahlen/bundesamt-in-zahlen-2015.pdf?__blob=publicationFile&v=16). Effective 15.01.2022.
- BAMF. 2017a. Integriertes Identitätsmanagement – Plausibilisieren, Datenqualität und Sicherheitsaspekte. Einführung in die neuen IT-Tools. Schulung AVS-Mitarbeiter, Entscheider und Volljuristen. Freedom of information request at fragdenstaat.de. Available at: [https://fragdenstaat.de/anfrage/foi-satzes-und-interpretationshilfen-zu-sprachanalyse/110994/anhang/schulung\\_idms\\_bamf.pdf](https://fragdenstaat.de/anfrage/foi-satzes-und-interpretationshilfen-zu-sprachanalyse/110994/anhang/schulung_idms_bamf.pdf). Effective 15.01.2022.



**Helene Hahn**

**Helene Hahn** arbeitet und forscht zu Governance-Prozessen im Kontext der Digitalität und der Wissensgesellschaft. Sie engagiert sich für Menschenrechte, transparentes Regierungshandeln und Beteiligungsmöglichkeiten, die neue Technologien eröffnen. Helene hat einen Abschluss in „Governance and Human Rights“ (M.A.) sowie in Kultur- und Sozialwissenschaften (B.A.).



- BAMF. 2017b. Moderne Technik in Asylverfahren: Vorsitzender der Innenministerkonferenz informiert sich über neue technische Assistenzsysteme. Available at: <https://www.bamf.de/SharedDocs/Meldungen/DE/2017/20170726-am-vorstellung-modellprojekt-bamberg.html?nn=282388>. Effective 15.01.2022.
- BAMF. 2018a. Dienstanweisung Asylverfahren: Identitätsfeststellung. Freedom of information request via fragdenstaat.de. Available at: [https://fragdenstaat.de/anfrage/dienstanweisungen-zum-umgang-mit-der-handyauswertung/110992/anhang/dienstanweisung\\_identitaetsfeststellung.pdf](https://fragdenstaat.de/anfrage/dienstanweisungen-zum-umgang-mit-der-handyauswertung/110992/anhang/dienstanweisung_identitaetsfeststellung.pdf). Effective 15.01.2022.
- BAMF. 2018b. Dienstanweisung Asylverfahren: Identitätsfeststellung. Available at: [https://fragdenstaat.de/anfrage/dienstanweisungen-zum-umgang-mit-der-handyauswertung/110992/anhang/dienstanweisung\\_identitaetsfeststellung.pdf](https://fragdenstaat.de/anfrage/dienstanweisungen-zum-umgang-mit-der-handyauswertung/110992/anhang/dienstanweisung_identitaetsfeststellung.pdf). Effective 15.01.2022.
- BAMF. 2018c. Verfahrensverzeichnis: Auslesen mobiler Datenträger. Freedom of information request at fragdenstaat.de. Available at: <https://fragdenstaat.de/anfrage/verfahrensverzeichnis/92175/anhang/Auslesen-mobilerDatentrger.pdf>. Effective 15.01.2022.
- BAMF. 2019a. Digitalisierungsagenda 2020: Bisherige Erfolge und Ausblick auf weitere digitale Projekte im Bundesamt für Migration und Flüchtlinge. Available at: <https://www.bamf.de/SharedDocs/Anlagen/DE/Digitalisierung/broschuere-digitalisierungsagenda-2020.html>. Effective 15.01.2022.
- BAMF. 2019b. Bilder für sprachbiometrische Tests. Available at: <https://fragdenstaat.de/anfrage/bilder-fur-sprachbiometrische-tests-1/>. Effective 15.01.2022.
- BAMF. 2019c. Testergebnisse biometrischer Sprachsoftware zur Erkennung von Dialekten. Available at: [https://fragdenstaat.de/anfrage/testergebnisse-biometrischer-sprachsoftware-zur-erkennung-von-dialekten/353954/anhang/2019\\_697\\_IFG\\_NAME\\_geschwaerzt.pdf](https://fragdenstaat.de/anfrage/testergebnisse-biometrischer-sprachsoftware-zur-erkennung-von-dialekten/353954/anhang/2019_697_IFG_NAME_geschwaerzt.pdf). Effective 15.01.2022.
- BAMF. 2019d. Datenschutz-Folgenabschätzung: Anfrage nach dem Informationsfreiheitsgesetz (IFG). Available at: [https://fragdenstaat.de/anfrage/datenschutz-folgeabschätzungen/353952/anhang/2019\\_689\\_IFG\\_Biselli\\_geschwaerzt.pdf](https://fragdenstaat.de/anfrage/datenschutz-folgeabschätzungen/353952/anhang/2019_689_IFG_Biselli_geschwaerzt.pdf). Effective 15.01.2022.
- BAMF. 2020a. Digitalisierungsagenda 2020 & IDM-S POC, Kosten-Nutzen, Evaluation, Feedback. Available at: [https://fragdenstaat.de/anfrage/digitalisierungsagenda-2020-idm-s-poc-kosten-nutzen-evaluation-feedback/482915/anhang/SPRN90620050609180\\_geschwaerzt.pdf](https://fragdenstaat.de/anfrage/digitalisierungsagenda-2020-idm-s-poc-kosten-nutzen-evaluation-feedback/482915/anhang/SPRN90620050609180_geschwaerzt.pdf). Effective 15.01.2022.
- BAMF. 2020b. Belehrung von Antragstellenden: Sprachbiometrie (DIAS), Namenstranskription (TraLiTA). Available at: <https://fragdenstaat.de/anfrage/belehrung-von-antragstellenden-sprachbiometrie-dias-namenstranskription-tralita/>. Effective 15.01.2022.
- BAMF. 2020c. Information zur Abgabe einer Sprechprobe für die Sprachbiometrie. D1728. Available at: <https://fragdenstaat.de/anfrage/belehrung-von-antragstellenden-sprachbiometrie-dias-namenstranskription-tralita/503448/anhang/D1728.pdf>. Effective 15.01.2022.
- BAMF. 2020d. Ihr Antrag nach dem Informationsfreiheitsgesetz (IFG). Auslesen mobiler Datenträger: FAQ-Liste und Antworten. Available at: <https://fragdenstaat.de/anfrage/auslesen-mobiler-datentrager-faq-liste-und-antworten/510153/anhang/SPRN91220072208050.pdf>. Effective 15.01.2022.
- BAMF; BFM. 2017. Integriertes Identitätsmanagement – Assistenzsysteme. Available at: <https://docplayer.org/108534301-Preseinformation-integriertes-identitaetsmanagement-assistenzsysteme-1-integriertes-identitaetsmanagement-im-ueberblick.html>. Effective 15.01.2022.
- Biselli, Anna. 2018. Eine Software des BAMF bringt Menschen in Gefahr. Available at: <https://www.vice.com/de/article/a3q8wj/fluechtlinge-bamf-sprachanalyse-software-entscheidet-asyl>. Effective 15.01.2022.
- Biselli, Anna; Beckmann, Lea. 2020. Invading refugees' phones: Digital forms of migration control in Germany and Europe. Gesellschaft für Freiheitsrechte e. V.. Available at: [https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study\\_Invading-Refugees-Phones\\_Digital-Forms-of-Migration-Control.pdf](https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf). Effective 15.01.2022.
- Bock, Jürgen. 2015. Chaos und Überforderung bei der Annahme von Asylanträgen. Available at: <https://www.stuttgarter-nachrichten.de/inhalt.fluechtlinge-in-baden-wuerttemberg-chaos-und-ueberforderung-bei-der-annahme-von-asylantraegen.dc5f2d08-8f31-4db0-9f94-fb32ff311505.html>. Effective 15.01.2022.
- Brekke, Jan-Paul; Staver, Anne Balke. 2019. Social media screening: Norway's asylum system. Forced Migration Review. The ethics issue. June 2019, 61. Available at: <https://www.fmreview.org/ethics/brekke-balkes-taver>. Effective 15.01.2022.
- Bundesregierung. 2017. Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. BT-Drucksache 18/11546. Available at: <https://dipbt.bundestag.de/dip21/btd/18/115/1811546.pdf>. Effective 15.01.2022.
- Deutscher Bundestag. 2017. Wortprotokoll der 111. Sitzung. Innenausschuss. Öffentliche Anhörung. Protokoll-Nr. 18/111. Available at: <https://www.bundestag.de/resource/blob/511642/d4c03aa26137310cf5568fa-7e9f179fc/Protokoll-111-Sitzung-data.pdf>. Effective 15.01.2022.
- Deutscher Bundestag. 2018a. Antwort der Bundesregierung auf die kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge. BT-Drucksache 19/6647. Available at: <https://dip21.bundestag.de/dip21/btd/19/066/1906647.pdf>. Effective 15.01.2022.
- Deutscher Bundestag. 2018b. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Ergänzende Informationen zur Asylstatistik für das zweite Quartal des Jahres 2018. BT-Drucksache 19/4961. Available at: <https://dipbt.bundestag.de/dip21/btd/19/049/1904961.pdf>. Effective 15.01.2022.
- Deutscher Bundestag. 2018c. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Einsatz von Spracherkennungssoftware durch das Bundesamt für Migration und Flüchtlinge. BT-Drucksache 19/1663. Available at: <https://dipbt.bundestag.de/dip21/btd/19/016/1901663.pdf>. Effective 15.01.2022.
- Deutscher Bundestag. 2019a. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Ergänzende Informationen zur Asylstatistik für das Jahr 2018. BT-Drucksache 19/8701. Available at: <https://dip21.bundestag.de/dip21/btd/19/087/1908701.pdf>. Effective 15.01.2022.
- Deutscher Bundestag. 2019b. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. BT-Drucksache 19/13945. Available at: <https://dip21.bundestag.de/dip21/btd/19/139/1913945.pdf>. Effective 15.01.2022.
- Deutscher Bundestag. 2020a. Gesetz zur besseren Durchsetzung der Ausreisepflicht. Dokumentations- und Informationssystem DIP. ID: 18-80058. Available at: <https://dipbt.bundestag.de/extrakt/ba/WP18/800/80058.html>. Effective 15.01.2022.
- Deutscher Bundestag. 2020b. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. Ergänzende Informationen zur Asylstatistik für das Jahr 2019. BT-Drucksache 19/18498. Available at: <https://dip21.bundestag.de/dip21/btd/19/184/1918498>.



- pdf. Effective Effective 15.01.2022.
- ECtHR. 2011. Case of M.S.S. v. Belgium and Greece. Application No. 30696/09. Judgment of January 21, 2011. Available at: [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-103050%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-103050%22]}). Effective 15.01.2022.
- Grote, Janne. 2018. Die veränderte Fluchtmigration in den Jahren 2014 bis 2016: Reaktionen und Maßnahmen in Deutschland. Fokusstudie der deutschen nationalen Kontaktstelle für das Europäische Migrationsnetzwerk (EMN). BAMF. 2018. Available at: [https://www.bamf.de/SharedDocs/Anlagen/DE/EMN/Studien/wp79-emn-fluchtmigration-2014-2016-reaktionen-ma%C3%9Fnahmen-deutschland.pdf;jsessionid=B559424AB94D5E4217F292ACAD091BA1.internet532?\\_\\_blob=publicationFile&v=19](https://www.bamf.de/SharedDocs/Anlagen/DE/EMN/Studien/wp79-emn-fluchtmigration-2014-2016-reaktionen-ma%C3%9Fnahmen-deutschland.pdf;jsessionid=B559424AB94D5E4217F292ACAD091BA1.internet532?__blob=publicationFile&v=19). Effective 15.01.2022.
- Hahn, Helene. 2021. Digital identification systems and the right to privacy in the asylum context. An analysis of implementations in Germany. Available at: <https://nbn-resolving.org/urn:nbn:de:gbv:lue4-opus4-11249>. Effective 15.01.2022.
- Jehle, Stefan. 2016. Lange Schlangen in Karlsruhe. Flüchtlinge müssen dreimal anstehen. Stuttgarter Zeitung. Available at: <https://www.stuttgarter-zeitung.de/inhalt.lange-schlangen-in-karlsruhe-fluechtlinge-muessen-dreimal-anstehen.efbc003a-243d-44d5-92ac-78e2b6baa5f8.html>. Effective 15.01.2022.
- Kaurin, Dragana. 2019. Data protection and digital agency for refugees. Centre for International Governance Innovation. World Refugee Council Research Paper No. 12. Available at: <https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees>. Effective 15.01.2022.
- Latonero, Mark; Hiatt, Keith; Napolitano, Antonella; Clericetti, Giulia; Penagos, Melanie. 2019. Digital identity in the migration and refugee context: Italy case study. Data & Society. CILD. Available at: [https://datasociety.net/wp-content/uploads/2019/04/DataSociety\\_DigitalIdentity.pdf](https://datasociety.net/wp-content/uploads/2019/04/DataSociety_DigitalIdentity.pdf). Effective 15.01.2022.
- Molnar, Petra. 2018a. Using AI in immigration decisions could jeopardise human rights. Centre for International Governance Innovation. Available at: <https://www.cigionline.org/articles/using-ai-immigration-decisions-could-jeopardize-human-rights>. Effective 15.01.2022.
- Molnar, Petra. 2018b. The contested technologies that manage migration. Centre for International Governance Innovation. Available at: <https://www.cigionline.org/articles/contested-technologies-manage-migration>. Effective 15.01.2022.
- Sánchez-Monedero, Javier; Dencik, Lina. 2020. The politics of deceptive borders: ‚biomarkers of deceit‘ and the case of iBorderCtrl. Available at: <https://doi.org/10.1080/1369118X.2020.1792530>. Effective 15.01.2022.
- Scheinost, Rudolf; Hüter, Gernot. 2015. Offener Brief an den Leiter des BAMF. Gesamt Personalrat; Örtliche Personalrat. BAMF. Available at: [https://www.tagesschau.de/inland/brandbrief-bamf-105-\\_origin-f6ce9f91-72e7-44f4-8685-ac9f20bfd5e.pdf](https://www.tagesschau.de/inland/brandbrief-bamf-105-_origin-f6ce9f91-72e7-44f4-8685-ac9f20bfd5e.pdf). Effective 15.01.2022.
- Voßhoff, Andrea. 2017. Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht. Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. German Bundestag. Innenausschuss. Ausschussdrucksache 18(4)831. Available at: <https://www.bundestag.de/resource/blob/500024/bf72784c6e0f00bc5d801ccd5aee690b/18-4-831-data.pdf>. Effective 15.01.2022.
- Zillekens, Janina. 2021. Erfolgreiche Klage für Privatsphäre Geflüchteter: VG Berlin erklärt BAMF-Handydatenauswertungen für rechtswidrig. Available at: <https://freiheitsrechte.org/pm-erfolg-gegen-bamf-handyauswertung/>. Effective 15.01.2022.



## Weizenbaum-Studienpreis – Laudatio für den dritten Preis

# Silke Meiser: Trust me! Vorschlag zum Umgang mit der Vertrauensfrage im digitalen Zeitalter

## Masterarbeit an der Universität Oldenburg

Vertrauen ist eine wesentliche Voraussetzung unseres alltäglichen Zusammenlebens. Niklas Luhmann, auf den sich auch die Arbeit bezieht, schrieb bereits 1968 einleitend zu seinem gleichnamigen Buch:

*„Vertrauen im weitesten Sinne eines Zutrauens zu eigenen Erwartungen ist ein elementarer Tatbestand des sozialen Lebens. Der Mensch hat zwar in vielen Situationen die Wahl, ob er in bestimmten Hinsichten Vertrauen schenken will oder nicht. Ohne jegliches Vertrauen aber könnte er morgens sein Bett nicht verlassen. Unbestimmte Angst, lähmendes Entsetzen befahlen ihn. Nicht einmal ein bestimmtes Misstrauen könnte er formulieren und zur Grundlage defensiver Vorkehrungen machen; denn das würde voraussetzen, dass er in anderen Hinsichten vertraut. Alles wäre möglich. Solch eine unvermittelte Konfrontierung mit der äußeren Komplexität der Welt hält kein Mensch aus.“*

Vertrauen macht unser Zusammenleben möglich, indem es die Komplexität unserer sozialen Umgebung reduziert. Dies gilt um

so mehr für die undurchschaubare Welt des Digitalen, die für uns noch weniger greifbar ist als die gegenständliche Alltagswelt. Die Frage des Vertrauens ist damit ein hochrelevantes Thema für die Digitalisierung und die damit verbundenen Entwicklungen.

Mit Vertrauen im digitalen Zeitalter setzt sich Silke Meiser in ihrer Arbeit *Trust me! Vorschlag zum Umgang mit der Vertrauensfrage im digitalen Zeitalter* auseinander. Sie fragt, inwieweit Vertrauen dazu beiträgt, Komplexität zu bewältigen und darüber hinaus, wie in Zeiten großer, technologisch beförderter Veränderung – die auch die Neuverteilung von Macht bewirken kann – eigene Handlungspläne unter realistischen Bedingungen verwirklicht werden können. In welchem Sinne erfolgt der Einsatz digitaler Technik: Welche Logik und Ansprüche entfalten sich darin?, und was bedeutet dies für das Handlungsvermögen des analogen Menschen in der zunehmend digital determinierten Gesellschaft, also auch für Menschen, die entsprechende Geräte bedienen, aber nicht verstehen? Wir verleihen ihr dafür einen dritten Preis.



Die Arbeit besteht aus zwei Teilen: Im ersten Teil behandelt sie das digitale System. Dies umfasst das zugrunde liegende Paradigma, die sich ergebenden Veränderungs- und Machtdynamiken, die treibenden Visionen und die dahinterstehende Ideologie. Sie geht dabei von Luhmanns Vertrauensbegriff und den Eckpunkten Autopoiesis, Kontingenz, Komplexität aus.

Bei der Nutzung des Internets sind wir an vielen Stellen auf Vertrauen angewiesen. Wir vertrauen, so wird in der Arbeit festgestellt, ...

- ... den Ergebnissen von Suchmaschinen, die komplexe Recherchen für uns übernehmen,
- ... den Bewertungen anderer Benutzer, die Empfehlungen für Produkte und Dienstleistungen abgeben,
- ... der Expertise, die im Internet steht und die wir – teilweise ungefiltert – von dort beziehen.

Dies schließt auch in zunehmendem Maß komplexe wissensbasierte Dienstleistungen ein, die früher einer Automatisierung nicht zugänglich waren und bei denen wir den Weg der Lösungsfindung nicht mehr oder nur noch schwer nachvollziehen können: beispielsweise bei der Personalauswahl, im Consulting, in der Rechtsberatung und -auslegung. Wir wissen, dass Systeme, die auf *Machine Learning* basieren, auch unerwünschte Effekte verursachen können, beispielsweise zu programmiertem Rassismus bei der Umsetzung von *Predictive Policing*. Die müssen wir berücksichtigen, bevor wir solchen Systemen „blind“ vertrauen.

Daten werden nach wie vor als „Öl des 21. Jahrhunderts“ bezeichnet. Diese Metapher ist vielschichtig. Meist bezeichnet sie den Wert, den diese Daten darstellen – man könnte aber auch die „Verschmutzungen“ damit paraphrasieren, wenn sie an der falschen Stelle und im falschen Kontext zum Einsatz kommen. Gehen wir vom „Wert“ aus, der Daten zugemessen wird, müssen wir feststellen: Dieser Wert wird nicht von den Besitzerinnen und Besitzern der Daten kapitalisiert, sondern zumeist von den Betreibenden der großen Plattformen. Das größte Gestaltungspotenzial haben dabei diejenigen, die sich nicht an die Spielregeln halten, denen es in besonderem Maße gelingt, ihre (technologische) Macht auszuüben.

Für die Nutzerinnen und Nutzer bleibt Selbstkolonisation, von ihnen wird begeistertes Mitmachen erwartet, eine Form der Unterwerfung unter eine neue Ordnung. Ihr Motiv, so die Autorin, ist die Sehnsucht nach einer starken Gemeinschaft, die die Akteure im Internet so gern simulieren. Das Netz erscheint dabei als ein Ort, an dem alles möglich ist. Konsequenzen aus der maschinell-algorithmischen Logik werden allzuoft ausgeblendet – auch, weil sie so gut unsichtbar gemacht werden.

Der zweite Teil kommt zum Kern der Arbeit: Vertrauen im digitalen System. Für deren Untersuchung wird ein Schema adaptiert, das von *Kelton* vorgeschlagen wurde. Die zentrale Frage, die in der Arbeit untersucht wird, ist damit: Wie kann, wenn Macht

und Vertrauen neu zu verhandeln sind, Vertrauen dazu beitragen, das Handlungsvermögen der Menschen in der vercloudeten Welt zu fördern? Sie untersucht die Relation von Macht und Vertrauen und differenziert zwischen (informiertem) Vertrauen und (naiver) Hoffnung. Orientiert an Kelton strukturiert sie die Argumentation in vier Abschnitte:

- Vorbedingungen für Vertrauen: Ungewissheit, Verletzbarkeit, Abhängigkeit;
- Stufen des Vertrauensaufbaus: Gefühlsbindung, Vertrautheit, Eigenkontrolle, Fremdkontrolle, Sinn;
- Rahmenbedingungen für Vertrauen: Selbstvertrauen, Vertrauen der Anderen, Kontext;
- Vertrauenswürdigkeit: Berechenbarkeit, Wohlwollen/Rücksichtnahme, Kompetenz, Ethik.

Dabei wird die Verbindung zu aktuellen politischen Debatten hergestellt. Im Abschnitt zur Ethik setzt sich die Arbeit beispielsweise ausführlich mit den im Auftrag der Europäischen Kommission erarbeiteten Ethik-Leitlinien für eine vertrauenswürdige KI auseinander.

Die zentrale Argumentation ist: Vertrauenswürdigkeit in digitalen Systemen muss stets kritisch überprüft werden. Dies erfordert rationales Vertrauen, das auch die Widersprüche und Unstimmigkeiten beachtet. „Wer sich hier auf eine Verheißung von Ethik, den nicht einzufordernden guten Willen des anderen verlässt, handelt fahrlässig. Um Macht wird gerungen, und wo dies nicht geschieht, ist die Machtfrage schon entschieden“, so die Autorin.

Die häufige Kommunikation vermeintlich positiver Wirkungen technischer Lösung auf die Gesellschaft zerlegt Silke Meiser anhand der Struktur des typischen Essay über *The impact of computers on society*, wie ihn Joseph Weizenbaum einmal beschrieben hat.

Die Arbeit behandelt ein gesellschaftlich sehr relevantes Thema: Das Verhältnis zwischen Plattformen und anderen Digital-Dienstleistern sowie deren Nutzer:innen aus soziologischer Sicht. Dies ist zugleich ein Vertrauens- und Machtverhältnis. Das Thema wird sehr umfassend, fundiert, fantasievoll und in beeindruckender Länge behandelt. Die Arbeit argumentiert stringent, wobei sich die Jury ein wenig an dem schwammigen Begriff der „Cloud“ gestört hat. Durch das Modell nach Kelton ist die Arbeit übergreifend und nachvollziehbar strukturiert. Angesichts des eher trockenen Stoffs ist sie flüssig und interessant zu lesen. Sie stützt sich auf sehr umfangreiches Quellenmaterial und enthält ausführliche Anmerkungen. Der Einschätzung, sie sprengte das Maß einer Masterarbeit, ist wohl zuzustimmen. Die Jury hat sich daher für die Auszeichnung der Arbeit entschieden.

**Herzlichen Glückwunsch, Silke Meiser, zum Weizenbaum-Studienpreis 2021.**





## Zur (Mit-)Gestaltung der digitalen Gesellschaft durch rationales Vertrauen

DATEN SIND MACHT

Auf dem Weg ins Totale System

„Ethische KI“ ist eine FALLE

Wie wollen wir leben?

Wie können technisch durchschnittlich begabte Menschen in einer zunehmend digitalen Gesellschaft bestehen? Ein Weg führt über rationales Vertrauen. Der Soziologe Niklas Luhmann schrieb schon 1968, man werde „damit rechnen müssen, daß Vertrauen mehr und mehr in Anspruch genommen werden muß, damit technisch erzeugte Komplexität der Zukunft ertragen werden kann.“<sup>1</sup>

Vertrauen kann man mit Luhmann als einen Mechanismus verstehen, der Komplexität reduziert. Mehr noch: Der bewusste und vernünftige Umgang mit Vertrauen macht es möglich, die Entwicklung von Gesellschaft und Technologie im eigenen Sinne mitzugestalten. Und obwohl Komplexität zunehmend digital erzeugt und aufgelöst wird, bleibt rationales Vertrauen eine zutiefst menschliche Praxis. Es gibt keinen Vertrauensalgorithmus. Vertrauen schließt Urteilsvermögen, Mut, die Hinwendung an eine gemeinsame, größere Sache und eine annähernd heroische Selbstaufgabe mit ein. Es ist damit weit mehr als ein achtloses oder hingebungsvolles JA – und auch das NEIN, die Möglichkeit, sich gegebenenfalls für Misstrauen zu entscheiden, gehört untrennbar zum Vertrauen dazu.

Am Ende dieses Artikels werden einige Elemente, die beim Vertrauen eine Rolle spielen, kurz vorgestellt. Im Folgenden geht es jedoch vor allem um Möglichkeiten der praktischen Anwendung. Dazu folgen vier Gedankenbilder, die einen Blick auf den Mechanismus Vertrauen im digitalen Alltag durch die Brille der Systemtheorie ermöglichen. Die Herangehensweise ist wissenschaftsbasiert, stark verkürzt und nicht objektiv: Im Fokus steht die Aufforderung, angesichts informationsverarbeitender Übermacht dennoch selbstbestimmt zu leben und Zukunft aktiv zu gestalten.

### Erstens: Daten sind Macht.

Wir leben, systemtheoretisch und metaphorisch, in einem digitalen System. In einem System wirken verschiedene Elemente aufeinander ein. Sie tun alles, um sich zu erhalten, während sie sich selbst und das System laufend verändern. Das Gesellschaftssystem, betrachtet als die Gesamtheit der Kommunikationen, funktioniert heute zunehmend nach digitalen Regeln. Das führt zu einigen neuen Eigenschaften. Unverändert gilt dabei Lernfähigkeit als evolutionärer Vorteil. Im Vorteil ist heute, wer Daten verarbeiten kann, wer also daraus Information ableiten und diese dann in Entscheidungen umsetzen kann – und das möglichst schneller als andere.

Um das zu tun, braucht man aber erst einmal Daten. Das wird im öffentlichen Hype um neue Technologien gern unter den Teppich gekehrt: Es besteht eine gegenseitige Abhängigkeit zwischen der Fähigkeit zur Informationsverarbeitung und der Herrschaft über Daten. Wer Daten bereitstellt oder zurückhält, übt gesellschaftliche Macht aus.

Unser Zugang zur digitalen Gesellschaft erfolgt vermittelt unserer Daten. Dadurch, dass wir persönliche Daten freigeben oder zurückhalten, drücken wir Vertrauen oder Misstrauen aus und gestalten gesellschaftliche Veränderung. Das vertrauende JA eskaliert gewünschte Veränderung. Das misstrauende NEIN entzieht unerwünschten Entwicklungen die Energie; es stößt Lernprozesse an und stabilisiert auch das System.

Kontrolle über persönliche Daten ist zugleich Kontrolle über die eigenen Grenzen. Ein JA lässt strukturelle Kopplungen zu. Das NEIN stellt sich gegen digitale Übergriffe und Antastbarkeit.

Daten freizugeben oder zurückzuhalten ist Voraussetzung für Selbstvertrauen und Ausdruck von Vertrauen in das eigene Urteilsvermögen. Es ist fundamental ein Machtanspruch: der Anspruch auf legitime Selbsterhaltung und gestaltende Teilhabe.

Selbstbestimmte Teilhabe an der Gesellschaft setzt ein grundlegendes Verständnis der Mechanismen von Macht und Einflussnahme voraus. Wir brauchen eine digitale Bildung, die uns unsere Möglichkeiten und Verantwortung aufzeigt und uns in die Lage versetzt, die Systeme der digitalen Gesellschaft nicht nur zu bedienen, sondern zu beherrschen. Und wir brauchen Datenschutz, damit unser JA und vor allem unser NEIN auch wirksam sind. All dies beginnt mit der Erkenntnis: Daten sind Macht.

### Zweitens: Wir befinden uns auf dem Weg in ein totales digitales System.

Das totale System, ein weiterer Begriff aus der Systemtheorie, beschreibt eine Situation, in der Elemente eines Systems in allen möglichen Dimensionen an das System gekoppelt sind. Je ge-



ringer die Freiheitsgrade der einzelner Elemente, desto größere Asymmetrien entstehen. Eine solche Entwicklung zeichnet sich im digitalen System Gesellschaft ab. Dies ergibt sich aus mehreren Faktoren, die hier zusammenkommen: Einseitige Transparenz, Informationsverarbeitungsmonopole und umfassende Vernetzung bei zunehmender Durchdringung des Alltags mit Technik. Soziale Sphären werden zusammengeführt und Kontextgrenzen werden geschleift.

Zum totalen System gibt es eine schöne Beschreibung bei Fritz Simon: „*Es gibt kein Entrinnen, keinen Raum, wo gegenüber der Organisation oder ihren Vertretern Abgrenzung legitim wäre und man ihnen sagen könnte: ‚Das geht Sie nichts an! Das ist meine Privatsache!‘* (Das gilt allerdings nur für die Insassen solcher Institutionen, nicht ihre Mitarbeiter.)“<sup>2</sup>

Die Institutionen und ihre Mitarbeiter:innen, die unsere Daten wollen, fordern zwar Vertrauen ein, und es wird viel getan, damit sich das auch so anfühlt, aber am Ende ist das, was mit unseren Daten geschaffen wird, keine vertrauensvolle Praxis. Sie können und sie wollen uns nicht vertrauen, Weizenbaums „*technological messiahs who, because they find it impossible to trust the human mind, feel compelled to build ‚trustworthy‘ computers ...*“<sup>3</sup>. Sie binden uns mit List oder Gewalt oder mithilfe unserer Bequemlichkeit und Tendenz, viel zu oft JA zu sagen, an ein uns in immer mehr Lebensbereichen erfassendes System instrumenteller Ereignisbeherrschung – an ein beschränkt wirksames funktionales Äquivalent zum Vertrauen, das mithilfe von Daten und Metadaten, Mustern und Wahrscheinlichkeiten Menschen als gutes oder schlechtes Risiko sortiert und ihnen daraufhin bestimmte Freiheitsgrade einräumt oder sie einschränkt – zwangsläufig eher einschränkt, im Sinne der Aufrechterhaltung von Ordnung und Asymmetrie.

Im totalen digitalen System entscheiden in wichtigen Dingen Maschinen über Menschen. Diese Maschinen kennen nur die Zustände „1“ und „0“. Vertrauenswürdig nach menschlichen Maßstäben sind sie nicht. Im besten Fall kann man von ihnen sagen, sie führten nur Befehle aus ...

Wer das nicht will, wem an vertrauensvollem Handeln auf Gegenseitigkeit gelegen ist, wer in einer Gesellschaft leben möchte, in der Ungleichheit begrenzt ist und in der Wohlwollen, Zweifel und Mäßigung überhaupt noch Platz finden – denn gerade diese sind hier vom Grundsatz her nicht angelegt –, wer Wert auf Privatsphäre, abweichende Ausdrucks- und auch Nichtausdrucksmöglichkeiten legt, und wer Raum für das erhalten will, was über 1 und 0 hinausgeht, der muss ein totales digitales System verhindern.

Und wie? Das Ausscheren aus der Spur kostet Zeit und Kraft. Es bedeutet, attraktive Angebote abzulehnen und auf andere, im Zweifel unbequemere Lösungen auszuweichen, soweit überhaupt vorhanden; gegen digitale Übergriffe und die Normalisierung von Überwachung Position zu beziehen; auf Netzwerkeffekte zu verzichten und neue Praktiken mühsam selbst mit zu etablieren; mit Tradeoffs und kognitiver Dissonanz und kontinuierlichem Rechtfertigungszwang für die gewählten Misstrauensstrategien zu leben. Im selbstbestimmt rationalen Vertrauen wird einem wirklich nicht viel geschenkt. Immerhin allerdings: Community.

### **Drittens: Die wichtigste Frage, die wir uns heute stellen müssen, lautet: „Wie wollen wir leben?“**

Selbstorganisierte, komplexe Systeme wie die Gesellschaft können am Rande des Chaos auch durch kleine Auslöser in ganz neue Systemzustände umschlagen. Derzeit sind viele Zukünfte denkbar. Um Veränderung in eine gute Richtung anzustoßen, müssen wir nicht nur wissen, was es zu verhindern gilt. Wir müssen auch überlegen, was sein soll und könnte.

Zu fragen, „*Wie wollen wir leben?*“ heißt, die Sinnfrage zu stellen. In der Systemtheorie markiert Sinn die Grenze des Systems nach außen und dient zur Orientierung ein- und ausgehender Kommunikationen. Sinn sagt, wer wir sind und wozu wir JA und NEIN sagen. In Bezug auf Vertrauen, und damit in Bezug auf Handlungsfähigkeit und Zukunftsgestaltung, steht am Ende immer die Sinnfrage.

Auch im Systemvertrauen, das wir in einer Gesellschaft immer leisten, stellt sich die Sinnfrage: Wann funktioniert das System für wen gut genug? Was soll als erstrebenswert gelten und welche Opfer nehmen wir dafür in Kauf?

Diese Fragen sind umso wichtiger, als datenverarbeitende Systeme durchaus Sinnangebote machen – mit Tendenz zu Sinnbildungs-Monopolen, die Sinn auf das reduzieren, was digital verarbeitet werden kann. Wir können uns weiter von digitalen Verheißungen, von Technik als Erwartung leiten lassen. Damit übernehmen wir den Sinn und die Ordnung der digitalen Gesellschaftsarchitekten, die mithilfe solcher Systeme ihre Macht verfestigen, und für die die entsprechenden Programme und Maschinen im Zentrum ihres Denkens und Handelns stehen. Wir akzeptieren dann intransparente Algorithmen als Autoritäten: proprietäre zentralisierte Systeme, die die Prozesse intersubjektiver Wahrheitsfindung unterlaufen und faktische Unbezweifelbarkeit erzeugen. Dabei schaffen sie Fakten und engen das, was machbar und was denkbar wird, zunehmend ein.

Die Frage „*Wie wollen wir leben?*“ bedeutet, Gesellschaft als durch Menschen gestaltbar zu verstehen. Alles könnte auch anders sein! Was soll im Zentrum unseres Denkens und Handelns stehen? Wir können eigene und vielleicht bessere Geschichten erzählen. Imaginierte Ordnung befördert nach Harari Kooperation und ist Grundlage gesellschaftsgestaltender Macht.<sup>4</sup> Sie drückt sich aus in den Bildern, die wir im Kopf haben, in unseren Mythen, Held:innen und unserem eigenen Rollenverständnis.

Das heißt: wir brauchen Phantasie und Mut. Wir müssen Refugien vorreduzierter Komplexität zumindest zeitweise verlassen. Wir müssen uns aus der Deckung wagen, mitreden und zuhören, um Neues und Anderes vorstellbar zu machen. Das bedeutet auch, sich von der Versuchung zu lösen, auf gesellschaftliche Fragen mit Technik zu antworten. Gemeinsamer Sinn erfordert, sich mit anderen Menschen, mit all ihrem unheimlichen Willen, ihrer offensichtlichen Fehlbarkeit auseinanderzusetzen, ihre natürliche Dummheit zu ertragen – und nicht zu vergessen, dass das immer auf Gegenseitigkeit beruht.

Die Frage „*Wie wollen wir leben?*“ ist eine echte Herausforderung. Aber wenn wir sie nicht stellen, machen andere für uns



eine Rechnung auf, in ihrem Sinn. Wagen wir neue Geschichten für eine im gemeinsamen Sinne gute analoge, digitale Zukunft.

#### Viertens: *Ethische KI ist eine Falle.*

Joseph Weizenbaum hat festgestellt: „*Unsere Gesellschaft hat die Technik entwickelt, Verantwortung so zu verteilen, dass niemand sie hat.*“<sup>5</sup> Diese Entwicklung erreicht in KI-Systemen ihren Höhepunkt.

KI, sogenannte *Künstliche Intelligenzen*, sind große Rechenmaschinen, die Daten in Entscheidungen ummünzen. In eng umrissenen Kontexten können sie wirklich erstaunliche Leistungen erbringen. Bei Entscheidungen im Alltag und im Umgang mit Menschen ist Vorsicht geboten. Wo angemessener Umgang mit Komplexität, Kontingenz, Varietät und Veränderung erforderlich ist, geraten Maschinen an ihre Grenzen. Von Sinn- und Bedeutungsfragen oder Zielkonflikten, die Situationsbewusstsein und Urteilsvermögen voraussetzen, sind sie zuverlässig überfordert. Sie soziale oder politische Entscheidungen treffen zu lassen, ist unverantwortbar.

*Ethische KI* dient dazu, das zu überwinden. Allerdings nur auf der Sprachebene. Damit ist *Ethische KI* eine Falle für alle, die auf sie vertrauen.

*Ethische KI* ist zunächst eine Einladung zum Systemvertrauen, zum Vertrauen ins digital geordnete Gesellschaftssystem. Systemvertrauen erweist man ziemlich alternativlos. Man durchschaut das System nicht, kann sich aber auch nicht entziehen und vertraut letztendlich auf das Vertrauen der anderen. Systemvertrauen funktioniert allerdings, weil es intern abgesichert ist. Es stützt sich, so Luhmann, auf sanktionsbewehrte Kontrollen, auf institutionalisiertes Misstrauen, und darauf, dass ausgeübte Macht in vielen kleinen Schritten nachvollziehbar bleibt. Wo das bei komplexen Computersystemen wie KI nicht der Fall ist, wenn also nicht sicher gesagt werden kann, was genau passiert, warum es passiert und wer dafür geradesteht, ist jedes Systemvertrauen komplett unbegründet.

Wenn jetzt also von *Ethischer KI* die Rede ist, dann ist das nichts anderes als ein Taschenspielertrick. Ethik suggeriert hehre Ziele, gute Absichten, „*wir nehmen das alles sehr ernst*“; und während man das Augenmerk darauf richtet, wird aus Vertrauen Hoffnung oder Glaube. Hoffnung, weil es nicht genug Anhaltspunkte gäbe, anhand derer sich Vertrauen rational begründen ließe; Glaube, also im Prinzip Gottvertrauen, weil einem letzten Endes nichts bleibt, als allein sich selbst in Frage zu stellen, wenn *Computer says no*.

Wer über *Ethische KI* spricht, der spielt die Moralkarte. Moral ist die höchste Stufe des Guten, um Otfried Höffe zu zitieren, sie besteht im „*höchsten Anspruch, den man an das menschliche Leben und Zusammenleben stellt, und zugleich in einem letzten Grund der Rechtfertigung.*“<sup>6</sup> Sie beansprucht im Konflikt mit instrumentellen oder pragmatischen Erwägungen kategorisch Vorrang, das Veto-Recht. Mit welcher Begründung sollte man dann das Vertrauen noch verweigern?

Guck mal!  
Ein Eichhörnchen!

*Ethische KI* legt nahe, dass Misstrauen und Kontrolle mindestens unangebracht sind, eigentlich gar nicht statthaft, und im Grunde verzichtbar, denn die KI ist ja ethisch. Wer darauf vertraut, begibt sich auf das dünne Eis der „freiwilligen Selbstverpflichtung“. Und wie gut das trägt, ist bekannt. Keine Rechenschaftspflicht, keine Verantwortung, keine Schuld. Dommage.

*Ethische KI* ist ein Etikett für ein nicht näher zu bezeichnendes Mensch-Maschinen-Ding, ein Triumph der Sprache über die Materie. *Sprache ist eine Waffe*, schrieb schon Tucholsky. So kann man den Begriff der *Ethischen KI* nämlich auch verstehen: als schärfste Waffe im Kampf um die Macht. *Ethische KI* präsentiert sich sprachlich zunächst überzeugend: hier wird das Bild eines Systems höherer Ordnung angerufen, das das Beste von Mensch und Maschine vereint. Bei näherem Hinsehen zeigt sich aber, dass mit *Ethischer KI* eine Gleichsetzung vorgenommen wird, die die Sache nicht hergibt. Die Zusammensetzung der Worte *Ethik* und *KI* verbindet zwei unterschiedliche Ebenen: die wissenschaftliche Auseinandersetzung mit Moral (Ethik) und die wissenschaftliche Anwendung von Technik (KI). Die Verkürzung dieser Ebenen auf den Begriff der *Ethischen KI* verdeckt, dass die Anwendung von Moral eben keine Frage der Wissenschaft ist, sondern von situativer Vernunft, Mäßigung und der Ausrichtung auf etwas Größeres. So wird eine sprachliche Unschärfe erzeugt, die zu einer gedanklichen Unschärfe führt, und zwar in einem starken, das Denken prägenden sprachlichen Frame: Der Begriff *Ethische KI* suggeriert, dass eine Maschine ethisch entscheiden kann, und lässt das durch ihn Bezeichnete als etwas erscheinen, dessen Wirken dank wissenschaftlicher Erkenntnisse moralisch nicht zu beanstanden ist.

*Ethische KI* klingt toll. Das ist eine Falle. Es ist ein Anspruch auf souveräne, unbezweifelbare Macht. Wer auf *Ethische KI* vertraut, lässt seinen eigenen Anspruch auf sinnvolle Mitgestaltung und Selbstbestimmung in der digitalen Gesellschaft fahren.

#### Abschließend, zu Vertrauen

Die oben beschriebenen Phänomene und Exhorte stammen aus der Masterarbeit „*Trust me! Vorschlag zum Umgang mit der Vertrauensfrage im digitalen Zeitalter.*“<sup>7</sup> Dort sind diese und etliche weitere Zusammenhänge ausgeführt und mit Quellenangaben belegt. Die Arbeit ist eine Annäherung an das Phänomen des Vertrauens, ein Versuch, den „Mechanismus“ hinter diesem Begriff für den rationalen Gebrauch fassbar zu machen und dabei den Blick für Aufforderungen zum Vertrauen zu schärfen, die in die digitale Fremdbestimmung führen.

Die Untersuchung von Vertrauen basiert auf einem Modell bei Kelton et al.<sup>8</sup> Sie umfasst vier Bereiche:

1. Die Vorbedingungen, die Vertrauen erforderlich und möglich machen: **Ungewissheit, Abhängigkeit** und **Verletzbarkeit**. Ohne diese kann es zu Interaktionen und auch zu irgendwie gearteten Beziehungen kommen, aber nicht zu Vertrauen.
2. Die Stufen des Vertrauensaufbaus: **Gefühlsbindung, Vertrautheit, Eigenkontrolle, Fremdkontrolle** und **Sinn**. Diese stellen verschiedene, auch instrumentalisierbare, Zugänge für vertrauensvollen Anschluss dar. Sie tragen dazu bei, dass Vertrauen, oder zumindest der Eindruck davon, entsteht.



3. Hinzu kommen einige indirekte, langsamer veränderliche Rahmenbedingungen des Vertrauens: **Selbstvertrauen**, **das Vertrauen der anderen** und **Kontext**. Sie prägen das Vertrauen in seiner Ausdrucksform und in dem, was es leisten soll und kann.
4. Schließlich geht es um Aspekte, an denen man sich orientieren kann, wenn man vor der Entscheidung steht, ob und wem man vertrauen will: **Kompetenz**, **Berechenbarkeit**, **Wohlwollen/Rücksichtnahme** sowie **Ethik**. Diese sind als Anhaltspunkte für das eigene Urteilsvermögen zu betrachten; sie sind weder maximal einzufordern noch in vollem Umfang überhaupt leistbar. Im nebenstehenden Kasten finden sich zu diesen Faktoren einige Leitfragen. Sie gelten ebenso für die vertrauensvolle Erwartungen anderer Menschen an uns.

#### Leitfragen Vertrauenswürdigkeit\*

##### Kompetenz:

Kannst du leisten, was ich mir von dir erwarte? Besitzt du das Wissen, die Expertise, die erforderlichen Fähigkeiten, um meine vertrauensvolle Erwartung einzulösen?

##### Berechenbarkeit:

Bietest du mir genug Anhaltspunkte, um daraus Schlüsse über dein zukünftiges Handeln abzuleiten?

##### Wohlwollen und Rücksichtnahme:

Wie stehst du zu mir? Bist du mir freundschaftlich verbunden? Liegt es in deinem Interesse, meine Interessen ernst zu nehmen?

##### Ethik:

Welchen allgemeinen Handlungsprinzipien folgst du?

- Handelst du gegen Gesetze, die ich als gerecht empfinde?
- Gibt es Anzeichen dafür, dass du nur das Minimum erfüllst, das zur Vermeidung von Sanktionen erforderlich ist?
- Urteilst du, oder führst du nur Regeln aus?
- Überlässt du es anderen, Probleme zu lösen, die du mit verursacht hast?
- Beförderst oder behinderst du soziale Gerechtigkeit?
- Unterstützt oder behinderst du die Ausbildung von Solidarität?
- Leitest du, was du sollst, oder nur, was du willst?
- Setzt du dir Grenzen?
- Lässt du mir Raum?

\*nicht abschließend, nicht maximal einzufordern

Vertrauen ist letzten Endes ein flexibles Konstrukt. Es ist für neue Maßstäbe offen und hält viele unterschiedliche Annäherungen und Deutungen aus. Nicht auszuschließen, dass in einer möglichen Zukunft jede riskante Hingabe, jede wie auch immer motivierte Zustimmung als Vertrauensbeweis herangezogen wird. Das wäre dann kein rationales oder selbstbestimmtes Vertrauen – aber wenn ein solches nicht praktiziert und eingefordert wird, zusammen mit den Bedingungen, unter denen es entstehen und gedeihen kann, wenn schließlich die Kosten für Misstrauen zu hoch werden, dann ist es sehr wohl möglich, dass Vertrauen in der digitalen Welt irgendwann tatsächlich nicht mehr bedeutet als ein resignierter oder eiliger Klick auf „ich stimme zu“.

Noch bestimmen wir, wem und wie wir vertrauen: welche Menschen wir bestärken und welche Entwicklungen wir befördern wollen. Wir können entscheiden, wozu wir mit unseren Daten beitragen und bei wem diese in guten Händen sind. Vertrauensvoll JA und vor allem auch NEIN zu sagen, ist nicht einfach. Aber unsere Entscheidungen machen einen Unterschied. Wir können, eine gute Zukunft im Blick, vertrauenswürdig sein.

## Anmerkungen

- 1 Luhmann, Niklas (2014): *Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität*. Konstanz und München: UVK Verlagsgesellschaft, S. 19-20.
- 2 Simon, Fritz B. (2007): *Einführung in die systemische Organisations- theorie*. Heidelberg: Carl-Auer-Systeme, S. 28
- 3 Weizenbaum, Joseph (1976): *Computer Power and Human Reason. From Judgement to Calculation*. San Francisco: Freeman, S. 245
- 4 vgl. Harari, Yuval Noah (2015): *Sapiens. A Brief History of Humankind*. London: Vintage, S. 117
- 5 Weizenbaum, Joseph mit Wendt, Gunna (2006): *Inseln der Vernunft im Cyberstrom? Auswege aus der programmierten Gesellschaft*. Bonn: Bundeszentrale für politische Bildung, S. 32
- 6 Höffe, Otfried (2013): *Ethik, Eine Einführung*. München: C.H.Beck, S. 19
- 7 Meiser, Silke (2019): *Trust me! Vorschlag zum Umgang mit der Vertrauensfrage im digitalen Zeitalter*. Masterarbeit an der Hochschule Emden-Leer in Kooperation mit der Universität Oldenburg. Veröffentlicht unter <https://www.ssoar.info/ssoar/handle/document/71013>
- 8 Kelton, Kari; Fleischmann, Kenneth R. & Wallace, William A. (2007). *Trust in Digital Information*. *JOURNAL OF THE AMERICAN SOCIETY FOR INFORMATION SCIENCE AND TECHNOLOGY*, 59(3):363–374.
- 9 Kontakt: [silke.meiser@meiserwerk.de](mailto:silke.meiser@meiserwerk.de)



Silke Meiser

Silke Meiser hat Management Consulting an der Hochschule Emden-Leer in Kooperation mit der Universität Oldenburg studiert. Sie setzt sich seit Jahren damit auseinander, warum Menschen tun, was sie tun, wie Systeme funktionieren und wie Sprache zur Wirklichkeitskonstruktion beiträgt. Sie ist in unterschiedlichen Funktionen beratend und im Projektmanagement tätig und freut sich über Anschluss und Austausch<sup>9</sup>, ganz besonders zu Datenschutz- und Zukunftsthemen.

## Martin Schmitt: Die Digitalisierung der Kreditwirtschaft. Computereinsatz in den Sparkassen der Bundesrepublik und der DDR, 1957-1991

Dissertation an der Technischen Universität Darmstadt



Die gesellschaftliche Entwicklung hin zu immer stärkerer Computernutzung bis in den Alltag hinein wird heute mit dem Schlagwort „Digitalisierung“ bezeichnet. Häufig entsteht der Eindruck, die Digitalisierung wurde erst von wenigen Jahren eingeleitet, so auch die Selbsterzählung der „kontinuierlichen Digitalen Revolution im Jetzt“; manche bringen es mit der Einführung des iPhone als erstem multifunktionalen Smartphone in Verbindung – einem Prozess, den wir als Mobilisierung bezeichnen. Doch die Nutzung von Computern begann bereits viel früher, als vor allem in der Arbeitswelt Leistungsprozesse verstärkt auf Rechneranlagen abgebildet wurden. Telefonen TR4, IBM 1401, später IBM System/360 oder in der DDR Robotron 300 sind Rechnersysteme, mit denen bereits in den 1960-er Jahren die Digitalisierung von Arbeitsprozessen begann – nachdem Rechner zunächst vor allem für Berechnungen im militärischen Umfeld genutzt wurden.

Einen konkreten Bereich der Digitalisierung nimmt Martin Schmitt mit seiner Arbeit *Die Digitalisierung der Kreditwirtschaft* in den Blick, um ihn historisch aufzuarbeiten. Er zeichnet die Entwicklungen anhand der Sparkassenorganisationen in Ost und West von den Anfängen 1956 bis 1991 nach, als mit der Vereinigung der deutschen Staaten auch die Sparkassenorganisationen zusammengeführt wurden. Der Bankbereich gehört zu den Branchen, in denen sich die Digitalisierung besonders anbietet, da dort Informationen in Reinform verarbeitet werden, und damit erfolgte dort die Digitalisierung zu einem relativ frühen Zeitpunkt – sowohl im kapitalistischen, marktwirtschaftlichen Wirtschaftssystem der Bundesrepublik als auch im sozialistischen, planwirtschaftlichen System der DDR. Wir verleihen ihm dafür einen dritten Preis.

Martin Schmitt orientiert sich in seiner Arbeit an folgenden erkenntnisleitenden Forschungsfragen:

- Was waren die Motive für die Banken und Sparkassen, die Verlagerung des Geschäfts in den Computer bei laufendem Geschäft zu wagen?
- Wie gestaltete sich das Wechselspiel zwischen den Kreditinstituten, ihren Mitarbeiter:innen und dem Computer aus?
- Welche Erkenntnisse erlaubt das über die breiteren wirtschafts- und zeithistorischen Entwicklungen in vergleichender Perspektive?

Dabei sieht er eine besondere Rolle in einem erweiterten Softwarebegriff und der Vernetzung als Schlüsselkategorien zur Analyse der Digitalisierung der Kreditwirtschaft.

Wir zeichnen damit eine (Technik-) Historische Arbeit aus, die gesellschaftliche Entwicklungen durch zunehmenden Computereinsatz nachzeichnet. Sie beschreibt Prozesse der Digitalisie-

rung von Beginn an, als 1954 die Städtische Spar- und Girokasse Stuttgart eine BULL Gamma 3 anschaffte – das war noch eine Rechenmaschine mit fester Verdrahtung – und dann 1957 als erster programmierbarer Computer eine IBM 650 bei der Deutschen Bau- und Bodenbank in Betrieb genommen wurde. Er illustriert grundlegende Digitalisierungsprozesse am konkreten Beispiel: Die Verlagerung der alltäglichen Arbeitsprozesse in den Computer, wo Computer vor allem zur Lösung von Wachstumsproblemen eingesetzt wurden.

Dabei werden die Entwicklungen in der damaligen Bundesrepublik und in der DDR vergleichend gegenübergestellt. Damit werden Unterschiede und Parallelen der Entwicklung in der kapitalistischen Marktwirtschaft und in der kommunistischen Planwirtschaft deutlich. Eine große Rolle spielt dabei die Software, die der Autor als Schnittstelle zwischen Computer und Gesellschaft sieht.

Die Arbeit ist in fünf Phasen der Digitalisierung gegliedert, die die Entwicklung im Zeitverlauf widerspiegeln und originell als Hochfahren – Datenverarbeitung – Vernetzung – Integration – Herunterfahren überschrieben sind:

- **Hochfahren** – Die Einführung erster Computer in bundesdeutschen Sparkassen, um die Rationalisierung aufgrund steigender Buchungszahlen durch erhöhte Sparquote und Anzahl von Girokonten zu fördern.
- **Datenverarbeitung** – Das Aufkommen des Computereinsatzes in der DDR, um die Planung in der Planwirtschaft zu perfektionieren. Da dies nicht durch Rechner aus eigener Produktion abgedeckt werden konnte, wurden Rechner aus dem westlichen Ausland eingeführt, was in der damaligen politischen Situation häufig schwierig war. Zusätzlich wurde die Entwicklung durch Machtkämpfe begleitet.
- **Vernetzung** – Die Entwicklung der Datenverarbeitung in den späten 1960-er Jahren bis Mitte der 1970-er Jahre. In der Bundesrepublik war das vor allem die IBM System/360, die später von System/370 abgelöst wurde und das Softwaresystem SODIS. In der DDR kamen Systeme der Eigenentwicklung Robotron 300 zum Einsatz, die durch importierte IBM-Rechner ergänzt wurden. Der Aufbau eines Netzwerks an Rechenstationen war auch Beitrag zur Stabilisierung der DDR.
- **Integration** – In den 1970-er und 1980-er Jahren wurde der Aufbau der digitalen Vernetzung vorangetrieben. Dadurch sollten die Kosten aus dem Verlustgeschäft der Überweisungen reduziert werden. Im Westen wurden die Leitungen durch die Deutsche Bundespost bereitgestellt. Die DDR hatte hingegen mit ihren maroden Telefonleitungen zu kämpfen. In dieser Zeit kamen auch die ersten Geldautomaten auf.



- **Herunterfahren** – Nach der Vereinigung der beiden deutschen Staaten kam es rasch zu einer Kooperation zwischen den Sparkassen in Ost und West. Bei der Vereinigung spielte erneut die Software eine wesentliche Rolle.

Die Arbeit kommt zu dem Ergebnis, dass es zwischen den beiden deutschen Staaten Ähnlichkeiten insbesondere bei den Übergängen von der mechanisierten Rechentechnik und der Rationalisierung gab. Unterschiedlich waren dagegen die Zahlungsverkehrssysteme. Die Differenz zwischen kapitalistischer Marktwirtschaft und sozialistischer Planwirtschaft wurde hauptsächlich durch die Software abgebildet.

Der Autor schließt die Arbeit mit fünf Thesen zur Digitalisierung ab:

- Sparkassen stiegen zu wesentlichen Prozessoren der Digitalisierung auf.
- Die Digitalisierung der Kreditwirtschaft prägte die Praktiken des Bezahlens.
- Der Computer vernichtete keine Arbeitsplätze.
- In der Software lässt sich ein sozialistisches digitales Zeitalter ausmachen.
- Die Digitalisierung wirkte als Restrukturierung der Betriebe.

Die Arbeit von Martin Schmitt ist eine historische Arbeit, die Technologieentwicklung und Technikgenese am Beispiel der Sparkassenorganisationen beider deutscher Staaten historisch aufarbeitet und die Schwierigkeiten der Digitalisierung anhand von Fallstudien darstellt. Sie besitzt eine hohe Relevanz für die Geschichte der Digitalisierung und damit für die gesellschaftlichen Prozesse, die die Digitalisierung bis heute begleiten. Dafür werden Technik- und Gesellschaftswandel umfassend und überzeugend verknüpft. Die Arbeit ist sehr umfangreich und stützt sich auf umfassendes Quellenmaterial.

Der große Umfang hat den Nebeneffekt, dass manche Ergebnisse auch in der Fülle des Materials „verschwinden“. Dies tut der Arbeit aber keinen Abbruch. Sie stellt die Verbindung zwischen technischer und gesellschaftlicher Entwicklung über einen langen Zeitraum überzeugend dar und leistet einen wichtigen Beitrag zum Verständnis gesellschaftlicher Prozesse der Digitalisierung, die die Grundlage der beschleunigten Entwicklungen der heutigen Digitalisierung und Mobilisierung bilden. Sie zeigt auch eindrucksvoll, dass technische Gestaltungsfragen an wesentlichen Punkten nicht technisch, sondern machstrategisch entschieden werden – ein Kernarbeitsfeld des FfF. Die Jury hat sich deswegen für die Auszeichnung der Arbeit entschieden.

**Herzlichen Glückwunsch, Martin Schmitt, zum Weizenbaum-Studienpreis 2021.**



**Martin Schmitt**

## Die Digitalisierung der Kreditwirtschaft

### Computereinsatz in den Sparkassen der Bundesrepublik und der DDR, 1957–1991



**3. Preis**

*Die Bankenbranche ist 2021 in hellem Aufruhr: Stellenabbau, Filialschließungen, Fusionen, Kundenverlust und neue Konkurrenten auf dem Markt prägen die letzten Jahre. Als Begründung wird oftmals die Digitalisierung angeführt. Ein Blick in die jüngere Geschichte der Digitalisierung hilft dabei, diesen Wandel einzuordnen und kritisch zu reflektieren.*

Derzeit durchläuft die Bankenbranche einen intensiven Wandel: Stellen werden abgebaut, Zweigstellen geschlossen, Institute fusionieren, die Zinsen bleiben niedrig und die Gebühren steigen. Die Zahl der Zweigstellen in der Sparkassenorganisation sank beispielsweise von etwa 19.000 im Jahr 1990 auf heute etwa 8.000. In der Folge wechseln Kund:innen reihenweise ihre Hausbank. Informatiker:innen setzen die Kernbankensysteme neu auf und alternative Akteure wie Google, Paypal oder kleinere FinTechs drängen auf den Markt. Hinzu kommt, dass neue Zahlungsformen und digitale Währungen die klassische Überweisung, das Bargeld und das Bezahlen mit der Girokarte ergänzen oder zurückdrängen. Als Begründung wird oft die Digitalisierung angeführt. Eine längere historische Perspektive zeigt, dass besagte „Digitalisierung“ von Menschen gemacht wurde und in der Kreditwirtschaft eine lange Vorgeschichte hat. Diese Vorgeschichte zu verstehen hilft, die gegenwärtige Problemlage einzuordnen. Denn etwa 8.000 Zweigstellen besaßen die Sparkassen auch im Jahr 1957, als die Digitalisierung in der Bankenbranche begann. In den folgenden Dekaden setzten Ban-

ken und Sparkassen umfangreiche digitale Systeme auf. Viele Bundesbürger:innen kamen abseits vom Arbeitsplatz oftmals in ihrer Bank zum ersten Mal mit digitaler Computertechnologie in Kontakt, sei es durch ihr Konto, eine Führung ins Rechenzentrum der örtlichen Sparkasse, am Schalter oder dem Geldautomaten. Banken brachten Computer in das Leben der Kund:innen – und bildeten sie digital weiter, beispielsweise in Computerkursen der 1980er-Jahren. Damit trugen sie zur digitalen Selbstbestimmung bei. Gleichzeitig erfassten Banken sehr früh Daten über ihre Kund:innen und sahen diese als ihr *Kapital* an. Daten setzten sie für Werbezwecke ein, beispielsweise auf dem neu eingeführten Kontoauszug. Sie *informationalisieren* ihre Kund:innen in ihren Computersystemen, ohne ihnen gleichermaßen eine digitale Selbstbestimmung zuzugestehen – der Begriff „informationalisieren“ verweist auf die Vorarbeiten von Christiane Floyd, die dieses Jahr mit der Weizenbaummedaille ausgezeichnet wurde [1]. Die neuen Akteure im Zahlungsverkehr wie Paypal oder Google zeigen, dass die Kreditwirtschaft mit dem Bankengeheimnis der Datennutzung vergleichsweise



enge Grenzen setzte. Es ist also Zeit, die „Digitalisierung der Kreditwirtschaft“ [2], so der Titel meiner jüngst erschienen Dissertation, in längerer Linie zu verstehen. Welche Tragweite hatte der Computereinsatz in der Kreditwirtschaft und was bedeutete dies für die Selbstbestimmung der Kund:innen? Im Mittelpunkt des Beitrags steht dabei das Endkundengeschäft der Sparkassen in der Bundesrepublik und der DDR von 1957 bis 1991. Sie bieten sich als Untersuchungsgegenstand an, da sie eine hohe Verbreitung und viele Kund:innen in beiden deutschen Staaten hatten.

### Anfänge

Die Digitalisierung begann in Deutschland früher als gemeinhin angenommen. Bisher blickte die Forschung meist auf die 1970er-Jahre, als sich digitale Computertechnologie in der Breite durchsetzte, oder auf die 1980er-Jahre und den PC. Demgegenüber lässt sich am Einsatz von Computertechnik in der deutschen Wirtschaft zeigen, wie vor allem in der Bundesrepublik die Digitalisierung früher wirkmächtig wurde (Abbildung 1).

1952 experimentierten Wissenschaftler:innen des Max-Planck-Instituts für Physik in Göttingen mit ersten Digitalcomputern. 1953 folgte die Optische Industrie, die auf Zuse-Fabrikate setzte; Unternehmen wie RWE in Essen nutzten elektronische Zusatzmodule zu ihren Lochkartenanlagen. 1955 unterschrieb die Betriebsleitung der Farbwerke Hoechst als Vorreiter der Chemiebranche den Vertrag zur Nutzung eines IBM-Großrechners. Im selben Jahr kam in der DDR der erste Computer zum Einsatz, ebenfalls in der optischen Industrie. Carl-Zeiss setzte in Jena die Eigenentwicklung Oprema zur Linsenberechnung ein. Die Firma wurde zu einem frühen Computerhersteller im sozialistischen Staat. An der TU Dresden bauten Wissenschaftler den ersten Kleincomputer D1. Auch kommunale Institutionen setzten auf Digitalcomputer; 1956 beispielsweise das Landesamt für Flurbereinigung Ludwigsburg.

1956 lässt sich zudem eine Entwicklung in der Breite feststellen: Mit dem Europäischen Rechenzentrum von Univac und dem IBM-Rechenzentrum in Sindelfingen markierten zwei US-Hersteller das Feld in Westeuropa. Auch staatliche Akteure setzten auf Computertechnik, beispielsweise die Bundeswehr oder die Staatliche Rentenversicherung. Universitäten wie die TH Mün-

chen profitierten nun von einem Förderprogramm der DFG. Unternehmen wie die Allianz, Opel oder Volkswagen betrieben Computer in der Verwaltung [3]. Das war der Kontext, in dem sich 1957 zum ersten Mal die eher konservative Kreditwirtschaft an den Computereinsatz wagte: Die Deutsche Bau- und Bodenbank in Mainz kaufte eine IBM 650 und ein Jahr später die Dresdner Bank einen Univac-Computer in Hamburg. Das ergibt ein klares Bild: Bereits Mitte der 1950er-Jahre setzten deutsche Unternehmen, Universitäten und öffentliche Einrichtungen auf Computer. Neben einer interessanten regionalen Häufung zeigt sich zudem: Die Kreditinstitute lagen bei der Digitalisierung ganz im Trend.

Unter *Digitalisierung* verstehe ich zwei Dinge: Erstens den technischen Prozess der Umwandlung analoger in digitale Signale (Abbildung 2). Etymologisch stammt „digital“ von lateinisch *digitus* ab, was „Finger“ oder „Zehe“ bedeutet. Unter Digitalisierung als technischem Prozess verstehe ich aber nicht nur die ziffernmäßig-zählende, sondern auch elektronische Repräsentation von Werten und Signalen. Das Elektronische miteinzubeziehen macht einerseits technisch Sinn, da es die Dimension des Digitalen enorm erweiterte, aber auch historisch, da dadurch das Digitale einen analytischen Differenzcharakter zu vorherliegenden Prozessen bekommt.



Abbildung 2: Die Digitalisierung der Kreditwirtschaft. Computereinsatz in den Sparkassen der Bundesrepublik und der DDR 1957-1991, Göttingen: Wallstein-Verlag 2021, 656 S., 58 €.



Jahr	Institution	Rechner
1952	Max-Planck-Institut für Physik, Göttingen	G1
1953	Optische Werken Ernst Leitz, Wetzlar	Zuse Z5
1954	MPI Göttingen	G2
1955	Carl-Zeiss, Jena	OPREMA
-	TU Dresden / Funkwerk Dresden	D1
1956	Univac, Europäisches Rechenzentrum Frankfurt	UNIVAC I
-	IBM, Rechenzentrum Sindelfingen	IBM 650
-	Maschinelles Berichtswesen, Bundeswehr	IBM 650
-	Bundesversicherungsanstalt Berlin (1)	IBM 650
-	Allianz, Hamburg	IBM 650
-	TH München	PERM
-	DEW Krefeld	IBM 650
-	Volkswagen, Wolfsburg	IBM 650
-	Chemische Werk Hüls, Marl	Siemens
-	Flurbereinigungsdirektion, Bamberg	Zuse Z11
-	Landesamt für Flurbereinigung, Ludwigsb	Zuse Z11

Jahr	Institution	Rechner
1957 /01	AEG Berlin	IBM 650
- /02	TH Darmstadt	DERA; 2x IBM 650
- /04	Mannesmann Düsseldorf	IBM 650
- /06	TH Hannover	IBM 650
- /09	BFA Berlin (2)	IBM 650
- /10	Quelle, Fürth	SEL ER-56
-	Bundesbahndirektion, Frankfurt	SEL
- /11	Bayer Leverkusen (1)	IBM 650
-	Farbwerke Hoechst AG, Frankfurt a.M.	IBM 705
-	Leitz, Wetzlar	Elliot 402 F
-	Opel, Rüsselsheim	SEL
-	Bayr. Landesvermessungsamt, Münch.	Zuse Z11
-	TU Dresden / Funkwerk Dresden	D2
-	Deutsche Bau- und Bodenbank Mainz	IBM 650
1957/58	Dresdner Bank, Hamburg	Univac S590
...	...	...

Abbildung 1: Computer in Deutschland (Auswahl), 1957

Zweitens verstehe ich unter Digitalisierung einen historischen Prozess: Die Verbreitung digitaler Informationstechnologie und deren Durchdringung aller Bereiche von Staat über Wirtschaft bis Gesellschaft. Die Betonung liegt hier auf dem zeitlichen Verlauf und der wechselseitigen Beeinflussung von Technik und Gesellschaft. Computerisierung war ein Teilprozess der Digitalisierung mit dem Computer als dominanter Technologie. Dieser lässt sich zum Teil bereits mit *klassischen* historischen Quellen wie Fachzeitschriften, Archivquellen aus Unternehmen, Sitzungsprotokollen, Beschlussvorlagen, Statistiken, Karten, Zeitzeugeninterviews, Gesetzestexten, Korrespondenzen, Sekundär- und grauer Literatur herausarbeiten. Zeitungsartikel sind mit Vorsicht zu genießen, können aber beispielsweise hoch aggregiert die Wahrnehmungen von Digitalisierung abbilden. Dabei herrscht eine gewisse Asymmetrie der Quellenherkunft. Während auf Seiten der DDR-Kreditinstitute zumeist staatliche Quellen vorliegen, handelt es sich in der Bundesrepublik um semi-staatliche, meist privatwirtschaftliche Provenienz.

In voller Konsequenz ist Digitalgeschichte nur mit digitalen Methoden zu verstehen. Innovativ ist daher der Ansatz, Software als neue Quellengattung nutzbar zu machen. Durch die Analyse von Software rücken die Anwender des Computers stärker in den Vordergrund. „Software“ verstehe ich in Anlehnung an Michael S. Mahoney nicht als Synonym für „Programm“, beispielsweise Photoshop. Vielmehr gehe ich von einem breiteren Software-Begriff aus und verstehe darunter eine *Assemblage* aus Programmcode, Daten, Arbeitsanweisungen, Betriebsprozessen, Routinen, Regulierungen, aber auch Hardware oder Kund:innen [4]. In der Software bildeten die Programmierer:innen die Sparkasse ab. Je nach historischer Situation wurde die Assemblage unterschiedlich konfiguriert, wodurch sich die sozial- und wirtschaftshistorische Dimension der Digitalisierung in ihrer komplexen Verflochtenheit im zeitlichen Verlauf aufzeigen lässt. Je nach Assemblage besaßen Kund:innen einen unterschiedlichen Grad der Selbstbestimmung. Der Untersuchungszeitraum lässt sich in vier Phasen unterteilen: Eine Phase der *Initialisierung* von 1957-67, eine Phase der *Datenverarbeitung* von 1968-75, eine *Vernetzungsphase* von 1976-87 und schließlich die Phase der *Integration* von 1988-91.

### 1957-1967

Die Phase der Initialisierung zeichnete sich durch tastende Experimente der Sparkassen und die Überführung der neuen Technologie in den Produktiveinsatz aus. Es war noch nicht ausgemacht, wofür Bankmitarbeiter:innen den Computer einsetzen konnten und ob er sich rentierte. Der 1957 angeschaffte IBM-Computer der Deutschen Bau- und Bodenbank in Mainz steht exemplarisch für viele andere; zahlreiche Sparkassen folgten in den 1960er-Jahren. Dem Management gelang es, bei konstanter Personalzahl eine steigende Bilanzsumme zu verwalten, zusätzliche Geschäftsfelder zu erschließen und überschüssige Rechenzeit zu vermieten. Die Bank digitalisierte die interne Verbuchung und ging von der analogen Kontokarte zum digital geführten Konto über. Dabei zeigte sich schnell, welche Eigendynamik die Digitalisierung bekam. Nach kurzer Zeit setzten die Mitarbeiter:innen den Computer für Zwecke jenseits der ursprünglich anvisierten Nutzung ein. Die Folge daraus war, dass sich innerhalb von drei Jahren der Software-Einsatz von einem

Programm zu 50 Programmen auswuchs. Mehr als die Hälfte erledigte bankfremde Arbeiten. Die Assemblage der Bank wurde branchenweit neu konfiguriert. Markante Chiffre des Wandels war die Einführung des kostenlosen Girokontos, beispielsweise bei den Sparkassen, das die Lohntüte ablöste.

Auf beiden Seiten des Eisernen Vorhangs strebte die Kreditwirtschaft nach Erfahrungen mit Computern. So gelangte eine Broschüre der Kreissparkasse Saarbrücken über die Grenze und wurde in der DDR über einhundert Mal reproduziert. Digitalisierung wurde nicht separat, sondern in internationalen Verflechtungen realisiert und stets politisch aufgeladen. In der DDR bettete die Partei sie einerseits in die kollektiven, von der Sowjetunion inspirierten Ansätze zentraler Großrechenzentren ein. Hauptziel war anfangs die Planoptimierung; die Rationalisierung in den Sparkassen folgte dem nur nachrangig. Andererseits importierten die Finanzorgane 1965 einen Rechner vom US-Militär. Sie setzten so auf Technik aus dem Westen, bevor eigene Technik verfügbar war. Dementsprechend zeigte sich ein sozialistischer Weg in das Digitale Zeitalter vor allem in der Software, so meine These.

### 1968-1974

Ab 1967/68 begann in den deutschen Kreditinstituten eine Phase, in der sich Computer und Software in der Breite durchsetzten: Die Phase der *Datenverarbeitung*. In beiden Staaten schafften die Kreditinstitute massenhaft Computer an und bauten große, regionale Rechenzentren auf (Abbildung 3). Treiber waren sowohl kleinere Institute in ländlichen Regionen, als auch Großinstitute in Metropolregionen. Die Untersuchung von Software heißt auch, den Blick in deutsche Rechenzentren und deren Arbeitsalltag zu werfen. Sparkassen verlagerten immer weitere Teile ihres Betriebs in die Software. Damit senkten sie die internen Transaktionskosten. Einerseits erhöhte dies die digitale Selbstbestimmung der Mitarbeiter:innen, beispielsweise von Frauen, die nun nicht mehr nur Lochkarten lochten. Während



Abbildung 3: Großrechenzentrum der Niedersächsischen Sparkassen, 1977. Quelle: DSGV



Kreditinstitute Computer anfangs wie Lochkartenmaschinen eingesetzt hatten, bekam deren Einsatz fortan eine neue Qualität. Andererseits engte eine zunehmende Standardisierung, Quantifizierung und Abrufbarkeit die Handlungsspielräume der Menschen ein. Hier ließe sich jenseits der Datenbanken der Sparkassen und der Informationalisierung der Kund:innen als Beispiel der Computereinsatz in den Sicherheitsbehörden anführen, der in beiden deutschen Staaten vorangetrieben wurde [5]. Dieses und viele weitere Beispiele unterstreichen, dass Computer Infrastruktur geworden waren. So lässt sich ab etwa 1970 vom Beginn des Digitalen Zeitalters sprechen. Ab dann ging es in vielen Bereichen wie dem Bankwesen schlicht nicht mehr ohne Computer.

### 1975-1987

Nach dem Aufbau der Infrastruktur in den Sparkassen beider Staaten begannen die Institute, ihre solitären Installationen miteinander zu vernetzen. Damit senkten sie die inter-institutionellen Transaktionskosten. *Vernetzung* wurde zum dominanten ökonomischen Leitbegriff. In der Bundesrepublik und DDR bauten die Sparkassen elektronische Zahlungsverkehrs-Netzwerke auf. An diese schlossen sie Terminals und Geldautomaten an. Parallel dazu experimentierten sie mit Formen bargeldlosen Bezahls wie BTX oder der Kartenzahlung. Das bildete die Grundlage für den Wandel der Sparkassen zu Bankdienstleistern aus einer Hand mit erweitertem Produktportfolio, während im Osten die Rationalisierung geldwirtschaftlicher Prozesse im Vordergrund stand. Dazu zählten auch die Geldautomaten, ein früherer Berührungspunkt für Menschen mit Computertechnik. Die neu geschaffenen Datennetze zogen schon bald die ersten Hacker an. Von großem medialem Interesse begleitet *hackten* sich die Gründer des Chaos Computer Clubs in die Rechner der Hamburger Sparkasse. Allerdings nicht, um sich zu bereichern, sondern um einer Aneignung von Computern durch die Gesellschaft spielerisch Vorschub zu leisten, auf soziotechnische Schwachstellen im Digitalen Zeitalter hinzuweisen und den Bürger:innen ihre digitale Selbstbestimmung zurückzugeben [6].

### 1988-1991

Im Prozess der Wiedervereinigung lässt sich schließlich erkennen, welche zentrale Stellung die elektronische Datenverarbeitung in Deutschland eingenommen hatte. Algorithmen auf di-



Abbildung 4: 1.000 PC für die DDR-Sparkassen, 1990.  
Quelle: DSGV

gitalen Computern trugen zu einer gelingenden Überleitung vom Sozialismus in den Kapitalismus bei (Abbildung 4), beispielsweise in der Währungsumrechnung oder in Überleitungsprogrammen. Auch ohne Computer wäre die Wirtschafts- und Währungsunion gelungen. Aber sie machte bestimmte Lösungen und Geschwindigkeiten in turbulenten Zeiten möglich. Auch machte sich die jahrzehntelange Erfahrung der Sparkassen der DDR in Digitalisierungsfragen bemerkbar. Sie und ihre Rechenzentren wurden eben nicht zu Spielbällen des Westens in einer schlichten *Übernahme*. Vielmehr gelang es Mitarbeiter:innen und Leitungsebene zusammen, im gemeinsamen Staat anzukommen. Dazu trugen Schulungen, Lehrprogramme und Arbeitsanweisungen bei. Die Assemblage Software wurde abermals neu konfiguriert.



### Martin Schmitt

**Martin Schmitt** ist Wissenschaftlicher Mitarbeiter an der TU Darmstadt sowie am Leibniz-Zentrum für Zeithistorische Forschung Potsdam assoziiert. Zu seinen Forschungs- und Publikationsfeldern gehören die Geschichte des Digitalen Zeitalters, Technik- und Wirtschaftsgeschichte. Zuletzt erschien von ihm sein Buch „Die Digitalisierung der Kreditwirtschaft. Computereinsatz in den Sparkassen der Bundesrepublik und der DDR 1957-1991“, Göttingen: Wallstein-Verlag 2021, 656 S., 58 €.

## Prozessoren des Digitalen Zeitalters

Welche Tragweite hatte der Computereinsatz in der Kreditwirtschaft und was bedeutete er für die Selbstbestimmung der Kund:innen? Antworten auf diese Fragen lassen sich in fünf Thesen pointiert zusammenfassen. Erstens: Banken und Sparkassen trieben die Digitalisierung in Deutschland voran, indem sie Massendaten aufzeichneten (Input), verarbeiteten (computing), über unterschiedliche Interfaces vom Kontoauszug bis zur Kreditvergabe ausgaben und damit Impulse setzten oder auf die technische Entwicklung Einfluss nahmen (Output). Sie sind dabei in eine breite Reihe von Impulsgebern des historischen Prozesses der Digitalisierung einzuordnen. Kreditinstitute und besonders Sparkassen brachten Computertechnik in den Alltag der Menschen, Kund:innen wie Mitarbeiter:innen. Zweitens: Die viel beschworene *Liebe der Deutschen zum Bargeld* lässt sich nicht allein auf die Inflation der Zwischenkriegszeit zurückführen, sondern hing eng mit dem Scheitern von Digitalisierungs-Prozessen in beiden deutschen Staaten zusammen. Drittens lässt sich feststellen, dass der Computer im Untersuchungszeitraum in absoluten Zahlen nicht zu einem Arbeitsplatzabbau in der Kreditwirtschaft führte. Er ermöglichte neben anderen Faktoren sogar einen Zugewinn an Arbeitnehmerrechten, beispielsweise die Fünf-Tage-Woche. Allerdings lässt sich eine *schleichende Rationalisierung* und ein Wechsel der Tätigkeitsprofile feststellen. Die Digitalisierung der Kreditwirtschaft betraf vor allem weibliche Beschäftigte. Sie bot allerdings Frauen auch neue Tätigkeitsfelder und Aufstiegschancen, im Osten mehr als im Westen. Viertens diente Digitalisierung oft als Legitimation für Veränderungen von Betriebsabläufen in beiden deutschen Staaten. Die Leitungsebene verknüpfte sie mit der Implementation neuer Formen der Betriebssteuerung und des *Controlling*. Digitalisierung der Kreditwirtschaft hieß dabei nicht nur eine Beschleunigung und quantitative Ausweitung der Abläufe, sondern erstmal ganz basal deren Standardisierung und Formalisierung in der Abbildung in Software. Das wiederum verringerte Handlungsspielräume. Die ersten Nutznießer der Digitalisierung der Kreditwirtschaft waren dabei nicht die Kreditinstitute selbst, sondern deutsche Unternehmen im historischen Wandel von der Lohntüte zum Girokonto. Fünftens und letztens lässt sich ein genuin sozialistischer Weg in das Digitale Zeitalter ausmachen. Dieser schlug sich in Software als neuer historischer Quellengattung nieder, die Historiker:innen bei der Analyse von Digitalisierungs-

Prozessen zu berücksichtigen haben. In ihr finden sich die systemischen und kulturellen Eigenlogiken des Ostblocks als *Spuren des Sozialismus*. Vor allem in der Phase der Wiedervereinigung treten diese Spuren markant hervor. Der Vergleich beider deutscher Staaten wirkt hier als ein stetes Korrektiv. Er mahnte, die gewonnenen Erkenntnisse zur Digitalisierung nicht leichtfertig zu generalisieren, sondern in ihren jeweiligen Systemspezifika zu denken. Jenseits eines reinen Vergleichs treten aber auch die Verflechtungsprozesse hervor. Die Digitalisierung in beiden Staaten war asymmetrisch aufeinander bezogen, teilweise sogar verflochten. Sie war keine lineare Erfolgsgeschichte, veränderte aber die Institute und damit auch die Möglichkeiten von Kund:innen für digitale Selbstbestimmung von Grund auf.

## Referenzen

- [1] Floyd, Christiane (1999) Menschsein in der informatisierten Gesellschaft – zur Virtualisierung des Selbst, in: Bittner, Peter und Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (Hrsg.): *Mensch – Informatisierung – Gesellschaft: Beiträge zur 14. Jahrestagung des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FifF) e. V.*, 13.-15. November 1998 an der TU Darmstadt, Münster: LIT-Verlag, S. 21–42.
- [2] Schmitt, Martin (2021) *Die Digitalisierung der Kreditwirtschaft. Computereinsatz in den Sparkassen der Bundesrepublik und der DDR 1957-1991*, Göttingen
- [3] Funke, Janine (2018) Digitalisierung in der frühen Bundeswehr. Die Einführung elektronischer Rechenmaschinen in Verwaltung, Forschung und Führungssystemen, in: Frank Bösch (Hrsg.): *Wege in die digitale Gesellschaft. Computernutzung in der Bundesrepublik 1955-1990*, Göttingen 2018, S. 86–101; Bösch, Frank (2020) *Wege in die digitale Gesellschaft. Computer als Gegenstand der Zeitgeschichtsforschung*, in: ebd., S. 7–36; Kasper, Thomas: *Wie der Sozialstaat digital wurde. Die Computerisierung der Rentenversicherung im geteilten Deutschland*, Göttingen;
- [4] Mahoney, Michael (2008) What Makes the History of Software Hard, in: *IEEE Annals of the History of Computing* 30/3, S. 8–18.
- [5] Bergien, Rüdiger (2019) Programmieren mit dem Klassenfeind. Die Stasi, Siemens und der Transfer von EDV-Wissen im Kalten Krieg, in: *Vierteljahresshefte für Zeitgeschichte* 67/1, S. 1–30.
- [6] Erdogan, Julia Gül (2021) *Avantgarde der Computernutzung. Hackerkulturen der Bundesrepublik und DDR*, Göttingen, S. 205-231.



#FifFKon21

12. bis 14. November 2021  
München, Schulzentrum-Nordhaide

Verleihung des Weizenbaum Studienpreises



## Neumitglieder-Onboarding & intergalaktischer FfF-Stammtisch

Alle Mitglieder, insbesondere Neumitglieder, sind viermal im Jahr herzlich eingeladen, am Neumitglieder-Onboarding und dem anschließenden intergalaktischen Online-Stammtisch teilzunehmen!

Beginnend im Januar heißen wir am jeweils dritten Mittwoch im Monat ab 19 Uhr alle Neumitglieder willkommen. Das FfF möchte euch kennenlernen, sich mit euch austauschen und eure Fragen beantworten. Wir geben einen kurzen Einblick in die Arbeitsweise des FfF und in unsere Online-Tools (Wiki, Pads, Nextcloud, Jitsi), damit ihr euch einbringen und informieren könnt.

Ab 20 Uhr findet dann der intergalaktische FfF-Stammtisch statt, in dem sich Mitglieder aus allen Regionen vernetzen und in regen Austausch miteinander treten können.

Schaut gern vorher ins Pad und tragt eure Themenvorschläge ein [pads.fiff.de/p/intergalaktischerStammtisch](https://pads.fiff.de/p/intergalaktischerStammtisch) oder stellt Fragen schon vorab an [onboarding@fiff.de](mailto:onboarding@fiff.de)

Wir freuen uns auf Euch und sehen uns das nächste Mal am 20. April 2022 unter [jitsi.fiff.de/onboarding](https://jitsi.fiff.de/onboarding).

FfF e. V.

## Mitgliederversammlung des FfF München, 14. November 2021, 12:40 – 15:15 Uhr – Beschlussprotokoll –

**Sitzungsleitung:** Stefan Hügel als Vorsitzender des FfF

### 1. Begrüßung und Feststellung der Beschlussfähigkeit und der Protokollführung

Zur Versammlung wurde satzungsgemäß eingeladen. Sie ist damit beschlussfähig. Die Online-Teilnehmer nehmen in einem Jitsi-Raum teil.

Protokollführung: Werner Winzerling

### 2. Beschlussfassung über Tages- und Geschäfts- und Wahlordnung

Vor dem Bericht des Vorstandes soll das Wahlverfahren erläutert werden.

Der Tagesordnung wurde in der vorliegenden Form mit der Ergänzung zugestimmt. Geschäfts- und Wahlordnung werden von der MV in bekannter Form genehmigt.

### 3a. Erläuterungen des hybriden Wahlablaufes

Die MV wählt einstimmig Frieder Strauß als Wahlleiter. Frieder Strauß erläutert den hybriden Wahlablauf. Einträge ins Wahlregister sind bis 13.30 Uhr möglich.

### 3b. Bericht des Vorstandes einschl. Kassenbericht

Stefan Hügel berichtet über die Arbeit des FfF seit der letzten MV am 15.11.2020 sowie über den Haushalt mit Stand 5.11.2021.

Außerdem berichten Vertreter der Regionalgruppen. Es gab keine Nachfragen zu dem Bericht des Vorstands. Es wurden keine Beschlüsse gefasst.

### 4. Bericht der Kassenprüfer

Für die am 28.7.2021 in Bremen durchgeführte Kassenprüfung durch Klaus Lüttich und Andreas Spillner berichtet Klaus Lüttich der MV. Es wurden keine Beschlüsse gefasst. Aus dem Kassenprüfungsprotokoll:

„Dem Vorstand wird eine dem Vereinszweck entsprechende, ordnungsgemäße Kassenführung bescheinigt. Einer Entlastung des Vorstandes steht nach unserer Auffassung nichts entgegen.“

### 5. Diskussion der Berichte

Es wurden keine Beschlüsse gefasst.

### 6. Entlastung des Vorstandes

Die Kassenprüfer schlagen die Entlastung des Vorstandes vor. Die MV entlastet den Vorstand einstimmig bei 3 Enthaltungen.

### 7. Neuwahl des Vorstandes

Wahlleiter Frieder Strauß wird bei der Durchführung der Wahl unterstützt von Benjamin Kees und Rainer Rehak. Es liegen 30 Registrierungen zur Wahl vor. Alle 30 sind stimmberechtigte Mitglieder.

Nach Diskussion und Abstimmung stimmt die MV der Kandidatur des Wahlleiters für den Vorstand zu.

Wahlgang:

**Vorsitzender:** Stefan Hügel (einziger Kandidat)

Abgegebene gültige Stimmen: 28 | (ja/nein/enth.): 26/1/1

**Wahl angenommen**

**Stellvertretender Vorsitzender:** Rainer Rehak (einziger Kandidat)

Abgegebene gültige Stimmen: 28 | (ja/nein/enth.): 24/3/1

**Wahl angenommen**

**Beisitzerinnen und Beisitzer** (siehe Tabelle S. 63 links oben)

Der wiedergewählte Vorsitzende, Stefan Hügel, dankt im Namen des gesamten Vorstands dem scheidenden Vorstandsmitglied Jens Rinne für seine langjährige Arbeit im FfF-Vorstand.

### Wahl der Beisitzerinnen und Beisitzer

Kandidat	Gültige Stimmen	ja/nein/enth.	Wahl angenommen?
Michael Ahlmann	28	19/8/1	Ja
Maximilian Hagner	27	12/8/7	Ja
Alexander Heim	28	21/5/2	Ja
Sylvia Johnigk	28	22/3/3	Ja
Benjamin Kees	28	26/1/1	Ja
Hans-Jörg Kreowski	28	26/2/0	Ja
Kai Nothdurft	28	26/2/0	Ja
Britta Schinzel	28	26/1/1	Ja
Ingrid Schlagheck	28	25/2/1	Ja
Anne Schnerrer	28	23/3/2	Ja
Frieder Strauß	28	20/6/2	Ja
Werner Winzerling	28	22/3/3	Ja

### 8. Neuwahl der Kassenprüfer

Die MV wählt im Block einmütig zu den neuen Kassenprüfern des FIF: Margita Zallmann (stimmt zu) und Berthold Hoffmann (hat Zustimmung in Falle der Wahl vorher erklärt)  
Abstimmung 25/0/0 (ja/nein/enth.)

### 9. Diskussion über Ziele und Arbeit des FIF, aktuelle Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen

Die Regionalgruppen hatten bereits unter TOP 3 berichtet. Es wurden keine Beschlüsse gefasst.

### 10. Anträge an die Mitgliederversammlung

- entfällt -

### 11. Verschiedenes

Es lagen keine Anträge vor.

### 12. Genehmigung des Protokolls

Das Protokoll wird von der MV einstimmig genehmigt.



Stefan Hügel und Rainer Rehak

## Jahresrückblick 2020/2021

### Freie Fahrt durch das FIF-Jahr – immer noch in Zeiten von Covid-19

Im Jahresrückblick stellen wir die wichtigsten Aktivitäten des FIF seit der FIF-Konferenz 2020 dar, die im November 2020 online stattfand. Mit Auszügen aus unseren Stellungnahmen, Pressemitteilungen und Beiträgen zur FIF-Kommunikation illustrieren wir die Aktivitäten. Die Liste ist nicht vollständig; wir sind auch darüber hinaus als Autor:innen, bei Veranstaltungen, Demonstrationen und weiteren Aktivitäten beteiligt. Klar ist aber, dass die Covid-19-Pandemie auch bei uns erhebliche Spuren hinterlassen hat.

#### November 2020

Am 14./15. November findet unsere **FIF-Konferenz 2020** statt – pandemiebedingt als digitale Konferenz, statt wie geplant in Weimar. Das Leitmotiv war diesmal **Mit dem Wissen wächst der Zweifel – Vereinbarkeit und Widersprüche der Designziele Datenschutz, IT-Sicherheit, Usability und Barrierefreiheit**:

*„Datenschutz, Informationssicherheit, Usability und Barrierefreiheit sind allgemein gesellschaftlich erwünschte Designziele und Anforderungen für Informationssysteme, die sich aber teilweise widersprechen. Wie können sie gemeinsam umgesetzt werden, wo stehen sie im Widerspruch? Wie können sie gesellschaftspolitisch realisiert und ausgehandelt werden? [...]“*

Im Rahmen der Konferenz verliehen wir wieder den **Weizenbaum-Studienpreis**: Dieses Jahr an Lisa Herfurth für ihre Arbeit **Schubladendenken 3.0 – Diskriminierung durch Social Scoring**.

Anne Schnerrer und Hans-Jörg Kreowski hielten auf dem **Nat-Wiss-Kongress 2020 Herausforderungen für Frieden und Umwelt** einen Vortrag zum Thema **Informatik zwischen Cyberpeace und Bits & Bäume**.

#### Dezember 2020

In einem gemeinsamen **offenen Brief** an Bundesministerien zur **Verbändebeteiligung** kritisierten wir gemeinsam mit mehreren Organisationen die zu kurzen Fristen, innerhalb derer Stellungnahmen zu Anhörungen erwartet werden:

*Leider werden seitens der Bundesministerien in zunehmendem Maße Stellungnahmen zu Gesetzesvorschlägen in weniger als drei Arbeitswochen – teilweise von gerade einmal wenigen Werktagen – erwartet. Trauriger Tiefpunkt waren im Dezember 2020 die Anfragen zu Stellungnahmen für den 4. Referentenentwurf zum IT-Sicherheitsgesetz 2.0 mit einer Kommentierungsfrist von 28 Stunden (bei 108 Seiten) und zur Novellierung des Telekommunikationsgesetzes mit einer Frist von 2 Tagen (bei 465 Seiten).*

Bei der **remote Chaos Experience rC3**, der Covid-19-bedingt virtuellen Ausgabe des **Chaos Communication Congress**, waren wir wieder an einer **Assembly** beteiligt.

## Januar 2021

Wolfgang Hofkirchner und Hans-Jörg Kreowski geben einen **Sammelband** zum **Transhumanismus** heraus: *Transhumanism – The Proper Guide to a Posthuman Condition or a Dangerous Idea?* Der Band enthält unter anderem Beiträge der FIF-Mitglieder Wolfgang Hofkirchner, Rainer Rehak, Britta Schinzel und Christian Stary.

## März 2021

Hans-Jörg Kreowski vertritt das FIF bei der digitalen **Zivilklausel**-Veranstaltung *Sag Nein! Der aufhaltsame Aufstieg der Militarisierung mit Künstlicher Intelligenz* mit dem Vortrag: *Für ein NEIN der Wissenschaft zu Killerdrohnen und autonomen Waffen.*

Hans-Jörg Kreowski und Wolfgang Krieger veröffentlichen einen Beitrag zur **Künstlichen Intelligenz**: *Künstliche Intelligenz – „künstlich“ ja, „Intelligenz“ wohl kaum* in dem von Anna Strasser, Wolfgang Sohst, Ralf Stapelfeld und Katja Stepec herausgegebenen Sammelband *Künstliche Intelligenz – Die große Verheißung.*

Das FIF unterstützt das Bündnis **Reclaim Your Face** bei der offiziellen **Europäischen Bürgerinitiative** (EBI) zum **Verbot biometrischer Massenüberwachung**. Mehr als 40 europäische Organisationen rufen ebenfalls dazu auf: Während die Europäische Kommission neue Gesetze zur Regulierung Künstlicher Intelligenz (KI) vorbereitet, warnt das Bündnis von Digital- und Menschenrechtsorganisationen vor den Gefahren von biometrischer Massenüberwachung für die Freiheit und Würde der Bürger:innen. Mit der Europäischen Bürgerinitiative (EBI) fordern Europäische Bürger:innen neue gesetzliche Rahmenbedingungen einschließlich eines Verbots von biometrischer Massenüberwachung.

Das FIF kritisiert den staatlich organisierten Hackathon **#UpdateDeutschland** und den Umgang Deutschlands mit der Zivilgesellschaft und der Digitalisierung – #UpdateDeutschland schafft keine nachhaltigen Lösungen für die Verwaltung:

*In 48 Stunden mit digitalen Tools die Welt retten? Die aktuellen Hackathons unter der Schirmherrschaft des Bundeskanzleramts suchen nach digitalen Innovationen, um eine Vielzahl gesellschaftlicher Probleme anzugehen. Doch dieser Ansatz kann nicht funktionieren, denn entweder sind die Probleme („Einsamkeit“, „soziale Ungleichheit“) überhaupt nicht sinnvoll mit Software lösbar oder aber die Lösungen können erfahrungsgemäß wegen kaputtgesparter Verwaltungen nicht langfristig in staatliche Strukturen eingebunden werden. Hier braucht es politisches Handeln, keine neuen Apps.*

Das FIF schließt sich der Kampagne **Heimatland Erde** – für planetares Denken und Fühlen, Planen und Handeln an. Aus dem Aufruf zur Kampagne:

*Wir müssen unsere heutige Lebens- und Produktionsweise ersetzen durch ein System, das das gesamte Ökosystem des Planeten nicht mehr bekämpft, sondern sich sinnvoll darin einfügt. Wir müssen die Biosphäre in ei-*

*nem funktionsfähigen Zustand erhalten, um unser eigenes Leben zu sichern.*

## Mai 2021

In der FIF-Kampagne zum **TRIPS-Waiver** der Regionalgruppe Berlin fordern wir Bundesregierung und EU-Kommission auf, nicht weiter die weltweite Bekämpfung der Corona-Pandemie zu blockieren, und veröffentlichen dazu eine detaillierte FAQ:

*Durch die Blockadehaltung von Bundesregierung und EU-Kommission wird der TRIPS-Waiver gefährdet. Die darin geforderte temporäre Freigabe der Corona-Impfstoffpatente ist ein essentieller Schritt für eine effektive globale und langfristige Bekämpfung der Pandemie. Es ist höchste Zeit, dass alle Regierungen der EU die Zeichen der Zeit erkennen und sich für den Antrag aussprechen.*

Das FIF gibt gemeinsam mit dem Chaos Computer Club eine Stellungnahme zum **Elektronischen Identitätsnachweis mit mobilem Endgerät** ab, die von Rainer Rehak in der Anhörung des Deutschen Bundestags vorgestellt wird:

*Hier zeigen sich trotz diverser IT-Sicherheitsgesetze erneut die allgemeinen Versäumnisse der deutschen Digitalpolitik: Sozio-ökonomische Ungleichheiten in der Gesellschaft werden weiter zementiert. Sichere und erschwingliche Endgeräte sind weder aktuell noch in naher Zukunft für die breite Bevölkerung vorhanden, weil Mindeststandards fehlen und politisch-wirtschaftliche Verantwortlichkeiten nicht gesetzt werden. Letztlich entscheidet dann der Geldbeutel der Nutzenden, und die Früchte der Digitalisierung bleiben bei den ohnehin Privilegierten. Unter diesen Versäumnissen leiden natürlich alle Digitalisierungsvorhaben.*

Der **Grundrechte-Report 2021**, mit herausgegeben vom FIF, erscheint. Darin ist ein Beitrag von Stefan Hügel zur **Vorratsdatenspeicherung** enthalten: *„Und täglich grüßt das Murmeltier“*. Die andauernde Debatte um die Vorratsdatenspeicherung, oder: Politik gegen die Grundrechte (auch bei netzpolitik.org veröffentlicht). Das FIF unterstützt beim Streaming der Pressekonferenz zur Veröffentlichung.

## Juni 2021

Das FIF ist Teil des Bündnisses **Wer hat der gibt** und fordert zusammen mit mehr als 100 zivilgesellschaftlichen Organisationen und Intellektuellen aus Wissenschaft, Kunst und Kultur eine gerechte Verteilung der Corona-Kosten.

FIF ist Mitorganisatorin der Demo **Gesundheit für alle – #Gebt-DiePatenteFrei!** mit Redebeitrag der Regionalgruppe Berlin.

## Juli 2021

Die Regionalgruppe Berlin des FIF beteiligt sich mit der **Do-Sport-For-Assange-Aktion** an der Mahnwache zu **Julian Assanges** Geburtstag.

Elisa Lindinger und Rainer Rehak organisieren eine Diskussion für den *Netzpolitischen Abend* der Digitalen Gesellschaft zur **Corona-Warn-App**: Dezentrales Contact-Tracing mit Apple und Google?

Beitrag von Hans-Jörg Kreowski: **Cyberpeace: Für Frieden, Freiheit und eine lebenswerte Welt** zur Kampagne Heimatland Erde bei der *Online ClimateSchool*, Students for Future.

## August 2021

Zwei Redebeiträge der FifF-Regionalgruppe Berlin durch Rainer Rehak und Paula P. auf der **Geradedenken-Demo** gegen Corona-Querdenkerei und -Schwurblerei.

## September 2021

Das FifF ist Bündnispartner der **#unteilbar**-Demo in Berlin für eine gerechte und solidarische Gesellschaft.

Für das FifF gibt Daniel Guagnin eine Stellungnahme zur **Cybersicherheitsstrategie 2021** der Bundesregierung ab.

Wolfgang Hofkirchner und Hans-Jörg Kreowski organisieren einen Workshop zum Thema **Digital Humanism – How to shape digitalisation in the age of global challenges?** für den Arbeitskreis Emergente Systeme, Information und Gesellschaft der Leibniz-Sozietät der Wissenschaften und des FifF im Rahmen des IS4SI-Summit. Vortrag von Hans-Jörg Kreowski: **A world worth living – Can Artificial Intelligence help to reach the goal?**

## Oktober 2021

Rainer Rehak hält einen Vortrag auf der Klausurtagung **Die irreführende Sprache der KI-Debatte**.

Hans-Jörg Kreowski hält einen Vortrag **Das Schlachtfeld der Zukunft – Die strategische Bedeutung von Cyberwaffen für das Militär** bei einer Veranstaltung des Bochumer Friedensplenums und der DFG-VK.

## November 2021

Am 12.-14.11.2021 findet in München und online unsere **FifF-Konferenz 2021** statt, mit dem Leitmotiv **Selbstbestimmung in digitalen Räumen**:

*Unsere elektronischen Geräte sehen wir öfter und länger als Freunde oder Familie. Sie sind wichtige Arbeitsmittel und bequeme, allzeit bereite Helfer im Alltag, ohne sie ginge gar nichts mehr. Das wirft Fragen auf: Nach der Technik – wie funktioniert das? Nach gesellschaftlichen Folgen – welche sind das? Geht es auch anders?*

*Informationstechnik verändert rasant, wie wir kommunizieren, denken, uns bewegen und handeln. Sie dringt in persönliche und zwischenmenschliche Bereiche vor*

*und beeinflusst unser Verhalten, ohne dass wir uns dessen immer bewusst sind. Wo wir uns als handelnde Subjekte sehen, werden wir oft als Objekte vermessen, bewertet und behandelt. Auf Plattformen und in sozialen Netzen, in smarten Infrastrukturen und in Scoring-Systemen wirken höchst profitable Geschäftsmodelle, die wir kaum durchschauen, geschweige denn (selbst) bestimmen können.*

Im Rahmen der FifF-Konferenz verleihen wir die **Weizenbaum-Medaille** an Christiane Floyd. Die Laudatio hält Britta Schinzel. Aus unserer Pressemitteilung:

*Die diesjährige Preisträgerin Christiane Floyd hat ihr Fach Softwaretechnik in Forschung und Lehre einzigartig geprägt. Mit ihren Forderungen nach Partizipation von Nutzenden und Betroffenen bei der Systementwicklung sowie nach Berücksichtigung sozialer und ethischer Anforderungen hat sie die Softwaretechnik maßgeblich beeinflusst und unter Einbeziehung sozialwissenschaftlicher, ethischer und philosophischer Gesichtspunkte beispielhaft ausgestaltet. Britta Schinzel: „Christiane Floyd hat ihr Fach im Sinne einer gesellschaftlichen Verantwortung für die Informatik aufgefasst, gestaltet und gelebt – eine außergewöhnliche Persönlichkeit und ein großes Vorbild.“*

Im Rahmen der Konferenz verleihen wir wieder den **Weizenbaum-Studienpreis** an:

- **Hendrik Heuer** für seine Arbeit *Users & Machine-Learning-Based Curation Systems*,
- **Helene Hahn** für ihre Arbeit *Digital identification systems and the right to privacy in the asylum context: An analysis of implementations in Germany*,
- **Silke Meiser** für ihre Arbeit *Trust me! Vorschlag zum Umgang mit der Vertrauensfrage im digitalen Zeitalter*,
- **Martin Schmitt** für seine Arbeit *Die Digitalisierung der Kreditwirtschaft. Computereinsatz in den Sparkassen der Bundesrepublik und der DDR, 1957-1991*.

Publikation von Hans-Jörg Kreowski und Aaron Lye (Hg.): **Künstliche Intelligenz zieht in den Krieg**, W&F-Dossier 93.

Vortrag von Aaron Lye: **NATO-Manöver im Cyberraum** beim IMI-Kongress in Tübingen.

## Dezember 2021

Das FifF veröffentlicht seine **Broschüre**, in der wir die Geschichte, die Grundsätze, die Arbeit und die Organisation des FifF darstellen, um Menschen für unsere Arbeit zu interessieren und zum Mitmachen zu motivieren.

Die FifF-Regionalgruppe Bremen und *Students for Future Bremen* laden zu einer Vortragsveranstaltung ein: **Leben in der Klimakrise**. Referent:innen sind Marie-Luise Abshagen, Nelly Grotefeldt und Bernhard Stoevesandt.



Im FIF 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 FIF 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 FIF-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 FIF regelmäßig an weiteren Veranstaltungen, Publikationen, vermittelt bei Presse- oder Vortragsanfragen ExpertInnen, führt Studien durch und gibt Stellungnahmen ab etc. Das FIF kooperiert mit zahlreichen Initiativen und Organisationen im In- und Ausland.

## FIF-Mailinglisten

### FIF-Mailingliste

An- und Abmeldungen an:

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

Beiträge an: [fiff-L@lists.fiff.de](mailto:fiff-L@lists.fiff.de)

### FIF-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](mailto:cctv-L@lists.fiff.de)

## FIF online

### Das ganze FIF

[www.fiff.de](http://www.fiff.de)

Twitter FIF e.V. – @Fiff\_de

### Cyberpeace

[cyberpeace.fiff.de](http://cyberpeace.fiff.de)

Twitter Cyberpeace – @Fiff\_AK\_RUIN

### Faire Computer

[blog.faire-computer.de](http://blog.faire-computer.de)

Twitter Faire Computer – @FaireComputer

### Mitglieder-Wiki

<https://wiki.fiff.de>

## FIF-Beirat

**Ute Bernhardt** (Berlin); **Peter Bittner** (Bad Homburg); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Wolfgang Coy** (Berlin); Prof. Dr. **Wolfgang Däubler** (Bremen); Prof. Dr. **Christiane Floyd** (Berlin); Prof. Dr. **Klaus Fuchs-Kittowski** (Berlin); Prof. Dr. **Michael Grütz** (München); Prof. Dr. **Thomas Herrmann** (Bochum); Prof. Dr. **Wolfgang Hesse** (München); Prof. Dr. **Wolfgang Hofkirchner** (Wien); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (München); **Ulrich Klotz** (Frankfurt am Main); Prof. Dr. **Klaus Köhler** (Mannheim); Prof. Dr. **Jochen Koubek** (Bayreuth); Dr. **Constanze Kurz** (Berlin); Prof. Dr. **Klaus-Peter Löhr** (Berlin); Prof. Dr. **Dietrich Meyer-Ebrecht** (Aachen); **Werner Mühlmann** (Calau); Prof. Dr. **Frieder Nake** (Bremen); Prof. Dr. **Rolf Oberliesen** (Paderborn); 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** (Mainz); Prof. Dr. **Eberhard Zehendner** (Jena)

## FIF-Vorstand

**Stefan Hügel** (Vorsitzender) – Frankfurt am Main  
**Rainer Rehak** (stellv. Vorsitzender) – Berlin  
**Michael Ahlmann** – Kiel / Blumenthal  
**Maximilian Hagner** – Jena  
**Alexander Heim** – Berlin  
**Sylvia Johnigk** – München  
**Benjamin Kees** – Berlin  
Prof. Dr. **Hans-Jörg Kreowski** – Bremen  
**Kai Nothdurft** – München  
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau  
**Ingrid Schlagheck** – Bremen  
**Anne Schnerrer** – Berlin  
Dr. **Friedrich Strauß** – München  
Prof. Dr. **Werner Winzerling** – Fulda

## FIF-Geschäftsstelle

**Ingrid Schlagheck** (Geschäftsführung) – Bremen  
**Philip Love** – Bremen

## Impressum

<b>Herausgeber</b>	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
<b>Verlagsadresse</b>	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 <a href="mailto:fiff@fiff.de">fiff@fiff.de</a>
<b>Erscheinungsweise</b>	vierteljährlich
<b>Erscheinungsort</b>	Bremen
<b>ISSN</b>	0938-3476
<b>Auflage</b>	1 300 Stück
<b>Heftpreis</b>	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.
<b>Hauptredaktion</b>	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck
<b>Schwerpunktredaktion</b>	Dagmar Boedicker
<b>V.i.S.d.P.</b>	Stefan Hügel
<b>Retrospektive</b>	Beiträge für diese Rubrik bitte per E-Mail an <a href="mailto:redaktion@fiff.de">redaktion@fiff.de</a>
<b>Lesen, SchlussFIfF</b>	Beiträge für diese Rubriken bitte per E-Mail an <a href="mailto:redaktion@fiff.de">redaktion@fiff.de</a>
<b>Layout</b>	Berthold Schroeder, München
<b>Cover</b>	Foto: Reinald Kirchner, <a href="https://www.flickr.com/photos/rkirchne/3538957268">https://www.flickr.com/photos/rkirchne/3538957268</a> , CC BY-SA 4.0 Tagungslogo, Benjamin Kees
<b>Druck</b>	Meiners Druck, Bremen Heftinhalt auf 100 % Altpapier gedruckt.



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 Abonnent:innen, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

## Aktuelle Ankündigungen

(mehr Termine unter [www.fiff.de](http://www.fiff.de))

### FIfF-Kommunikation

2/2022 Künstliche Intelligenz, Automatisierung und Ethik  
Hans-Jörg Kreowski, Stefan Hügel  
Redaktionsschluss: 6. Mai 2022

3/2022 Politik, Staat und Verwaltung  
Jörg Pohle, Stefan Hügel  
Redaktionsschluss: 5. August 2022

4/2022 100 Jahre Joseph Weizenbaum  
Stefan Ullrich, Andrea Knaut  
Redaktionsschluss: 4. November 2022

### Zuletzt erschienen:

- 4/2020 Digitalisierung in der Bildung
- 1/2021 FIfFKon 2020 – Datenschutz, Usability, Barrierefreiheit und Sicherheit – Teil 1
- 2+3/2021 FIfFKon 2020 Teil 2
- 4/2021 Künstliche Intelligenz zieht in den Krieg

### W&F – Wissenschaft & Frieden

- 3/21 Frieden lernen, aber wie? – Aktuelle Fragen der Friedenspädagogik
- 4/21 Chinas Welt? – Zwischen Konflikt und Kooperation
- 1/22 Täter:innen

### vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

- #230 30 Jahre Deutsch-Deutsche Wiedervereinigung
- #231/232 Zwei Jahre Datenschutz-Grundverordnung
- #233 Kirchliches Sonderarbeitsrecht
- #234 Strafvollzug in der Pandemie

### DANA – Datenschutz-Nachrichten

- 2/21 Bildung
- 3/21 E-Government
- 4/21 Datenschutz-Visionen

## Das FIfF-Büro

### Geschäftsstelle FIfF e. V.

Ingrid Schlagheck (Geschäftsführung)  
Philip Love  
Goetheplatz 4, D-28203 Bremen  
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56  
E-Mail: [fiff@fiff.de](mailto:fiff@fiff.de)  
Die Bürozeiten finden Sie unter [www.fiff.de](http://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](mailto:redaktion@fiff.de)

Schluss *E..I..f..F..*

**„Die weißen Tauben sind müde ...**



**... sie fliegen lange schon nicht mehr“**

Geeignete Texte für den SchlussFliff bitte mit Quellenangabe an [redaktion@fiff.de](mailto:redaktion@fiff.de) senden.