Nutzungshinweise

H 7625

FIfF-Kommunikation

Zeitschrift für Informatik und Gesellschaft

42. Jahrgang 2025 Einzelpreis: 7 EUR 2/2025 – Juni 2025

Informatik und Gesellschaft

ISSN 0938-3476

• Denkende Maschinen • Desinformation • Fediverse • Zivilklausel •

FIfF-Kommunikation

Zeitschrift für Informatik und Gesellschaft

Titelbild: Impression von der FIfF-Konferenz 2022
FIfFKon22 CC BY XPulse

Inhalt

Ausgabe 2/2025

Editorial

Eine bunte Mischung von Beiträgen aus dem Themenfeld *Informatik und Gesellschaft* enthält diese Ausgabe der *FIfF-Kommunikation*. Dabei decken wir Bereiche wie IT-Sicherheit, Friedenspolitik, Künstliche Intelligenz und Öffentlichkeit ab.

Den Anfang macht *Maja Warlich* mit ihrem Beitrag zu der Spyware *FinFisher*. Sie untersucht die technischen Details und Produktmerkmale bis hin zu den Auswirkungen auf die Menschen- und Bürgerrechte. Sie stellt fest, dass die Möglichkeiten der Software, in private Bereiche einzudringen, mit grundlegenden Prinzipien der Menschenrechte im Widerspruch stehen.

Die beiden folgenden Beiträge widmen sich der Künstlichen Intelligenz. *Maurice Haugk* weist auf die Bedeutung des *AI Act* der Europäischen Union hin und geht auf Chancen und Risiken der KI ein. *Hans-Jörg Kreowski* geht der Frage nach, ob die Entwicklung der Künstlichen Intelligenz zu denkenden Maschinen, also zu einer Künstlichen Allgemeinen Intelligenz führen wird. Er stellt dazu natürliches Denken dem maschinellen Denken gegenüber. Nach allgemeinem Verständnis gilt bei maschinellem Denken die Church-Turing-These, nach der kein Computer hergestellt werden kann, dessen theoretische Rechenfähigkeiten die der heute bereits existierenden Computer übersteigen. Die Existenz eines superintelligenten Computers würde die Church-Turing-These widerlegen. Es sei unwahrscheinlich, dass er gebaut werden kann, die Möglichkeit aber nicht völlig auszuschließen.

Unter dem Pseudonym *three monkeys awoken* wird in einem sehr pointierten Manifest die menschgemachte Produktivkraftentwicklung im Zeitalter Künstlicher Intelligenz untersucht. Genannt werden vier Mindestbedingungen zur Verwirklichung einer menschlichen Zukunft: radikale Transformation der Produktionsverhältnisse, globale Kooperation und gerechte Verteilung, gesellschaftliche Kontrolle der Technologien und Ethik und Sicherheit in der KI-Entwicklung. Es wird dazu aufgerufen, die planetare Zerstörung, Kriegshetze, Verhetzung und Verrohung aufzuhalten und eine gemeinsame gute Zukunft für die Menschheit aufzubauen.

Nicht erst seit den jüngsten Ereignissen in Israel und Gaza steht die Bekämpfung des Antisemitismus in Deutschland ganz oben auf der Tagesordnung. *Marie-Theres Tinnefeld* behandelt in ihrem Beitrag die *Streitfrage Antisemitismus und Wege des Friedens*. Klar ist: Jeder Diskriminierung von Jüdinnen und Juden ist eine eindeutige Absage zu erteilen. Doch mit Omri Boehm fragt sie auch: „Soll, muss nicht etwa auch in der Palästinenserfrage ‚das Ideal des Friedens der Ursprung menschlicher Beziehungen, menschlicher Politik und menschlichen Rechts' sein?"

Die seit einiger Zeit breit geführte Debatte über Desinformation auf Social Media gehe am Kern des Problems vorbei, sagt die Politikwissenschaftlerin *Jeanette Hofmann* im Interview, das wir mit freundlicher Genehmigung vom Weizenbaum-Institut übernommen haben. „Obwohl sie sicher zur Desinformation beitragen, sind also nicht die Plattformen die wirkliche Gefahr, sondern es sind häufig Regierungsparteien oder wichtige Oppositionsparteien, die einflussreiche Produzierende von Desinformationen sind." Auch die klassischen Massenmedien tragen zur Desinformation bei: „Studien zeigen, dass Desinformationen erst durch die Massenmedien in die Breite getragen werden, weil sie nach wie vor ein Publikum erreichen, dass weit über das der sozialen Medien hinausgeht." Desinformation sei ein Symptom des Demokratieverfalls, zu dem alle politischen Kräfte beitragen, wenn sie auf die Beeinflussung oder Manipulation ihrer Wähler:innen zielen – auch mit gezielten Falschinformationen. „In diesem Sinne müssen sich die Qualitätsmedien fragen, welchen Beitrag sie in der Bekämpfung von Desinformation spielen wollen. Ist es tatsächlich sinnvoll, über jedes Stöckchen zu springen, das ihnen populistische Politiker:innen hinhalten?" Mit politischer Kommunikation in Sozialen Medien und ihren Konsequenzen befasst sich auch das Interview mit *Natascha Strobl* aus *netzpolitik.org* in unserer gleichnamigen Rubrik.

„Die Social-Media-Landschaft befindet sich in einem tektonischen Umbruch, seit Elon Musk Twitter übernahm und Donald Trump die USA", leitet *Volker Grassmuck* seinen Beitrag zur Governance in offenen Gemeinschaften ein. Das Fediverse sei ein Gegenmittel gegen die Macht populistischer Politiker:innen in Verbindung mit der zentralisierten Nutzung von Medien: „… lokale, überschaubare Gemeinschaften bilden die Grundlage, spannen untereinander diplomatische Netze und wachsen organisch zu einem Fediverse, das mehr ist, als die Summe seiner Teile. *Small is Beautiful* als Voraussetzung für *Bigger is Better*."

Mit den Herausforderungen von Rücküberweisungen durch Migrant:innen befasst sich *Alexandra Keiner* in ihrem Beitrag. Rücküberweisungen sind kostspielig und werden häufig als „verdächtige" Transaktionen eingestuft. „Um Rücküberweisungen einfacher und günstiger zu gestalten, müssen sie als politische und soziale Prozesse verstanden werden, die nicht einfach mit digitalen Technologien gelöst werden können. … Darüber hinaus müssen Migration und Rücküberweisungen als langfristige Phänomene betrachtet, entkriminalisiert und entstigmatisiert werden."

Von einer erfreulichen Entwicklung berichtet *Christian Heck* aus Köln in seinem Beitrag *Zivilklausel@KHM*: „Während an vielen Universitäten und Hochschulen Zivilklauseln infrage gestellt werden, hat der Senat der Kunsthochschule für Medien Köln (KHM) am 19. Dezember 2024 den Beschluss gefasst, diese in der Grundordnung zu verankern." Wir gratulieren den Kolleg:innen herzlich zu diesem Erfolg.

Auch diese Ausgabe enthält ausgewählte Beiträge aus *netzpolitik.org*. Neben dem bereits genannten Interview ist dies unter anderem ein Beitrag zur kürzlich durch das BMI eher verstohlen veröffentlichten Überwachungsgesamtrechnung – ein Thema, dem die *FIfF-Kommunikation* bereits in der Ausgabe 4/2019 einen Schwerpunkt gewidmet hatte.

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

Stefan Hügel
für die Redaktion

Gute Zusammenarbeit: Trump und die Medien

Liebe Freundinnen und Freunde des FIfF, liebe Mitglieder,

es ist nun bald ein halbes Jahr her, dass Donald Trump wieder das Weiße Haus übernommen hat – manchen erscheint es schon viel länger – und wir verfolgen teilweise fassungslos in den Medien seine täglichen Äußerungen, Ankündigungen und Drohungen. Häufig sind dies Ankündigungen, die nur wenig später bedeutungslos sind, wieder zurückgenommen werden, teilweise rechtswidrig sind, immer aber sofort zu großer Aufregung führen. Manchmal muss man bei einem anerkannten Nachrichtenportal wie *Spiegel Online* weit nach unten scrollen, um auf andere Nachrichten zu stoßen, die mindestens ebenso bedeutend sind. Es gibt ohne Zweifel genug davon: Regierungswechsel in Deutschland, andauernder Konflikt im Nahen Osten mit vielen zivilen Opfern, Krieg in der Ukraine, … Doch wichtiger scheint immer wieder die neueste Ankündigung von Donald Trump, die er mit einiger Wahrscheinlichkeit am nächsten Tag revidiert. Aktuell sind es die Proteste in Los Angeles, die die US-Regierung, Berichten zufolge, anscheinend gezielt in die Eskalation treibt, einschließlich des Militäreinsatzes gegen die eigene Bevölkerung. Bei Erscheinen dieser Ausgabe der *FIfF-Kommunikation* wird es schon längst etwas ganz anderes sein.

„Flood the zone with shit", so beschreibt der rechtsextreme Publizist Steve Bannon das Prinzip[1]. Doch ich habe zunehmend den Eindruck, dass auch die als seriös wahrgenommenen Medien einen erheblichen Anteil an der Entwicklung haben. Müssen sie jede Scheiße gleich unbesehen weiterpumpen? Aufgabe der Medien ist es, Informationen einzuordnen, zu bewerten, wirklich Wichtiges von Unwichtigem zu unterscheiden und manchmal Nachrichten eben auch nicht zu bringen. Stattdessen wird ebenso aufgeregt wie eilfertig jede neue (Nicht-) Nachricht zugespitzt, aufgebauscht und verbreitet.

Nur ein Beispiel: Während der Wahl des neuen Papstes veröffentlichte das Weiße Haus ein KI-generiertes Bild von Trump als Papst. Klar, superlustig, müssen wir sofort bringen. Dann folgt große Empörung! In einzelnen Medien[2] wird sogleich ernsthaft die Frage diskutiert, ob Donald Trump wirklich Papst werden kann (Spoiler: Nein, kann er nicht). Und schon wieder haben wir unsere Nachrichtenseiten gefüllt, ohne uns mit unappetitlichen Fragen wie der rechtswidrigen Abschiebung von Migrant:innen oder der Zerstörung amerikanischer Universitäten und ihren realen Konsequenzen einmal ernsthaft auseinandersetzen zu müssen. Und wenn doch, werden die offiziellen Statements häufig unkritisch übernommen. Der offenbar gerade (bei Erscheinen dieses Textes noch immer?) in Ungnade gefallene Elon Musk hat(te) mit seinem sogenannten *Department of Government Efficiency* (DOGE) offensichtlich die Aufgabe, als „Einsparungen" bemäntelt, die politischen Ziele der US-Regierung durchzusetzen. Das hindert Nachrichtenportale wie *Spiegel Online* nicht daran, DOGE immer noch naiv als „Kostensenkungstruppe" zu bezeichnen.

Doch Trumps Kommunikationsstrategie scheint zu wirken. Schon vor dem Start der neuen Regierungskoalition, nachdem Trump gemeinsam mit seinem Vizepräsidenten Vance den ukrainischen Präsidenten im Weißen Haus sehr undiplomatisch abgefertigt hatte, vermittelten Union und SPD den Eindruck, sie wollten als Rüstungskoalition in die bundesrepublikanische Geschichte eingehen. Eine eilige Verfassungsänderung schon vor der Übernahme der Regierungsverantwortung mit (wenn auch formal legalen) Verfahrenstricks zur Aufhebung jeglicher Begrenzung der Rüstungsausgaben, eine erneute Wehrpflichtdebatte und die Orientierung an der Forderung von US-Präsident Donald Trump, fünf Prozent des BIP – das entspricht ungefähr der Hälfte des Bundeshaushalts – für Verteidigung und Rüstung auszugeben, sind wesentliche Eckpunkte der Außen- und Sicherheitspolitik der ersten Wochen. Nachdem sich mehrere Bundesregierungen seit Jahren dagegen stellen, auch „nur" die zuvor geforderten zwei Prozent des BIP (ca. 15-20 % des Bundeshaushalts) bereitzustellen, geht Trumps Strategie, sie mit seinen umgehend von den Medien verbreiteten Statements zu erpressen, offenbar binnen Stunden auf.

Dies wird dann zusätzlich medial flankiert durch die Drohkulisse, bis 2029 sei mit einem Angriff Russlands auf die NATO oder gar Deutschland zu rechnen, gegen den wir uns verteidigen müssen – eine Drohkulisse, die anscheinend wieder ebenso von vielen Medien, weitgehend ungeprüft, übernommen wird. Immerhin: In einem Beitrag der Wochenzeitung *Die Zeit*[3] wird der aktuelle Kriegsalarmismus kritisch eingeordnet, indem selbst Carlo Masala, Professor für Internationale Politik an der Universität der Bundeswehr in München und bekannt aus vielen Talk-Shows als Verfechter verstärkter Verteidigungsanstrengungen, zitiert wird: „[D]ie Zahl 2029 [wird] von Politikern strategisch genutzt. Sie müssen sagen, dass Russland 2029 einen Krieg führen könnte, um die Menschen auf höhere Verteidigungsmaßnahmen einzustimmen."

Lassen sich Ausgaben für die Bundeswehr, um ihre Einsatzbereitschaft zu sichern, vielleicht noch begründen – ich persönlich ziehe weniger militaristische Lösungen vor, was aber in der Konsequenz sicherlich nicht zur Wehrlosigkeit führen darf –, macht der Trend zur Militarisierung der Gesellschaft[4], wie sie im Koalitionsvertrag[5] als Ziel gesetzt wird, erhebliche Sorgen: „Wir verankern unsere Bundeswehr noch stärker im öffentlichen Leben und setzen uns für die Stärkung der Rolle der Jugendoffiziere ein, die an den Schulen einen wichtigen Bildungsauftrag erfüllen." Offenbar sollen bereits unsere Kinder wieder zur „Kriegstüchtigkeit" erzogen werden. Dann sind sie bereit für den „neuen attraktiven Wehrdienst", der „zunächst" auf Freiwilligkeit basieren soll. „Wertschätzung durch anspruchsvollen Dienst, verbunden mit Qualifikationsmöglichkeiten, werden die Bereitschaft zum Wehrdienst dauerhaft steigern", so glauben die Koalitionäre. Aber für alle Fälle wird zwischen den Zeilen deutlich gemacht: „Wir können auch anders." Größer wird das Reservoir an verfügbaren Kapazitäten, indem der Anteil von Frauen und Menschen mit Migrationsgeschichte bei der Bundeswehr erhöht

wird. Ein vergifteter Beitrag zur Abbildung der gesellschaftlichen Vielfalt beim Militär. Migranten sollen bitteschön erst einmal „dienen", bevor sie hier bleiben dürfen – werden wir das demnächst dann von der AfD hören?

Und auch die an vielen Hochschulen geltenden Zivilklauseln, das heißt der Verzicht auf militärische Forschung, werden unter der christlich-sozialdemokratischen Koalition unter Druck[6] geraten: „Wir setzen uns dafür ein, dass Hemmnisse, die beispielsweise Dual-Use-Forschung oder auch zivil-militärische Forschungskooperationen erschweren, abgebaut werden." Zudem soll der Weltraum verstärkt für das deutsche Militär erschlossen werden.

Auch im Inneren zeichnet sich eine „Zeitenwende" ab. Sie beginnt für die Koalition mit einem alten Hut: erweiterten Überwachungsbefugnissen für die Sicherheitsbehörden. Als Erstes ist die seit 2010 in mehreren Varianten von höchsten deutschen und europäischen Gerichten immer wieder verworfene anlasslose Vorratsdatenspeicherung zu nennen, die nun reaktiviert werden soll. Ergänzt wird dies durch die Quellen-TKÜ, die kleine Schwester der Online-Durchsuchung und technisch kaum von dieser abzugrenzen. Dazu kommen automatisierte Datenrecherche und -analyse, biometrischer Abgleich mit öffentlich zugänglichen Internetdaten unter Nutzung von KI-Verfahren und die automatisierte Aufzeichnung von Kraftfahrzeug-Kennzeichen, selbstredend unter „Berücksichtigung verfassungsrechtlicher Vorgaben". Besonders fragwürdig sind Überlegungen, die Überwachungssoftware *Palantir* des US-amerikanischen Antidemokraten Peter Thiel einzusetzen und ihm damit Daten der deutschen Bevölkerung frei Haus zu liefern[7]. Wo ist eigentlich der Verfassungsschutz, wenn man ihn ausnahmsweise mal braucht?

Dass sich auch sonst die Bundesregierung vor allem auf repressive Maßnahmen – Bekämpfung, Verfolgung und Überwachung – für die Sicherheit vor Kriminalität und politischem Extremismus verständigen kann, ist sehr bedauerlich. Zweifellos müssen wir Feinde der Demokratie (mit demokratischen Mitteln) bekämpfen, vor allem sollte sie aber gestärkt, ihre Werte positiv vermittelt und die demokratische Gesellschaft in ihrer ganzen Vielfalt gefördert werden. Nicht zuletzt schafft die Regierungskoalition mit ihren Plänen ein Instrumentarium, das rechtsextremistische Parteien, sollten sie einmal an die Macht kommen, begierig aufgreifen und letztlich gegen die dann noch bestehenden Reste der Demokratie wenden werden.

Die Militärpolitik der kommenden vier Jahre wird wohl durch massive Aufrüstung und eine Militarisierung der Gesellschaft, Wissenschaft und Erziehung gekennzeichnet sein. Ob dies den richtigen Weg weist zu dem einleitend im Kapitel des Vertrags zur Außen- und Verteidigungspolitik genannten Ziel – die „Bewahrung eines Friedens in Freiheit und Sicherheit" – oder ob es ein Abstieg in eine neue Rüstungsspirale mit wachsender Kriegsgefahr wird, wird sich zeigen. Angesichts unserer historischen Erfahrungen ist wohl große Skepsis angebracht. Aber letztlich hängt unsere Existenz davon ab, dass die politischen Entscheidungen so getroffen werden, dass der Krieg in der Ukraine beendet und die Gefahr einer Ausweitung des Krieges in das Zentrum Europas abgewendet und nicht im Gegenteil noch provoziert wird. Vergleichbares gilt für die Innenpolitik, bei der echte Demokratie bewahrt und gegen Angriffe des Rechtsextremismus und gegen ein Abgleiten in einen Überwachungsstaat verteidigt werden muss.

Mit FIfFigen Grüßen
Stefan Hügel

Anmerkungen

1 *Deutschlandfunk (2025) „Flood the zone" – Warum Trumps Flut an Dekreten und Provokationen Methode hat, https://www.deutschlandfunk.de/flood-the-zone-warum-trumps-flut-an-dekreten-und-provokationen-methode-hat-100.html*
2 *n-tv (2025) Trump zum Konklave: „Ich würde gerne Papst werden", https://www.n-tv.de/politik/Trump-zum-Konklave-Ich-wuerde-gerne-Papst-werden-article25736276.html*
3 *Joeres A, Kireev M (2025) Der Russe kommt. Vielleicht, in: Die Zeit Nr. 21, https://www.zeit.de/2025/21/carlo-masala-russland-angriff-europa-nato-aufruestung.*
4 *Zuckmayer C (1931) Der Hauptmann von Köpenick: Ein deutsches Märchen in drei Akten. Frankfurt am Main: Fischer*
5 *CDU, CSU, SPD (2025) Verantwortung für Deutschland, https://www.koalitionsvertrag2025.de*
6 *Obwohl wir in dieser Ausgabe der FIfF-Kommunikation einen Erfolg an der Kölner Hochschule für Medien (KHM) vermelden können (Seite 36).*
7 *Joswig G (2025) Dobrindt schließt Palantir-Nutzung nicht aus, taz.de, https://taz.de/Gruene-kritisieren-Ueberwachungssoftware/!6093377/*

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. Dazu gehören unsere jährlich stattfindende FIfF-Konferenz, der Weizenbaum-Preis, weitere Publikationen und die 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

Digitaler Humanismus
für eine techno-öko-soziale Transformation der Weltgesellschaft

21.-23. November 2025 | Kulturzentrum 4lthangrund für Alle | Wien

Die Konferenz des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) wird heuer auf Einladung von The Institute for a Global Sustainable Information Society (GSIS) vom 21. bis zum 23. November 2025 nach Wien einberufen (https://4lthangrund.jetzt).

Wien zeichnet sich als Hub des Digitalen Humanismus aus. Darunter versteht sich humane Digitalisierung, eine philosophisch fundierte Technikgestaltung in Zeiten, in denen, getrieben von den Profitinteressen der Konzerne – wie sich im Hype um die KI zeigt –, Grenzen zwischen dem Humanen und dem Künstlichen zu verschwimmen scheinen. 2018 haben Julian Nida-Rümelin und Natalie Weidenfeld mit ihrem wegweisenden Buch den Begriff *Digitaler Humanismus* geprägt. 2019 ist an der Informatik der Technischen Universität (TU) Wien das *Vienna Manifesto on Digital Humanism* verabschiedet und *The Digital Humanism Initiative* begründet worden. Peter Knees und Julia Neidhardt teilen sich an der TU Wien seit 2023 The UNESCO Chair on Digital Humanism. Die Stadt Wien und Wiener Fonds unterstützen internationale Projekte auf diesem Gebiet (*https://informatics.tuwien.ac.at/digital-humanism/*).

Das in Wien angesiedelte unabhängige Forschungsinstitut GSIS greift den Digitalen Humanismus auf und stellt ihn in den Zusammenhang der Polykrise, in der die existenziellen Bedrohungen der Menschheit einander gegenseitig verstärken. Um das Überleben und ein gutes Leben für alle Mitglieder der Weltgesellschaft gewährleisten zu können, ist eine abgestimmte Transformation der gesellschaftlichen Verhältnisse, der gesellschaftlichen Naturverhältnisse, aber auch der gesellschaftlichen Technikverhältnisse notwendig. Digitaler Humanismus ist hier hilfreich. Aber er muss auch nachgeschärft werden, was seine Aufgaben in dieser Transformation betrifft (*https://gsis.at/2022/03/11/digital-humanism-on-the-test-bench/*, *https://gsis.at/2022/06/22/digital-humanism-and-the-future-of-humanity/*).

Sinnvolle Technologie muss heute Vorrang haben. Sinnvoll ist sie, wenn ihre Erforschung und Entwicklung, ihre Verbreitung und ihr Gebrauch argumentativ gesellschaftlich verantwortet werden kann. Die Grundfrage lautet daher: Welche Tätigkeiten und Resultate der Informatik sind unter den Bedingungen, dass die Möglichkeitsräume durch die fortschreitende Polykrise immer stärker eingeschränkt werden, noch verantwortbar? Welche Tätigkeiten und Resultate also unterstützen die Überwindung der Polykrise oder sind sogar unverzichtbar für den Aufbau einer sozial- und umweltverträglich angepassten technischen Infrastruktur weltweit? Welche Tätigkeiten und Resultate stehen dem im Weg oder befeuern die Krise sogar? Und wie kann eine Förderung der sinnvollen Technologien erreicht werden, und wie kann denjenigen Technologien, die nicht zu einer Lösung beitragen können oder sogar schädlich für die transformativen Ziele sind, verwehrt werden, auf Kosten der sinnvollen Technologien gefördert zu werden?

Die Beantwortung dieser ethischen Frage ist wie eine Weichenstellung, von ihr hängen alle weitergehenden Verzweigungen

Wien Aktionstag #SaveYourInternet, Foto: Karola Riegler ,CC BY

in die Beachtung der kulturellen, politischen und ökonomischen, der ökologischen und schließlich der technischen Fragestellungen zur Gestaltung der erwarteten Anwendungen ab, auch wenn sie deren Antworten nicht im Detail vorherzubestimmen mag. Alle Antworten zusammen, im Großen wie im Kleinen, entscheiden mit über die Zukunft der Menschheit, sobald sie umgesetzt werden. Sie gehen besonders alle an, die von den Informationstechnologien betroffen sind, und sollten von ihnen auch entsprechend erörtert werden. Ganz sicher aber tangieren sie das Selbstverständnis der im Bereich der Informatik Tätigen.

Deshalb wollen wir auf der kommenden FIfF-Konferenz die möglichen Antworten auf diese Fragen verhandeln. Richtig verstanden, kann uns der Digitale Humanismus helfen, die richtigen Entscheidungen zu treffen.

Das Programm wird Vorträge und Diskussionen einschließen. Wir erwarten aber gerne Vorschläge zu speziellen Thematiken, in welchen Formaten auch immer, wie etwa – im Sinne von *Informatik und Gesellschaft* – zu Informatik und

- die Militarisierung der Gesellschaft,
- den Stellenwert von Desinformation im öffentlichen Diskurs,
- die politische Rechtsentwicklung,
- die Simulationen des Klimawandels,
- die Zuschreibung von Bewusstsein und Emotionen zur KI,
- ihre eigene Dekolonisierung,
- …

Vorschläge sind bis zum 31. Juli 2025 formlos per E-Mail an *office@gsis.at* erbeten.

Wolfgang Hofkirchner, Irena Mostowicz, Annette Grathoff, *Renate C.-Z.-Quehenberger (GSIS)*

Maja Warlich

Reeling in Secrets

A Deep Dive into FinFisher Spyware

FinSpy is a notorious government–sponsored spyware capable of infiltrating major operating systems to gather private data, intercept communications, and record audio or video. Criticized by human rights organizations for enabling surveillance and intimidation of dissidents, its use by authoritarian regimes raises serious concerns. This paper explores FinSpy's technical details, features, discovery, analysis, and human rights implications.

1 The Advent of Spyware

The practice of espionage, privacy invasion, and peeking over the neighbor's fence to see what exactly they are up to is as old as civilization itself. Whether in times of war or peace, the work of a spy, who must venture into the enemy's sphere of influence, can be extremely dangerous. However, the dawn of digital data, the internet, and online communication transformed at least a part of the world of espionage and intelligence into a more secure, HQ–based setting, where no spy has to risk bodily harm. It is the advent of spyware.

Alongside HackingTeam's Remote Control Systems and software suites like Pegasus and Flame [3, 15, 19], the FinSpy spyware suite developed by the FinFisher company group may be one of the most prominent state trojans. Since its surveillance methods first gained public attention through leaked marketing documents at a conference in 2011 [26], it has been revealed that at least 32 states employed the spyware [16], hinting towards its widespread global proliferation. Numerous FinSpy samples have emerged from the electronic devices of journalists, activists, and opposition leaders, allowing cybersecurity experts to conduct in–depth analyses of various versions of the spyware. While results vary among samples, they all are equipped with sophisticated techniques for infiltrating devices, obfuscating their activities, and extracting sensitive data. In researching FinSpy's server infrastructure and taking apart samples, experts have pinpointed their likely origin, creation date, and proliferation.

2 The Mechanics of FinSpy

Since its first discovery, multiple samples of FinSpy have been detected in spoofed e-mails, trojanized software updates, and infected devices. Different versions of the spyware exist for all major operating systems Windows, Linux, Mac OS, Android, iOS, Blackberry, and Symbian, with their method of operation and functionalities varying somewhat. This section gives an overview of how FinSpy operates on a target device, which functions it offers, and how it communicates with its operator.

2.1 Infiltration and Obfuscation Methods

Product portfolios from FinFisher and FinFisher's parent company Gamma Group leaked to WikiLeaks in 2011 detailing several components from the FinFisher product suite. Among them are the FinFly tools, a variety of tools FinFisher offers buyers to covertly deliver the FinSpy spyware to a target device [7, Page 21ff], see Figure 1. While some rely on an attacker having physical access to the device, others can infiltrate a device without the spyware operator ever leaving their office. An overview of FinFly is shown in Figure 2.

Figure 1: The FinSpy operator uses FinFly tools to covertly deploy FinSpy onto target devices [7].

In conjunction with FinFly tools, social engineering methods are used to deceive victims into admitting FinSpy payloads onto their devices. One such example happened in the context of the 2017 *March for Justice* in Turkey. Several Twitter and Facebook users began promoting a website named *Adalet*, Turkish for *justice*. Björksten and Krahulcova [2] reveal that the *Adalet* site was used as bait to attract government critics interested in the protest. The site prompted visitors to download an Android application, which really was a version of FinSpy designed for mobile phones.

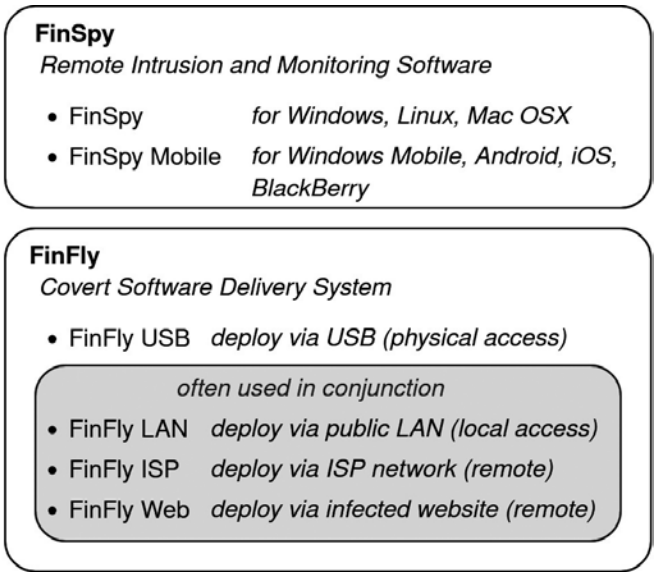


Figure 2: Overview of FinFisher's FinSpy and FinFly products [7].

In an earlier incident in 2012, Bahraini activists received e–mails from a presumably spoofed sender claiming to be correspondent Melissa Chan from the Al Jazeera media network [17]. Attached to the e–mails were FinSpy executables disguised via *Right–to–left–override* (RLO) [6] as images of arrested or tortured individuals. RLO causes text, such as a filename, to be displayed in reverse. Here, this was used to make the true filename of the executable attachment file `gpj.bajaR.exe` appear as `exe.Rajab.jpg`, a harmless image file. When clicked on, the attached files indeed showed images, while in the background and unbeknownst to the victim, the installation process began.

One of the methods FinSpy uses to install itself and operate in secret is the *process hollowing* technique [1]. This involves starting legitimate Windows processes, immediately suspending them, and deallocating their memory. Malicious code is then injected into the hollowed–out address space and the process resumed [1, 17]. Other steps FinSpy takes to conceal itself and resist analysis in the case of discovery include the use of hidden directories [10], not displaying a menu icon on mobile devices [2], junk instructions, continuous code jumps, encryption of binaries, and crashing commonly used debugging tools [9, 10, 17, 23, 24].

2.2 Functionalities

FinFisher's portfolio describes FinSpy's surveillance capabilities, which include fully surveilling a victim's Skype profile, monitoring e–mails, recording via webcam or microphone, and extracting files [7, Page 13].

Independent analyses have confirmed these claims and uncovered additional capabilities, demonstrating that the spyware evolved to stay up to date with commonly used communication methods. For instance, the FinSpy Mobile sample from the *Adalet* Website (often referred to as the *Adalet* Sample) has been found to collect "communications and media files from messengers like Line, WhatsApp, Viber, Telegram, Skype, Facebook Messenger, Kakao, and WeChat" [2]. In addition to the already mentioned capabilities, the *adalet* sample also collects address book data, calendar information, and personal photos. It also monitors calls, the device's geolocation, and its screen [2]. Another sample was even found to include a module for monitoring keystrokes [10], which means it could record any text, including passwords, typed on the keyboard of the infected device.

2.3 Communication between FinSpy and Operator

FinSpy allows operators to retrieve data remotely, transmitting it to a FinSpy Master server provided by FinFisher [16]. This server stores harvested data, controls infected devices, and sends commands to FinSpy instances on infected devices [7, Page 14f].

To obscure the operator's identity and location, FinFisher advises using FinSpy Relay servers as proxy servers mediating between infected devices and the Master server [16], see Figure 3. These Relay servers are often hosted on third–party Virtual Private Servers and merely forward data to the Master Server [2, Page 11].

3 Context Derived from FinSpy's Metadata

This chapter analyses the broader picture surrounding FinSpy and summarizes various analyses conducted on metadata of the spyware. These analyses were mainly done to find proof of FinSpy's time of creation, origin, and global proliferation.

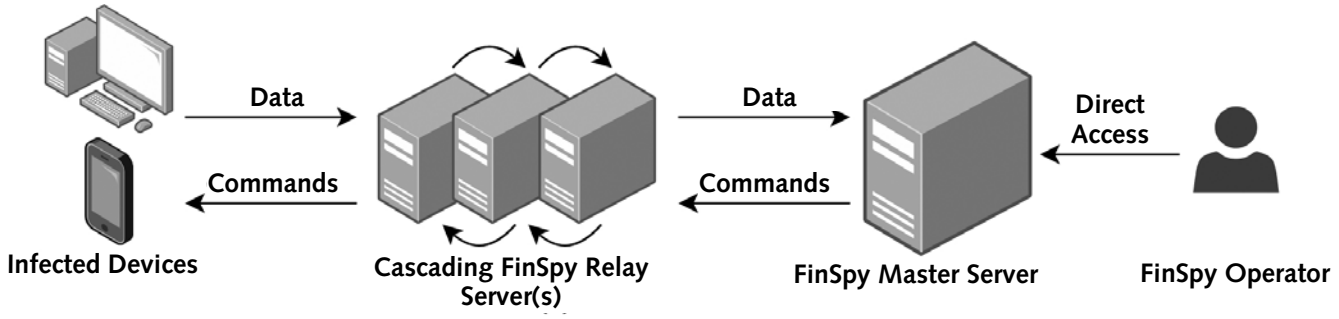


Figure 3: Devices infected with FinSpy transmit harvested data to one or more cascading FinSpy Relay servers. The final Relay server sends the data to the Master server, from where it is accessed by the FinSpy operator. In turn, the FinSpy operator sends commands through the FinSpy Master and FinSpy

3.1 Creation Time

On July 18, 2015, intrusion software was added to the German *Foreign Trade and Payments Ordinance*, thus requiring official authorization for export [25]. In July 2019, the German government confirmed that no export permits for software like FinSpy had been issued since the regulation took effect [13]. To investigate potential violations, the GFF commissioned the Chaos Computer Club (CCC) to analyze whether FinSpy samples exported outside the EU were created before July 2015, when exports were still legal, or after, making them illegal [25]. The resulting CCC report focuses on determining the earliest possible compilation date of the *adalet* sample and its authorship, using three dating methods detailed in the following sections and summarized in Table 1.

Dating Method	Details	Relevant Date	Significance
Library Version	Usage of open-source SQLite Version 3.13.0 released on relevant date	May 18, 2016	Sample created after relevant date
Certificate Validity	Sample signed with certificate valid from relevant date	October 10, 2016	Sample likely signed at or after relevant date
Compilation Timestamps	File contains timestamp of its compilation date (relevant date)	September 23, 2016	Parts of sample likely compiled on relevant date

Table 1: Overview of the dating methods used by Schröder and Neumann [25]. The information is further elaborated on in Section 3.1.

3.1.1 Library Version Release Date

The sample uses a library file `libsqliteY.so`, which contains version 3.13.0 of the open–source database library *SQLite [25]*. This version was released on May 18th, 2016 [4], and could not have been available to FinFisher's developers at an earlier date. This proves the *adalet* sample was created after May 18th, 2016.

3.1.2 Certificate Validity Date

The certificate used to digitally sign the *adalet* sample is valid from October 10th, 2016 [25]. Although the validity date of certificates can be freely chosen, it is usually the time of the creation of the certificate. As software is digitally signed prior to its distribution to ensure customers of its authenticity and integrity, it is highly likely that the *adalet* sample was distributed after October 10th, 2016.

3.1.3 Compilation Timestamp

Finally, the file `build-data.properties` contains a timestamp of its compilation date, September 23rd, 2016 [25]. Though this timestamp can be manipulated with reasonable effort, the researchers in the report argue that there is no motivation for the developers to manipulate this timestamp and set it to represent a date in the future. This means that parts of the *adalet* samples are likely to have been compiled on September 23rd, 2016.

3.1.4 Conclusion

The report concludes that the *adalet* sample must have been created after May 18th, 2016, with parts of it likely compiled on September 23rd, 2016, and distribution likely not occurring before October 10th, 2016. It is thus proven that the earliest possible date of creation lies after July 18th, 2015, the date when the addition of intrusion software was made to the German Foreign Trade and Payments Ordinance. Having been created by FinFisher after July 2015 and with no authorization for export granted, the Society for Civil Rights reasons that the proliferation of the *adalet* sample was illegal and filed charges against FinFisher, see Section 4.1.

3.2 Attribution

Unlike most proprietary software, spyware typically conceals its authorship to complicate efforts of tracing its development and proliferation. The attribution of a malware sample can significantly aid in examining it, comparing it to other samples, developing countermeasures against it, and possibly taking legal action against the author and developer [25]. Following this doctrine, FinFisher has taken steps to conceal its authorship of FinSpy samples. In the following sections, the results of two research groups attempting to prove the authorship of suspected FinSpy malware samples are presented.

3.2.1 CCC Research Report

After estimating the creation time of the *adalet* sample, the CCC report seeks to determine the author of the samples it analyzes. For this purpose, it compares 28 different malware samples suspected to be developed by FinFisher [25]. This includes twelve samples leaked in a hacker attack on the Gamma Group in 2014 and therefore unequivocally attributed to FinFisher. By demonstrating a sufficiently high degree of similarity between these samples and samples of unknown authorship, the report demonstrates with high certainty that samples of previously unknown authorship also belong to the FinFisher group.

Certificates. Usually, cryptographic certificates are used to sign software before it is sold. Due to modern cryptography, they are almost impossible to reconstruct or falsify. Unless the private part of a certificate was somehow obtained by a third party, any software samples sharing the same certificate almost certainly stem from the same developer or company.

Three unknown FinSpy samples (*JHANUK*, *Android*, and *derise*) share the same certificate as the *421and* sample, which was part of the 2014 leak and linked to FinFisher. This confirms that these three samples were also created by FinFisher. While some other samples share certificates, no additional matches between leaked samples and samples of unknown authorship were found.

Code Structure. The researchers also found similarities in the code structure between the FinSpy sample *421and* and the sample *adalet*, which was the main focus of their research [25]. They illustrate this with an example: The function `run()` is present in the SMS section of both samples. The *421and* sample implements it in the Java class *SmsInbox* (`Smsinbox.java`, `com\android\services\sms`), while the *adalet* sample implements it in class *e* (`e.java`, `org\customer\fu\s1ms`). The researchers suspect that the code was refactored after the hacker attack leaked the *421and* sample to mislead anti–malware programs. However, analysis of the code structure and the control flow of both `run()` functions show clear similarities unlikely to be random chance.

Language. The *adalet* sample often uses so–called leet–speak, where certain letters are exchanged for similar–looking numbers. Therefore the string *s1ms* (see class *e* in Paragraph *Certificates*) can be assumed to mean *sims*, a word derived from the German colloquialism *simsen* (English: to text message [5]). The same string contains the word *fu*, the German pronunciation of the English *foo*, a word often used in code examples. Both occurrences are indicative of German–speaking developers, and as the FinFisher company is based in Munich, Germany, it stands to reason that many of their employees speak German. Therefore, the use of these German–based words is a further indication of *adalet* sample being developed by FinFisher.

Conclusion. The researchers conclude that there are strong indications for the 28 analyzed samples sharing the same origin. They further ascertain that the *adalet* sample was developed by FinFisher. This is proven by the *adalet* sample's non–random and high similarities to older samples unequivocally linked to FinFisher.

3.2.2 Citizen Lab Research Reports

In 2012, Marquis–Boire and Marczak from the Citizen Lab of the Munk School of Global Affairs & Public Policy at the University of Toronto released *From Bahrain With Love: FinFisher's Spy Kit Exposed?* [17], which examines malware samples found in e–mail attachments to Bahraini activists. A month later and with the added co–authorship by Claudio Guarnieri, the team released *The SmartPhone Who Loved Me: FinFisher Goes Mobile?* [18], in which they analyzed additional FinSpy Mobile samples sent to them by security activists in response to their first analysis.

Bahraini Sample. Section 2.1 describes the *process hollowing* technique used to secretly execute the malware in the Bahraini e–mails. The Citizen Lab research group shows that memory dumps of two hollowed and infected processes contain the following strings, here displayed with an emphasis on the relevant parts added by us:

- `y:\lsvn_branches\`**`finspy`**`v4.01\`**`finspy`**`v2\src\libs\libgmp\mpn-tdiv_qr.c`
- `y:\lsvn_branches\`**`finspy`**`v4.01\`**`finspy`**`v2\src\target\bootkit_x32driver\objfre_w2k_x86\i386\bootkit_x32driver.pdb`

They point out the string *finspy* as the name of the FinSpy component in FinFisher's intrusion and monitoring toolkit [17], a strong indication as to where these malware samples were developed.

FinSpy Mobile Samples. The mobile samples examined by the group also include references to their origin. The distribution developed for iOS contains the *finspy* string in its binaries and a developer's certificate found in the same distribution belongs to Martin Muench, who was Managing Director of Gamma International GmbH and head of the FinFisher product portfolio [22]. In the Android sample, the Base64 decoded hexdump of the `84c.dat` file, which contains internal and external file attributes, reveals the hostname `demo-de.gamma-international.de` [18]. These findings link these mobile samples not only to FinFisher's product FinSpy, but also to FinFisher's parent company Gamma International.

3.3 Proliferation

Another area of interest when it comes to research around FinSpy is the question of proliferation. To obfuscate the operator's identity, no obvious tags in FinSpy samples declare its buyer and operator. However, the context in which a sample is deployed as well as country–specific data hidden in its configuration can indicate which state or organization may be responsible for the operation of a FinSpy sample. Some of the samples that researchers could attribute to a state are reviewed below.

3.3.1 Bahraini Samples

The Bahraini samples were discovered in 2012 and extensively analyzed by Marquis–Boire and Marczak [17]. Disguised as sensitive information on state–sanctioned torture, they were sent to Bahraini pro–democracy activists. Given the highly targeted nature of these attacks, it is plausible that the operators are either Bahrain–friendly entities or even the Bahraini government or security apparatus itself. The deployment of such spyware against political dissidents aligns with the interests of a regime seeking to suppress opposition and monitor activist activities.

3.3.2 Turkish Sample

Björksten and Krahulcova [2] meticulously document a similarly targeted attack on sympathizers of the 2017 *March for Justice* in Turkey. Section 2.1 explains how the *Adalet* website was advertised to protestors and covertly deployed the *adalet* FinSpy sample onto mobile phones under the pretense of downloading a mobile application. Like with the Bahrain incident, the targeting of individuals involved in this protest strongly suggests that the operators behind this attack are aligned with the Turkish government or its security agencies.

3.3.3 Ethiopian and Vietnamese Samples

Marquis–Boire et al. [14] attribute another FinSpy Mobile attack to Ethiopia. Images of the Ethiopian opposition group *Ginbot 7*

were used as bait for the victim of the intrusion attack and the FinSpy sample communicated with an Ethiopian–based server hosted by Ethiopia's state–owned telecommunications provider Ethio Telecom [14, 27]. Another sample connects to a Vietnamese server and transmits text messages to a Vietnamese phone number [14]. While this does not definitively prove that the operators of these FinSpy attacks are Ethiopian or Vietnamese, respectively, it strongly indicates their affiliation.

4 Controversies

Section 4.1 recounts the legal consequences the FinFisher company faced for their proliferation of FinSpy. Additionally, FinSpy and its developer FinFisher are analyzed through the lens of ethics and human rights in Section 4.2.

4.1 Legal Consequences

In 2013, Privacy International and others filed a complaint with the Organization for Economic Cooperation and Development (OECD) alleging Gamma International violated guidelines by selling FinSpy to Bahrain, enabling human rights abuses [11]. Based on reports of targeted attacks on Bahraini activists, the UK OECD Contact Point confirmed in 2014 that Gamma breached the guidelines but issued only recommendations, as the OECD guidelines are voluntary.

In 2019, the GFF, along with other human rights organizations, leveled an accusation based on the CCC report [25] against FinFisher for violating German export regulations [13]. The criminal complaint against FinFisher alleged that the company sold FinSpy to Turkish authorities between 2016 and 2017 without the legal authorization necessary. In the following investigation, German authorities raided FinFisher's offices and the private residences of several FinFisher executives. In March 2022, the Public Prosecutor's Office announced it had seized the company's business accounts [8, 13]. In the same month, FinFisher declared bankruptcy [8]. A year later, in May 2023, four FinFisher executives were charged for violating export requirements for dual–use goods when selling FinSpy to Turkey [8, 21]. The trial is yet to be concluded.

4.2 Ethical Concerns and Implications

The level of privacy invasion FinSpy enables stands in conflict with fundamental human rights principles. If anything, the only acceptable use of FinSpy would be in accordance with international law and in a non–arbitrary way to protect more rights and freedoms than are harmed. This could entail gathering intelligence on criminal actors to use as evidence or spying on terrorist networks to prevent attacks. The best–case scenario, therefore, is for FinSpy to be used exclusively under the strict oversight of elected officials, with its deployment authorized by independent courts in cases where its benefits clearly outweigh the potential harms.

This scenario, however, is far from reality: FinSpy regularly contributed to the surveillance and oppression of human rights activists, journalists, and opposition politicians [21]. The Bahraini FinSpy campaign targeted dissidents and activists such as Dr Saeed Shehabi and Moosa Mohammed [12, 17]. The *adalet* sample was aimed at Turkish citizens interested in the 2017 opposition movement *March for Justice* [2]. FinSpy's deployment by authoritarian regimes against politically determined targets highlights its potential as a tool for oppression, rather than legitimate law enforcement.

The accountability for FinSpy's misuse extends beyond the government and law enforcement entities operating the spyware. In providing this powerful surveillance tool to potentially repressive regimes, the Munich–based company FinFisher not only violated OECD guidelines for corporate responsibility [20] but also German and European law [13, 21]. In our opinion, the lack of transparency, oversight, and responsibility is concerning. This is especially true as the FinFisher executives, developers, and other employees responsible for FinSpy's global proliferation lived and worked in a country that guarantees them the same rights to privacy that their product violates. The global proliferation of FinSpy, despite legal regulations, underscores the need for stronger international controls and oversight.

A slightly longer version of this paper was written as part of the conference seminar IT Security *which was organized by the IT Security Infrastructures Lab at the FAU during the summer term 2024. Special thanks to Lisa Marie Dreier und Julian Geus for the support provided while this paper was written.*

Maja Warlich

Maja Warlich studiert noch bis 2025 Informatik mit einem Fokus auf IT-Sicherheit an der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU). Sie arbeitet in der Nachwuchsgruppe *Geographien digitaler Infrastrukturen* am Institut für Geographie der FAU und forscht im interdisziplinären Rahmen der digitalen Geographie und IT-Sicherheit.
Nach Abschluss ihres Masters wird sie dort eine Promotion zu geopolitischen Konflikten um Internet-Routing beginnen.

References

[1] The MITRE Corporation. 2023. Process Injection: Process Hollowing. https://attack.mitre.org/techniques/T1055/012/ Accessed 2024-06-10.

[2] Gustaf Björksten and Lucie Krahulcova. 2018. Alert: FinFisher Changes Tactics to Hook Critics. https://www.accessnow.org/wp-content/uploads/2018/05/FinFisher-changes-tactics–to-hook-critics-AN.pdf Accessed 2024-06–08.

[3] Ajay Chawla. 2021. Pegasus Spyware – 'A Privacy Killer'. http://dx.doi.org/10.2139/ssrn.3890657 Accessed 2024–06–02.

[4] SQLite contributors. 2016. SQLite Release 3.13.0 On 2016–05–18. https://www.sqlite.org/releaselog/3_13_0.html Accessed 2024–06–30.

[5] Wiktionary contributors. 2024. simsen. https://en.wiktionary.org/wiki/simsen Accessed 2024–06–29.

[6] Unicode Explorer. [n. d.]. RIGHT–TO–LEFT OVERRIDE. https://unicode–explorer.com/c/202E Accessed 2024–06–08.

[7] FinFisher. 2011. FinFisher: Governmental IT Intrusion and Remote Monitoring Solutions. https://wikileaks.org/spyfiles/document/gamma/299_finfisher–governmental–it–intrusion–and–remote–monitoring/ Accessed 2024–06–07.

[8] European Center for Constitutional and Human Rights. 2023. Surveillance software "made in Germany" for Turkish authorities? Public Prosecutor's Office charges FinFisher executives. https://www.ecchr.eu/en/case/surveillance–software–germany–turkey–finfisher/ Accessed 2024–07–17.

[9] Microsoft Threat Intelligence. 2018. FinFisher exposed: A researcher's tale of defeating traps, tricks, and complex virtual machines. https://www.microsoft.com/en–us/security/blog/2018/03/01/finfisher–exposed–a–researchers–tale–of–defeating–traps–tricks–and–complex–virtual–machines/ Accessed 2024–06–10.

[10] Amnesty International. 2020. German–made FinSpy spyware found in Egypt, and Mac and Linux versions revealed. https://www.amnesty.org/en/latest/research/2020/09/german–made–finspy–spyware–found–in–egypt–and–mac–and–linux–versions–revealed/ Accessed 2024–06–10.

11] Privacy International. 2013. Briefing note on OECD Complaints against Gamma International and Trovicor in the UK and Germany. https://www.oecdwatch.org/complaint/privacy–international–et–al–vs–gamma–international/ Accessed 2024–07–15.

[12] Leighday. 2023. High Court rules dissidents can bring FinFisher spyware claims against Kingdom of Bahrain in the UK. Leighday (2023). https://www.leighday.co.uk/news/news/2023–news/high–court–rules–dissidents–can–bring–finfisher–spyware–claims–against–kingdom–of–bahrain–in–the–uk/ Accessed 2024–07–31.

[13] Sarah Lincoln. 2023. Illegaler Export von Überwachungssoftware. https://freiheitsrechte.org/themen/freiheit–im–digitalen/export–von–uberwachungssoftware Accessed 2024–07–09.

[14] Morgan Marquis–Boire, Bill Marczak, Claudio Guarnieri, and John Scott–Railton. 2013. You Only Click Twice: FinFisher's Global Proliferation. https://citizenlab.ca/2013/03/you–only–click–twice–finfishers–global–proliferation–2/ Accessed 2024–07–02.

[15] Bill Marczak, Claudio Guarnieri, Morgan Marquis–Boire, and John Scott–Railton. 2014. Mapping Hacking Team's "Untraceable" Spyware. https://issuu.com/citizenlab/docs/mapping_hacking_team___s__untraceab Accessed 2024–06–02.

[16] Bill Marczak, John Scott–Railton, Adam Senft, Irene Poetranto, and Sarah McKune. 2015. Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation. https://citizenlab.ca/2015/10/mapping–finfishers–continuing–proliferation/ Accessed 2024–06–02.

[17] Morgan Marquis–Boire and Bill Marczak. 2012. From Bahrain with Love: Fin–Fisher's Spy Kit Exposed? https://citizenlab.ca/2012/07/from–bahrain–with–love–finfishers–spy–kit–exposed/ Accessed 2024–06–08.

[18] Morgan Marquis–Boire, Bill Marczak, and Claudio Guarnieri. 2012. The Smart–Phone Who Loved Me: FinFisher Goes Mobile? https://citizenlab.ca/2012/08/the–smartphone–who–loved–me–finfisher–goes–mobile/ Accessed 2024–06–24.

[19] Kate Munro. 2012. Deconstructing Flame: the limitations of traditional defences. Computer Fraud Security 2012, 10 (2012), 8–11. https://doi.org/10.1016/S1361–3723(12)70102–1

[20] UK NCP. 2014. Privay International Gamma Insternationa UK LTD: Final Statement After Examination Of Complaint. https://www.oecdwatch.org/complaint/privacy–international–et–al–vs–gamma–international/ Accessed 2024–07–15.

[21] Reporter ohne Grenzen. 2023. Anklage gegen FinFisher–Verantwortliche. https://www.reporter–ohne–grenzen.de/pressemitteilungen/meldung/staatsanwaltschaft–klagt–finfisher–verantwortliche–an Accessed 2024–07–18.

[22] Nicole Perlroth. 2012. Elusive Finspy spyware pops up in 10 countries. https://archive.nytimes.com/bits.blogs.nytimes.com/2012/08/13/elusive–finspy–spyware–pops–up–in–10–countries/ Accessed 2024–06–26.

[23] Rolf Rolles. 2018. FinSpy VM Part 2: VM Analysis and Bytecode Disassembly. https://www.msreverseengineering.com/blog/2018/1/31/finspy–vm–part–2–vm–analysis–and–bytecode–disassembly Accessed 2024–06–10.

[24] Rolf Rolles. 2018. A Walk–Through Tutorial, with Code, on Statically Unpacking the FinSpy VM: Part One, x86 Deobfuscation. https://www.msreverseengineering.com/blog/2018/1/23/a–walk–through–tutorial–with–code–on–statically–unpacking–the–finspy–vm–part–one–x86–deobfuscation Accessed 2024–06–10.

[25] Thorsten Schröder and Linus Neumann. 2019. Evolution einer privatwirtschaftlichen Schadsoftware für staatliche Akteure. https://www.ccc.de/system/uploads/291/original/FinSpy_Report_CCC_v1.0.pdf Accessed 2024–06–02.

[26] Jennifer Valentino–Devries, Julia Angwin, and Steve Stecklow. 2011. DocumentTrove Exposes Surveillance Methods. http://aldeilis.net/mumbai/1757.pdf Accessed 2024–06–02.

[27] Wikipedia contributors. 2024. Ginbot 7 – Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/wiki/Ginbot_7 Accessed 2024–07–02.

Maurice Haugk

Chancen und Risiken von KI und Auswirkung des EU AI Act

Künstliche Intelligenz, kurz auch KI, hat immer größeren Einfluss auf die Prozesse von Unternehmen, und auch im Privaten begegnet man dem Thema immer häufiger. Diese zunehmende Präsenz von KI im Alltag sorgt für die Notwendigkeit, sich mit diesem Thema auseinanderzusetzen und sich über Chancen und Risiken bewusst zu werden.

KI wird von Unternehmen zunehmend mit in die Wertschöpfungskette einbezogen und nimmt Mitarbeitenden Routinetätigkeiten ab. So wird KI beispielsweise in der Betrugserkennung von Finanzdienstleistern eingesetzt, kann Dokumente auswerten und zusammenfassen, Anomalien erkennen oder kommt in Antivirus-Software zur Erkennung von noch unbekannter Schadsoftware zum Einsatz.

Neben diesen vielfältigen Einsatzmöglichkeiten birgt KI aber auch Risiken, insbesondere für die Informationssicherheit. So lassen sich durch KI Deepfakes erstellen, die für Social-Engineering-Angriffe missbraucht werden können. Außerdem beschleunigt KI die Erstellung von Malware und macht diese auch für Angreifer mit wenig technischem Verständnis zugänglich. Auch ist unklar, wie eingegebene Daten von der KI verwendet werden und ob diese anderen Anwendern offengelegt werden.

Daraus resultieren einige Empfehlungen zum Umgang mit KI. Man sollte grundsätzlich der KI keine vertraulichen Informationen preisgeben und sich immer bewusst sein, dass man mit einer Maschine interagiert. Auch ist es für Unternehmen von Vorteil und in einigen Fällen sogar durch den EU AI Act vorgeschrieben, eine Risikobewertung der eingesetzten KI-Use-Cases unter Einbeziehung eines interdisziplinären Teams durchzuführen. Der AI Act verlangt auch unabhängig von der Risikokategorie der eingesetzten oder benutzten KI die Sicherstellung von KI-Kompetenz, was beispielsweise Schulungen beinhaltet.

Der AI Act stellt eine gute Möglichkeit für Unternehmen in der EU dar, im Bereich vertrauenswürdiger KI eine Führungsrolle einzunehmen. Allerdings zeigt sich derzeit noch nicht flächendeckend der Bedarf nach solcher KI, wodurch KI-Startups in der EU im Wettbewerb das Nachsehen haben.

Maurice Haugk

Maurice Haugk studierte an der DHBW Stuttgart Wirtschaftsinformatik im Bachelor und studiert nun neben seiner Tätigkeit als Information Security Officer im Master Wirtschaftsinformatik Branchenfokus Cyber Security an der FHAM Ismaning. In seiner Bachelorarbeit schrieb er über die Chancen und Risiken von KI. Auch nach seinem Bachelorabschluss beschäftigte er sich weiterhin mit dem Thema KI, insbesondere in Bezug auf den EU AI Act und dessen Auswirkungen auf Entwicklung und Betrieb von KI.

Hans-Jörg Kreowski

Die (Un-)Möglichkeit, denkende Maschinen zu entwickeln

Der Hype um die Künstliche Intelligenz wird neben den teilweise beeindruckenden Erfolgsmeldungen und euphorischen Erwartungen zusätzlich gesteigert durch die Diskussion um Superintelligenz. Es geht dabei um das Vorhaben, Maschinen zu bauen, die so intelligent sind und so gut denken können wie Menschen oder sogar intelligenter sind als diese. Ist das überhaupt möglich? Die Frage hat offensichtlich eine technische Seite, macht aber nur Sinn als Gegenstück zum Denken in der Natur, zu intelligenten Lebewesen und insbesondere zum denkenden Menschen. Die Frage hat aber auch eine ethische und philosophische Dimension. Denn sollte es eines Tages Maschinen geben, die besser denken als Menschen, wäre interessant, wie sie sich gegenüber Menschen verhalten werden: freundlich und partnerschaftlich oder feindlich und aggressiv. Sollte die Menschheit nicht besser auf eine derartige technische Entwicklung verzichten? In diesem Artikel möchte ich mich mit dem Für und Wider denkender Maschinen auseinandersetzen. Es ist mein dritter Versuch, mich der Thematik zu nähern (Kreowski 1998, Kreowski & Krieger 2021).

Von der Künstlichen Intelligenz zur Künstlichen Allgemeinen Intelligenz

Gefördert durch die Rockefeller-Stiftung, trafen sich 1956 zehn junge, später sehr berühmte US-amerikanische Wissenschaftler für einige Wochen im Dartmouth College in Hanover, New Hampshire, um das Fachgebiet der Künstlichen Intelligenz (KI) zu gründen. Sie gingen von der Annahme aus, dass Computer durch geeignete Programmierung dazu gebracht werden können, Merkmale von Intelligenz zu simulieren wie die Nutzung von Sprache, Lernen, Abstraktion, Kreativität, Problemlösen, Konzeptentwicklung und Selbstverbesserung (McCarthy et al. 1955). Schon damals galt das aus den 1940er-Jahren stammende Konzept der künstlichen neuronalen Netze als eine vielversprechende methodische Grundlage, die in den letzten Jahren so viel Furore gemacht hat. Auch wenn KI als Gegenkonzept zur

bis dahin schon etablierten *Computer Science* gedacht war, ist festzuhalten, dass Computer von Anfang an entwickelt und eingesetzt wurde, weil damit schnell und komplex gerechnet, gesucht, sortiert, gespeichert, überwacht und kontrolliert werden konnte. Also ging es auch da schon um die Simulation kognitiver Prozesse. Frieder Nake charakterisiert in (Nake 1992) als Aufgabe der Informatik die Maschinisierung der Kopfarbeit und eben nicht nur als die der KI.

Zwei der Gründungsväter der KI, John McCarthy und Marvin Minsky, habe ich in der 1980er-Jahren selbst sagen hören, dass das eigentliche Ziel sei, Maschinen zu bauen, die intelligenter sind als Menschen. Diese Absicht wurde anfangs unter dem Begriff der harten oder starken KI propagiert, inzwischen ist dafür eher die Bezeichnung *Künstliche Allgemeine Intelligenz* etabliert (im Englischen *Artificial General Intelligence* (AGI)). Der überwiegende, weniger ambitionierte Teil der KI wird demgemäß oft als schwache KI bezeichnet. Die Zahl derer, die der These von der Machbarkeit allgemein intelligenter und denkender Maschinen anhängen, ist immer noch recht klein, aber es finden sich eine Reihe Prominenter darunter. Neben den glühenden Anhänger:innen gibt es auch einige, die damit große Befürchtungen verbinden. Hier kann der offene Brief des Future of Life Institute (2023) angeführt werden, den viele bekannte und weniger bekannte Fachleute unterschrieben haben und der einiges Aufsehen erregt hat. Ein weiteres Beispiel ist das von mehr als 300 KI-Größen aus Wirtschaft und Wissenschaft unterschriebene 1-Satz-Statement des Center for AI Safety (2023): „Mitigating the risk of extinction from A. I. should be a global priority alongside other societal-scale risks, such as pandemics and nuclear war."

Gerade jetzt ist die Diskussion über AGI wieder neu aufgeflammt. So hat beispielsweise kürzlich erst Dario Amodei, CEO der OpenAI-Ausgründung Anthropic, prognostiziert und Jeff Bezos, der zweitreichste Mann der Welt, hat ihm beigepflichtet, dass schon 2027 AGI realisiert werden kann, während Demis Hassabis, CEO von Google DeepMind und einer der Nobelpreisträger für Chemie 2024, das erst in fünf bis zehn Jahren erwartet (Boulton 2025). Erwähnenswert in diesem Kontext ist auch die Auffassung von Geoffrey Hinton, der auch „Patenonkel der KI" genannt wird und einer der beiden ist, denen 2024 der Nobelpreis für Physik in Anerkennung ihrer Leistungen bei der Entwicklung künstlicher neuronaler Netze verliehen wurde (Loftus 2025). Er befürchtet, dass KI-Systeme anfangen könnten zu denken und dann die Weltherrschaft übernähmen. Der Physiker Max Tegmark, einer der Gründer des Future of Life Institute, haut in einem Interview, das in der ZEIT am 24. April 2025 auf Seite 36 abgedruckt ist, in dieselbe Kerbe. Ansonsten ist AGI vor allem auch ein Sachbuchthema mit Bestseller-Aussicht (siehe z. B. Bostrom 2014, Brockman 2017, Hägström 2017, Harari 2024, Kurzweil 2024, Spitzler 2023, Walsh 2018). Die Gegenposition wird allerdings nicht weniger prominent vertreten (siehe z. B. Dreyfus 1989, Dreyfus & Dreyfus 1986, Gabriel 2018, Hesse 1992, Hofstetter 2014, Precht 2020, Weizenbaum 1976).

Superintelligente Maschinen werden auch von einer Fraktion der erstaunlich starken und finanzkräftigen philosophischen Bewegung des Transhumanismus propagiert (Hofkirchner & Kreowski 2021). Deren Ziel ist die Überführung der Menschheit in die Postmenschheit vor allem auf technologischem Wege mit Hilfe von Gentechnik oder Künstlicher Intelligenz.

Bis in die 1970er-Jahre hinein fielen die Erfolge der KI bei Mustererkennung sowie bei Beweis- und Expertensystemen auf der Basis von Schlussregeln nach Art der mathematischen Logik noch recht bescheiden aus. Die Entwicklung der KI erhielt aber durch das japanische 5th-Generation-Computer-Programm und die US-amerikanische Antwort mit der Strategic Computing Initiative (SCI) in den 1980er-Jahren einen gewaltigen Schub (siehe Shapiro 1983 und Roland & Shiman 2002). Beide Projekte konnten für damalige Verhältnisse auf gigantische Finanzmittel von mehreren 100 Millionen US-Dollar zugreifen. Während das zivil angelegte japanische Projekt methodisch die logische Programmierung zur Grundlage von wissensverarbeitenden Systemen gemacht hat, waren denkende Maschinen ein erklärtes Ziel von SCI, wobei aber die militärisch geprägten, konkret konzipierten Anwendungen mit einem Sprachassistenten für die Luftwaffe, einem Schlachtenmanagementsystem für die Marine und mit autonomen Vehikeln für das Heer nur wieder auf kognitive Einzelleistungen fokussiert waren. Die zehnjährige Laufzeit von SCI und die damaligen technischen Möglichkeiten haben nicht gereicht, um solche Systeme funktionsfähig zu entwickeln. Heutzutage – rund 40 Jahre später – ist vieles davon umgesetzt. Die bedeutenden Erfolge der KI sind vor allem in diesem Jahrhundert zustande gekommen und maßgeblich beeinflusst durch die wesentlich verbesserten technischen Grundlagen dank viel schnellerer Rechenzeiten und gewaltiger Speicherkapazitäten. Zu erwähnen sind eindrucksvolle Leistungen bei der Mustererkennung, bei der Sprachübersetzung, bei der Generierung von Sprache und Bildern sowie bei Spielen wie GO und Dota 2.

Natürliches Denken

Der Natur ist es im Laufe der Evolution gelungen, denkende Lebewesen hervorzubringen. Vor allem wird Menschen die Fähigkeit des Denkens zugestanden. Es handelt sich allerdings um ein Phänomen, dessen genaue Funktionsweise bisher nicht entschlüsselt ist (vgl. z. B. Hasler 2012). Es ist wohl klar, dass Denken im Gehirn stattfindet; es ist aber völlig unklar, wie ein einzelner Gedanke, wie eine Idee entsteht, welche Prozesse dabei konkret ablaufen. Die Leistung des menschlichen Gehirns besteht auch nicht nur im Denken, sondern es befähigt zu vielen weiteren kognitiven Fähigkeiten wie Lernen, Verstehen, Rechnen, Schließen, Entscheiden, Wissen, Glauben, Fühlen, Hassen, Lieben, Hoffen, Spekulieren, Phantasieren, Angst Haben usw. Außer vernünftige Überlegungen kann es auch völlig irrwitzige Ideen und grenzenlose Dummheit entwickeln. Was davon unter Denken subsummiert werden kann und muss und was nicht, ist ungewiss. Wenn sich aber Denken überhaupt gar nicht sauber von anderen Gehirnleistungen abgrenzen lässt, könnte das bedeuten, dass denkende Maschinen immer auch all die anderen kognitiven Erscheinungsformen realisieren müssten. Wenn Intelligenz und Denken gar nicht präzise beschrieben werden können, wird sich auch kaum sicher feststellen lassen, ob eine Maschine denkt. Es wird nicht ausreichen, dass sie einen Intelligenztest besteht.

Wenn man davon ausgeht, dass alle Prozesse in der Natur einer materiellen Grundlage bedürfen, also von chemischer, physikalischer, biogenetischer Art sind – und kein (Welt-)Geist, keine göttliche Fügung zusätzlich wirkt –, dann ist auch Denken nichts anderes. Die Natur hat sich allerdings sehr viel Zeit gelassen, denkende Wesen hervorzubringen, und sie hatte dafür wohl

auch keinen Plan oder Auftrag. Die Evolution nachzuahmen, ist sicher keine Option. Es bleibt ohnehin die Frage, welche natürlichen Prozesse sich als maschinelle und algorithmische Prozesse nachbauen lassen. Obwohl in den Naturwissenschaften beeindruckend viele Erkenntnisse zusammengetragen worden sind, geben sie darauf keine Antwort – ganz abgesehen davon, dass vieles auf unbewiesenen Annahmen wie der Relativitätstheorie und der Existenz dunkler Materie und Energie beruht.

Maschinelles Denken

Nach dem Stand der Technik wird eine denkende Maschine ein Computer sein, auf dem Programme ablaufen, die das maschinelle Denken produzieren, oder sie wird eine Maschine sein, in die ein solcher Computer eingebaut ist. Die Frage nach maschinellem Denken ist somit die Frage, was Computer können, was sich programmieren lässt. In der Informatik gibt es ein gewisses Einverständnis in dieser Hinsicht: die Churchsche oder Turingsche These (Turing 1937). Es handelt sich um eine Hypothese nach Art der Relativitätstheorie. Sie besagt, dass sich alles, was berechenbar, was also algorithmisch ausführbar ist, mit einer Turing-Maschine berechnet oder – allgemeinverständlicher ausgedrückt – in einer Programmiersprache wie Java programmiert beziehungsweise mit einem gleichwertigen Berechnungsmodell beschrieben werden kann. In der Informatik sind viele solcher Modelle bekannt, von denen nachgewiesen ist, dass sie aus algorithmischer Sicht alle dasselbe leisten (oder weniger). Die meisten Berechnungsmodelle folgen einem gemeinsamen Grundschema. Es wird eine Form von Daten vorausgesetzt, z. B. Zahlen, Zeichenketten, Ausdrücke, Formeln, Diagramme, Graphen, chemische Moleküle o. ä., für die elementare Operationen verfügbar sind wie die Grundrechenarten für Zahlen. Ein „Programm" besteht dann aus einer Sammlung von Regeln, die festlegen, wie und in welcher Reihenfolge die Operationen auf welche Daten angewendet werden. So erlauben die beiden Rechenregeln „m *mal* 0 *ist* 0" und „m *mal* n+1 *ist* (m *mal* n)+m" alle Produkte zweier natürlicher Zahlen zu berechnen durch wiederholte Anwendung der zweiten Regel, bis der zweite Faktor zu 0 verkleinert ist. Berechnen läuft immer nach einem ähnlichen Prinzip, auch wenn in der Regel die Daten und Regeln viel komplizierter sein mögen. So hat ein künstliches neuronales Netz zum Erkennen von Hautkrebs eine riesige Datenbank mit Beispielbildern zur Verfügung und versucht durch Zerlegen und Vergleichen zu einem eingegebenen vermeintlichen Hautkrebsbild die wahrscheinlichsten Übereinstimmungen mit den vorhandenen Bildern zu entdecken.

Die Turingsche These ist allerdings alles andere als konstruktiv. Sie verrät im Allgemeinen nicht, ob ein Problem algorithmisch gelöst werden kann. Und selbst wenn etwas berechenbar ist, hat man lange noch kein Programm oder Verfahren, das das realisiert. Die These hat außerdem einige unangenehme Konsequenzen. So vergeht beim Berechnen immer Zeit und oft mehr, als verfügbar ist. So braucht Berechnen Speicherplatz und oft mehr, als vorhanden ist. So gibt es kein allgemeines Verfahren, mit dem sich feststellen lässt, was ein Programm leistet.

Für den Bau einer denkenden Maschine ergeben sich daraus eine Reihe von Problemen. Selbst wenn Denken algorithmisch machbar, also programmierbar ist, hat man noch lange kein Programm. Es müsste also ein Entwicklungsprojekt aufgesetzt werden, dessen Ergebnis ein denkendes Programm ist. Das Programm könnte dann aber länger laufen, als man warten kann. Es könnte mehr Speicherplatz benötigen, als sich bereitstellen lässt. Auch könnte der Versuch scheitern, nachzuweisen oder zumindest plausibel zu machen, dass das Programm wirklich denkt. Darüber hinaus wäre ein solches Projekt sicherlich anspruchsvoller als alles, was bisher an informationsverarbeitenden Systemen entwickelt worden ist. Einige dieser Projekte haben viele Millionen verschlungen, haben viele Jahre gedauert mit Hunderten von beteiligten Entwickler:innen und sind teils dennoch gescheitert.

Maschinelles Denken setzt voraus, Denken zu programmieren, also durch ein ausführbares Regelsystem formal zu beschreiben. Solche Versuche zur Formalisierung des Denkens – allerdings beschränkt auf das logische Denken – hat es in Philosophie, Mathematik und Informatik zahlreich gegeben. Ein lesenswerter Ein- und Überblick dazu kann bei Wolfgang Coy (Coy 1988) gefunden werden. Von den Sophisten, Aristoteles und Euklid in der griechischen Antike über Leibniz, Descartes und Hobbes bis zu den Logikern des 20. Jahrhunderts mit Boole, Church, Frege, Gödel, Hilbert, Kleene, Russell und Whitehead sowie den verschiedensten Ansätzen in der KI hat es eine beachtliche Zahl an Versuchen gegeben, Denken mit Hilfe von Logikkalkülen und logischen Schlussregeln zu beschreiben, zu deuten und zu verstehen. Denken ist aber – fürchte ich – nicht nur logisch, sondern kann auch extrem unlogisch und töricht sein. Kann man das Unlogische und Dumme einfach außer Acht lassen? Wenn ich das richtig verstehe, sind darüber hinaus alle solche Kalküle in dem Sinne passiv, dass sie benutzt werden müssen durch Anfragen oder Aufgabenstellungen und oft auch durch zusätzliche gezielte Steuerung. Sie haben keinen eigenen Antrieb, keine Intuition, kein (Selbst-)Bewusstsein, keinen Ehrgeiz und keinerlei Verständnis von ihrem Tun, sie „denken" nicht selbst. Soweit sie durch ausführbare Regeln definiert sind, kann man sie laufen lassen und Schritt für Schritt alles erzeugen, was möglich ist. Das ist aber immer nur ein kleiner Ausschnitt aus einer meist unendlichen Menge an Möglichkeiten. Das ist auch völlig ziellos, so dass sich selten etwas Brauchbares und Sinnvolles ergeben wird.

Über Denken hinaus kann man fragen, ob alle Prozesse in der Natur algorithmischer Art sind. Bei chemischen Prozessen liegt das nahe, denn Moleküle und ihre Reaktionen miteinander lassen sich durch chemische Strukturformeln beschreiben, die einen ähnlichen Charakter wie Rechenregeln und logische Schlussregeln haben. Bei physikalischen Prozessen wird es davon abhängen, ob sie überhaupt diskret ablaufen und alle Materie aus kleinsten Teilen aufgebaut ist. Sonst können es keine algorithmischen Prozesse sein. Ich fürchte allerdings, dass man so auch nicht weiterkommt und der Kenntnisstand der Naturwissenschaften wie der der Technikwissenschaften dafür nicht reicht.

Was denn nun?

Die Frage, ob es möglich ist, denkende, superintelligente Maschinen zu bauen, kann ich nicht mit JA oder NEIN beantworten. Keins meiner Argumente schließt das völlig aus. Aber es spricht auch äußerst wenig dafür. So ist vor allem gar nicht klar, was Denken überhaupt ist oder wie es sich bauen lassen könnte. Darüber hinaus scheint die Leistungsfähigkeit des Gehirns so umfassend, dass ein Nachbau, selbst wenn er möglich ist, an-

spruchsvoller, teurer und aufwändiger wäre als alles von Menschen bisher Erschaffene.

Einige Apologeten der Machbarkeit denkender Maschinen sehen die technische Basis dafür in künstlichen neuronalen Netzen in Verbindung mit den großen Sprachmodellen und entsprechenden Bildverarbeitungsmodellen rund um ChatGPT & Co. Sie werden gerade mit viel Geld und Personal weiterentwickelt. Aber werden sie denken können? Diese Modelle stellen Texte, Bilder u. ä. nach vorgegebenen Anforderungen her. Ihr Grundprinzip ist, verfügbare riesige Datenbestände dahingehend zu durchsuchen, was am wahrscheinlichsten ein Resultat ergibt, das den Anforderungen gerecht wird. Die Qualität des Ergebnisses hängt von der Qualität der Datenbestände und der Wahrscheinlichkeitsbewertung ab. Inhaltliches Verständnis, Eigeninitiative, Interesse, Intuition, Phantasie, Ambition – Fehlanzeige. Das soll Denken sein oder werden können? Die Ergebnisse dieser Modelle sind immer im Alten, Bekannten, Hergebrachten verhaftet, das nur neu zusammengesetzt wird. Daran ändert auch nichts, dass manche Antworten überraschen und von einer Art sind, auf die Menschen wohl nicht gekommen wären. Daran ändert auch nichts, dass sie durch „Lernen" besser werden können. Denn es handelt sich eher um ein „Trainiert Werden", bei dem Antworten auf Testanforderungen bewertet werden, so dass das Modell schlecht bewertete Antworten später vermeiden kann. Alles, was sich mit Hilfe mehrschichtiger künstlicher neuronaler Netze auf der Basis großer Sprachmodelle erreichen lässt, bewegt sich im Rahmen der angewandten Wahrscheinlichkeitstheorie. Die jedoch funktioniert nur für Ereignisse, die sich beliebig oft wiederholen lassen, und für Gegebenheiten, die in großer Zahl vorhanden sind, also für Münzwurf, Würfeln, Spiele, Texte, Bilder u. ä. Diese Modelle können keine sinnvollen Ergebnisse produzieren, wenn etwas selten vorkommt, wenig darüber bekannt ist, neu ist. Sie produzieren auch dann schlechte Ergebnisse, wenn die vorliegenden Informationen überwiegend falsch oder irreführend sind. Das menschliche Gehirn, scheint mir, entwickelt Gedanken ohne tausendfache oder millionenfache Testläufe und ohne eine gigantische Zahl an Informationen, auf die es zugreifen kann, und entscheidet sich keineswegs immer für das Wahrscheinlichste.

Soweit ich weiß, gibt es daneben kein ernsthaftes Projekt, das von der Zielsetzung, vom Umfang, von der Anlage und von den Finanzmitteln her auch nur den Hauch einer Chance bietet, zu einer denkenden Maschine zu führen. Am ehesten könnte man in diesem Zusammenhang noch das Human-Brain-Projekt der EU deuten, das von 2013 bis 2023 gelaufen ist – und in der einen oder anderen Form fortgesetzt werden wird –, das über eine halbe Milliarde Euro gekostet hat, an dem mehr als 500 Wissenschaftler:innen aus 19 Ländern beteiligt waren (European Commission 2024). Es hat sehr erfolgreich eine Sammlung wissenschaftlicher Erkenntnisse über das menschliche Gehirn zusammengetragen, einen detaillierten 3D-Atlas des Gehirns entwickelt und eine Infrastruktur für Gehirnforschung bereitgestellt, die inzwischen von mehr als 10.000 Fachleuten und mehr als 1500 Instituten genutzt wird. Es wurden viele neue Einsichten in die Funktion des Gehirns und insbesondere in neurologische Krankheiten gewonnen. Umgekehrt sind viele gehirninspirierte Methoden im Bereich von Künstlicher Intelligenz und Robotik angeregt worden. Das Ziel, einen „Zwilling" des Gehirns zu bauen, wurde nicht erreicht.

Eine Reihe prominenter KI-Fachleute und Wirtschaftsbosse der KI-Industrie warnen vor der Gefahr, dass eine denkende, superintelligente Maschine die Macht ergreifen und die Existenz der Menschheit gefährden könnte. Das scheint mir abstrus. Denn es bedarf nicht nur denkender Maschinen, die aus meiner Sicht vorläufig gar nicht absehbar sind, sondern auch der Verfügungsgewalt und Kontrolle über einen Machtapparat aus Polizei, Geheimdiensten und Militär sowie über alle wichtigen Produktionsmittel. Wären ihre Warnungen berechtigt, könnten sie selbst etwas tun. Denn viele von ihnen treiben mit ihren Unternehmen und dem verfügbaren Kapital die aktuelle Entwicklung von KI-Systemen voran. Niemand zwingt sie dazu, den von ihnen angeblich befürchteten Untergang der Menschheit zu befördern.

Die wissenschaftlichen und technologischen Fortschritte seit Tausenden von Jahren sind wesentliche Faktoren der gesellschaftlichen Entwicklung. Wissenschaft und Technik dienen allerdings nicht automatisch dem Wohle der Menschheit, sondern werden von den Herrschenden oft für Krieg, Unterdrückung, Machterhalt, Ausbeutung, Bereicherung und für ihre eigenen Interessen eingesetzt. Das gilt heute insbesondere für Künstliche Intelligenz, weil sie eine – wenn nicht die – Schlüsseltechnologie für die Entwicklung vieler gesellschaftlicher Bereiche ist. Aber es ist nicht die KI, die Missbrauch und Fehlentwicklungen verursacht, sondern es ist den Menschen geschuldet, die sie einsetzen. Alle Risiken und Gefahren, die von Technologien ausgehen, sind menschengemacht. Um die negativen Wirkungen zu vermeiden oder einzudämmen und um echten Fortschritt zu sichern, bedarf es eines umfassenden demokratischen Diskurses und Handelns im Sinne des Gemeinwohls. Daran mangelt es.

Trotz aller Erfolgsmeldungen und Fortschrittsversprechen sind KI-Systeme bisher nicht sehr wirksam eingesetzt worden, um die drängendsten Probleme der Menschheit wie Klimawandel, Naturzerstörung, Fluchtbewegungen, Kriegsgefahren, Ar-

Hans-Jörg Kreowski

Hans-Jörg Kreowski (Jahrgang 1949) ist Professor (i. R.) für Theoretische Informatik an der Universität Bremen. Er ist Mitglied im Vorstand des *Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung* (FIfF) und vertritt das FIfF im Vorstand der Zeitschrift *Wissenschaft und Frieden*. Er ist Mitglied der *Leibniz-Sozietät der Wissenschaften zu Berlin*, wo er zusammen mit Wolfgang Hofkirchner in Wien den Arbeitskreis Emergente Systeme, Information und Gesellschaft organisiert. Von 2019 bis 2022 war er außerdem Mitherausgeber des Grundrechte-Reports.

mut, Hunger, Kampf um die Weltherrschaft usw. zu bewältigen. Wäre es nicht sinnvoll, die ungeheuren Ressourcen, die aktuell weltweit in die Entwicklung von KI gesteckt werden, dafür zu nutzen – mit oder ohne KI?

Referenzen

Boulton H (2025) Jeff Bezos-backed CEO predicts AI will hit frightening milestone in 2027. UNILAD Tech, https://www.uniladtech.com/news/ai/jeff-bezos-backed-ceo-frightening-ai-prediction-2027-993296-20250326 [abgerufen am 25. April 2025].

Bostrom N (2014) Superintelligenz – Paths, Dangers, Strategies. Oxford University Press, Oxford.

Brockman J Hg. (2017) Was sollen wir von KI halten – Die führenden Wissenschaftler unserer Zeit über intelligente Maschinen. Fischer Taschenbuch, Frankfurt am Main.

Center for AI Safety (2023) AI Extinction Statement Press Release. https://safe.ai/work/press-release-ai-risk [abgerufen am 2. Mai 2025].

Coy W (1988) Industrieroboter. Zur Archäologie der zweiten Schöpfung. Rotbuch Verlag, Berlin.

Dreyfus HL (1989) Was Computer nicht können – Die Grenzen künstlicher Intelligenz. Athenäum Verlag, Königsstein/Taunus.

Dreyfus HL, Dreyfus SE (1986) Künstliche Intelligenz: Von den Grenzen der Denkmaschine und dem Wert der Intuition. Rowohlt rororo, Reinbek (englisches Original: Mind Over Machine: The Power of Human Intuition and Expertise in the Era of the Computer. Free Press, New York).

European Commission (2024) Human Brain Project – 10 Years Assessment. Publications Office of the European Union, Luxembourg.

Future of Life Institute (2023) Pause Giant AI Experiments: An Open Letter. https://futureoflife.org/open-letter/pause-giant-ai-experiments/ [abgerufen am 2. Mai 2025].

Gabriel M (2018) Der Sinn des Denkens. Ullstein, Berlin

Hägström O (2017) Here be Dragons – Science, Technology and the Future of Humanity. Oxford University Press, Oxford.

Harari YN (2024) NEXUS: Eine kurze Geschichte der Informationsnetzwerke von der Steinzeit bis zur künstlichen Intelligenz. Penguin, München.

Hasler F (2012) Neuromythologie – Eine Streitschrift gegen die Deutungsmacht der Hirnforschung. transscript Verlag, Bielefeld.

Hesse W (1992) Können Maschinen denken – eine kritische Auseinandersetzung mit der harten These der KI. In: Kreowski HJ Hg. (1992) Informatik zwischen Wissenschaft und Gesellschaft. Informatik-Fachberichte, Band 309. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-77449-2_16

Hofkirchner W, Kreowski HJ Hg. (2021) Transhumanism – The Proper Guide to a Posthuman Condition or a Dangerous Idea?, Springer Cham, https://doi.org/10.1007/978-3-030-56546-6.

Hofstetter Y (2014) Sie wissen alles: Wie intelligente Maschinen in unser Leben eindringen und warum wir um unsere Freiheit kämpfen müssen. Bertelsmann Verlag, München.

Kreowski HJ (1998) Künstliche Intelligenz und Gehirn. In: Sandkühler HJ Hg. (1998) Repräsentation, Denken und Selbstbewusstsein, Band 20 der Schriftenreihe des Zentrums Philosophische Grundlagen der Wissenschaften, S. 193-204. Universität Bremen.

Kreowski HJ, Krieger W (2021) Künstliche Intelligenz – ‚künstlich' ja, ‚Intelligenz' wohl kaum. In: Strasser A, Sohst W, Stapelfeldt R, Stepec K Hg. (2021) Künstliche Intelligenz – Die große Verheißung, MoMo Berlin, Philosophische KonTexte, Band 8, xenomoi Verlag, Berlin, S. 259-278.

Kurzweil R (2024) Die nächste Stufe der Evolution: Wenn Mensch und Maschine eins werden. Piper Verlag GmbH, München.

Loftus R (2025) Expert dubbed 'Godfather of AI' makes scary prediction for future of humanity that could happen very soon. UNILADTech, https://www.uniladtech.com/news/ai/expert-godfather-ai-scary-prediction-humanity-threat-587253-20250101 [abgerufen am 2. Mai 2025]

McCarthy J, Minsky ML, Rochester N, Shannon CE (1955) A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html [abgerufen am 2. April 2025].

Nake F (1992) Informatik und die Maschinisierung von Kopfarbeit. In: Coy W, Nake F, Pflüger JM, Rolf A, Seetzen J, Siefkes D Hg. (1992) Sichtweisen der Informatik. Vieweg+Teubner Verlag, Wiesbaden, S. 181-201.

Precht RD (2020) Künstliche Intelligenz und der Sinn des Lebens. Wilhelm Goldmann Verlag, München.

Roland A, Shiman P (2002) Strategic Computing: DARPA and the Quest for Machine Intelligence, 1983-1993. MIT Press, Cambridge, Mass.

Shapiro EY (1983) The Fifth Generation Project – A Trip Report. Communications of the ACM 26.9 (1983): S. 637-641.

Spitzer M (2023) Künstliche Intelligenz: Dem Menschen überlegen – wie KI uns rettet und bedroht. Droemer HC, München.

Turing AM (1937) On Computable Numbers, with an Application to the Entscheidungsproblem. Proceedings of the London Mathematical Society, 2, 42 (1937), S. 230–265.

Walsh T (2018) It's Alive – Wie Künstliche Intelligenz unser Leben verändern wird. Übersetzung aus dem Englischen von Naemi und Sonja Schuhmacher, Edition Körber, Hamburg.

Weizenbaum J (1976) Computer Power and Human Reason. W.H. Freeman and Company, New York, Deutsch: Die Macht der Computer und die Ohnmacht der Vernunft. Suhrkamp Verlag, Frankfurt a. M. 1978.

three monkeys awoken

Manifest der Drei Erwachten Affen

Proklamation zur Befreiung und Wiederaneignung unserer Zukunft

I. Schöne neue Welt – Die Welt am Abgrund

Ein Gespenst geht um in der Welt. Es ist das Gespenst zunehmender Agonie, Ignoranz und Erstarrung angesichts eskalierender Mitweltzerstörung, globalen Krieges, Hungers, Vertreibung und Flucht, veitstanzendem Libertarismus, Militarismus, Autoritarismus und wiedererstarkenden Faschismus weltweit. In der gegenwärtigen Weltordnung wird der Mensch systematisch und strukturell seiner Würde beraubt und zum bloßen Objekt im unaufhörlichen Streben nach Macht und profitorientierter Kapitalverwertung degradiert – ohne Ausnahme, ohne Rückzugsorte.

Die Logik des globalisierten Kapitalismus instrumentalisiert und vernutzt den Menschen auf allen Ebenen und ignoriert seine

grundlegenden Bedürfnisse und Rechte. Krisen, Krieg, klimatische Verwüstungen, Verhetzung, Verrohung und Entsolidarisierung sind zur Norm geworden und signalisieren wie in einem Brennglas die fundamentale Krise dieser Ordnung, die den Menschen einem ausschließlich verwertungsorientierten, zunehmend technokratischen, maschinellen und entfremdenden System unterordnet.

‚Nichts sehen. Nichts hören. Nichts sagen.', einst Ausdruck konfuzianischer Weisheit und Gelassenheit im Umgang mit dem Weltgetümmel, wird diese Haltung heute zu einer, die eigene Passivität rechtfertigenden, aktiven Blockade der final erforderlichen persönlichen und gesellschaftlichen Veränderung, zu täterhafter tödlicher Erstarrung. Es ist hohe Zeit, dass die Weisheit des ‚Rückzugs aus der Niedrigkeit' durch eine Weisheit der radikalen Einmischung ersetzt wird. Inmitten eines historisch beispiellosen Wandels haben wir nicht mehr die Wahl, uns zurückzuziehen und am Flussufer sitzend darauf zu warten, bis die Leichen unserer Feinde einst im Strom an uns vorüberziehen. Denn die Welt brennt. Die Menschheit ist nicht im Frieden mit der Natur. Die Menschheit ist nicht im Frieden mit ihrer Mitwelt. Die Menschheit ist nicht im Frieden mit sich selbst. Es herrscht Krieg; alltäglicher globaler bestialischer Krieg.

Wir leben heute in einem in sein finales Stadium getretenen globalen System kapitalistischer Reproduktion, das in seiner kompetetiven Logik aus sich heraus zwingend tagtäglich Gewalt gegen das Individuum und unsere Mitwelt übt, weltweit und ohne Grenzen und Gnade; ein Wirtschafts- und Gesellschaftssystem, das längst nicht mehr zu ertragen ist. Ein System, das Krieg führen muss, um zu überleben. Über 730 Millionen Menschen sind weltweit von Mangelernährung, Hunger und Gewalt betroffen, fast 130 Millionen auf der Flucht[1]; jedes fünfte Kind auf der Welt ist unterernährt, alle 13 Sekunden stirbt ein Kind an Hunger.[2] Die kapitalistische Verwertungslogik reduziert den Menschen zunehmend offensichtlich zur bloßen Ressource und zum normierten Konsumenten von Produkten ohne realen Gebrauchswert, ohne jede Rücksicht auf die tatsächlichen menschlichen Bedürfnisse, Rechte oder gar das individuelle und kollektive (Über-)Leben.

Die Welt in ihrem heutigen Zustand ist eine Welt der Zerstörung in der die apokalyptischen Reiter entfesselt sind.

Sie ist gekennzeichnet durch einen globalen Wettlauf um Ressourcen und Macht ohne Rücksicht auf die Menschen, die Natur, die planetaren Grenzen und die langfristige Zukunft der Menschheit. Das dahinter stehende System kann bei Fortbestehen nur in einer Dystopie enden, in der die Menschheit und die planetaren Lebensgrundlagen ausgelöscht werden, weil sie ausschließlich in den Dienst unbegrenzten kompetetiven Wachstums und maximalen privatwirtschaftlichen Profits gestellt sind.

Die Menschheit kann es sich nicht mehr leisten, die Augen und Ohren zu verschließen und zu schweigen. Der Moment der radikalen Umkehr und des engagierten Einmischens ist gekommen. Jetzt oder nie mehr!

II. Über die Dialektik menschgemachter Produktivkraftentwicklung im Zeitalter Künstlicher Intelligenz

In der Geschichte der Menschheit gibt es ein Gesetz, das niemals gebrochen wurde – das ‚Gesetz der technologischen Expansion': Jede grundlegende Technologie, vom Rad bis zur Druckerpresse, von der Spitzhacke bis zum Flugzeug, von der Fotografie bis zum Internet, wird mit jedem Innovationszyklus billiger und zugänglicher – verbreitet sich unaufhaltsam. Der Mensch als ‚homo technologicus' hat diesen technologischen Prozess immer vorangetrieben. Es ist ein Gesetz der Erfindungen, das in jeder Epoche zur wirtschaftlichen Expansion geführt hat, zur Demokratisierung von Wissen und Werkzeugen. Heute steht die Menschheit erneut vor einer epochalen Zäsur, der Entwicklung zunehmend umfassender und autonomer Künstlicher Intelligenz (KI). Auch die Entwicklung der KI folgt dem Gesetz der technologischen Expansion. Was heute noch als Zukunftsvision erscheint, ist bereits im Anrollen und vielfach unbemerkt schon verbreitet Realität. KI, die auf den Prinzipien des exponentiellen Wachstums basiert, wird bereits in wenigen Jahren flächendeckend und in allen Lebensbereichen zur Verfügung stehen. Die Verbreitung dieser Technologie, die sich in zunehmend kürzeren zeitlichen Zyklen rasant verbessert, ist nicht nur eine technologische, sondern auch eine gesellschaftliche Zäsur. Die weltweite Rechenleistung wächst schneller als jede vorherige Technologie – in den letzten zehn Jahren stieg sie um ein Hundertfaches, während gleichzeitig immer mehr Systeme autonom agieren können.

Der unter ‚Digitalisierung' nur unzureichend erfasste Prozess der disruptiven Produktivkräfteentwicklung im Rahmen der vierten und fünften industriellen Revolution erfasst sämtliche gesellschaftlichen Reproduktionsverhältnisse in einem tiefgreifenden, umfassenden und beschleunigten Ausmaß, wie es historisch nur vergleichbar ist mit den Begleiterscheinungen der ersten industriellen Revolution, in deren Ergebnis die Ablösung des Feudalismus durch die kapitalistische Gesellschaftsformation stand.

Es ist unvermeidlich, dass KI wie jede andere grundlegende Technologie alle Lebensbereiche, alle Schichten der Kultur durchdringen wird: in der Kommunikation, in Forschung und Lehre, der Medizin, der Verwaltung, der Energieerzeugung, im Transportwesen und zuvorderst und treibend in der Kriegsführung. Der Übergang von KI als der fortgeschrittensten Form maschinellen Lernens hin zu einer ‚künstlichen fähigen Intelligenz' (Artificial Capable Intelligence (ACI)), die in ihrem spezifischen, klar definierten Bereich eine große Bandbreite komplexer Aufgaben selbständig bewältigen kann, ist bereits im Gange. In dieser Phase treten KI-Agenten nicht mehr nur als Assistenten auf, sondern als autonome Akteure, die Geschäftsbereiche führen, Wirtschaftszweige steuern und sogar ganze Gesellschaften beeinflussen können.

Der Weg zur ‚allgemeinen künstlichen Intelligenz' (Artificial General Intelligence (AGI)), in der Maschinen in der Lage sein werden, jede intellektuelle Aufgabe zu bewältigen, die auch ein Mensch ausführen kann, scheint nur noch eine Frage von einigen Jahren, vielleicht etwas mehr als einem Jahrzehnt zu sein.[3]

Doch wie jede andere Technologie ist auch KI nicht neutral. Wie alle Technologien ist sie abhängig von den Kräften, die sie ent-

wickeln und nutzen. Die KI hat eine neue Ära der Automatisierung eingeläutet, die das Potential hat, die (individuellen) materiellen Reproduktionsbedingungen, die Art und Weise des Arbeitens und die sozialen und auch gesellschaftlich-politischen Strukturen zu destabilisieren. KI wird zur Waffe der Desinformation, sie erzeugt Deepfakes, die schwer von der Realität zu unterscheiden sind. Diese Entwicklung wird die Möglichkeiten zur Manipulation und Kontrolle durch staatliche und nichtstaatliche Akteure massiv erweitern. Autonome Waffensysteme (AWS) und militärische KIs sind nicht länger Fiktion, sondern bereits heute auf fast allen Schlachtfeldern der Welt im EInsatz. In einer Welt, in der Maschinen nicht nur arbeiten, sondern entscheiden – auch über Leben und Tod von Menschen, geht der Verlust der menschlichen Kontrolle einher mit einer Verschiebung der Machtverhältnisse in der Gesellschaft.

Die Macht von KI-Systemen wird zunehmend auf allen Ebenen der Gesellschaft verfügbar: in den Händen von Großunternehmen, autoritären Staaten, libertaristisch autoritären Regierungen in sogenannten ‚demokratischen Staaten' und kriminellen Netzwerken gleichermaßen. Dies führt zu einem Zustand der permanenten gesellschaftlichen Unsicherheit und Verunsicherung und potentiellen Zerstörung menschlicher Beziehungen und menschlichen Lebens ganz konkret.

Technologie und KI entwickeln sich seit Jahren mit weltumspannender Wirkung, schneller als jede andere Technologie zuvor, und vor allem auch schneller als unser individuelles und kollektives Bewusstsein – vom kollektiven Unbewussten ganz zu schweigen. KI wird nicht nur als Werkzeug und Hilfsmittel zu Fortschritt und Verbesserung von Wissensvermehrung, Forschung, Medizin und Bildung genutzt, sondern wird in Form von KI-gesteuertem Kriegsgerät und AWS zum eigen- und verselbständigten Machtinstrument, das die Kriegslogik und -maschinerie weiter anheizt, während die Profiteure des Militärisch-Industriellen-Komplexes mit ihren Kumpanen des Digital-Industriellen-Komplexes und ihren kriegstreibenden Steigbügelhaltern in Politik und Medien eine Aktienhausse nach der nächsten feiern, bis zum finalen Säckeplatzen.

In einem System, das ausschließlich auf privatwirtschaftliche Profitmaximierung und Machterhalt orientiert, bedroht die KI mittlerweile die Fundamente menschlicher Existenz. Die Büchse der Pandora ist sperrangelweit geöffnet: Statt die neuen Technologien der vierten und fünften industriellen Revolution und ihre Entwicklung in den Dienst der Menschheit und ihres nachhaltigen Überlebens als Spezies zu stellen, werden sie im wahrsten Sinne des Wortes zu Waffen der Entwertung und Vernutzung der planetaren Ressourcen, des Lebens im Allgemeinen und des Menschen im Besonderen, zu Instrumenten der Sicherung der Macht der Wenigen über das Leben der Vielen, der Erhaltung eines Wirtschafts- und Gesellschaftssystems, das mit historisch zwingender Logik auf seine finale menschheitsvernichtende Implosion zustrebt, wenn den Herrschenden nicht umgehend in den Arm gefallen wird.

In einer Zeit, in der die Auseinandersetzung um die begrenzten planetaren Ressourcen zunehmend wieder militärischer Logik als der Fortsetzung der Politik mit anderen Mitteln unterworfen wird; in einer Zeit, in der in zeitlich zunehmend kurzfristigen Zyklen technologischer Fortschritt und militärische Aufrüstung Hand in Hand gehen, und in einer Zeit, in der global agierende Tech-Konzerne über faktisch mehr Kapital und gesellschaftlichen Einfluss verfügen als die meisten Nationalstaaten der Welt, steht die Menschheit an einem Scheideweg:

Werden wir die Produktivkraftentwicklung nutzen, um die planetaren Lebensgrundlagen zu schützen und ein gutes Leben für alle Menschen zu ermöglichen – oder werden wir uns von den Zauberlehrlingen der KI und ihren Technologien (weiter) beherrschen lassen?

> *„Ob sie es zugeben oder nicht, die Erfinder der KI sind selbst geopolitische Akteure, und ihre Souveränität über die KI festigt die entstehende ‚technopolare' Ordnung weiter – eine Ordnung, in der Technologieunternehmen in ihren Bereichen die Art von Macht ausüben, die früher den Nationalstaaten vorbehalten war. (…) Wir haben eine technologische Ordnung, die wirklich eine globale Ordnung ist, mit geopolitischer Macht, die zählt. Und die Hauptakteure in dieser Ordnung sind Technologieunternehmen."*[4]

so Mustafa Suleyman, CEO und Mitbegründer von Inflection AI und DeepMind, zwei der weltweit führenden Unternehmen im Bereich der Entwicklung von KI; ein Mann also, der weiß, wovon er spricht.

III. Geister, die ich rief, werd´ ich so nicht los

Zunehmend wird auch vielen politisch Verantwortlichen die Dramatik der Situation bewusst. Anhörungen von Tech-Milliadären vor dem US-Senat[5], in denen festgestellt wird, dass diese ‚Blut an den Händen' haben, es aber keine gesetzliche Grundlage dafür gäbe, sie in ihrem Treiben zu stoppen, der am 1. August 2024 in Kraft getretene AI-/KI-act der Europäischen Union und auch die Resolution 78/2416[6] – die erste Resolution zu autonomen Waffensystemen in der Generalversammlung der Vereinten Nationen, vom 22. Dezember 2023, stellen klägliche Versuche dar, innerhalb des bestehenden Systems eben jene Dynamik aufzuhalten, die selbst einerseits Ergebnis als auch andererseits Antriebsriemen genau der kritisierten und zu Recht als bedrohlich erkannten Entwicklung ist, ein Unterfangen dem gegenüber die Quadratur des Kreises als einfache Denksportaufgabe erscheint. Das ist auch der tatsächliche Grund dafür, weshalb die seit über 10 Jahren in Genf bei den Vereinten Nationen im Rahmen der Konvention über bestimmte konventionelle Waffen (Convention on Certain Conventional Weapons (CCW)) laufenden Verhandlungen zu den ‚Tödlichen Autonomen Waffensystemen' (Lethal Autonomous Weapon Systems (LAWS)) stocken und festgefahren sind.

> *„Dass die Verhandlungen zu den von KI angetriebenen autonomen Systemen getrennt nach militärischen und zivilen Anwendungen geführt werden, hilft einerseits, die Ängste der Bevölkerung auf wirtschaftliche und soziale Anwendungen zu fokussieren. Gleichzeitig trägt dies jedoch dazu bei, dass die erträumten Vorteile noch stärker überschätzt werden, weil die militärischen Anwendungen taktisch ausgeblendet und ausgelagert werden."*[7]

Der final gescheiterte Versuch der Kontrolle des atomaren Wettrüstens und die zunehmende Hybris der Herrschenden, die bereits wieder ernsthaft und öffentlich über die ‚Führbarkeit von Atomkriegen' nachdenken und diese sogar konkret zu planen beginnen, sind der letzte Beweis dafür, dass unter kapitalistischen Reproduktionsbedingungen die Produktivkraftentwicklung nicht der Förderung friedlichen Miteianders, nachhaltiger Entwicklung und eines guten Lebens für die Menschheit, sondern am Ende immer zugunsten des maximalen Profits, für Krieg und Vernichtung dient; so wie es Karl Marx schon vor über 160 Jahren festgestellt hatte:

> *„Das Kapital hat einen Horror vor Abwesenheit von Profit oder sehr kleinem Profit, wie die Natur vor der Leere. Mit entsprechendem Profit wird Kapital kühn. Zehn Prozent sicher, und man kann es überall anwenden; 20 Prozent, es wird lebhaft; 50 Prozent, positiv waghalsig; für 100 Prozent stampft es alle menschlichen Gesetze unter seinen Fuß; 300 Prozent, und es existiert kein Verbrechen, das es nicht riskiert, selbst auf Gefahr des Galgens."*[8]

Statt der nach der Implosion der Sowjetunion und des mit ihr verbundenen Warschauer-Vertrags-Systems beschworenen ‚Ernte einer Friedendividende' erleben wir seit über dreißig Jahren und angesichts der fortschreitenden Mensch gemachten Klimakrise eine zunehmend abnehmende internationale Kooperation wider besseres Wissen, eine immer umfassendere und brutalere Militarisierung internationaler Beziehungen und daraus folgende weltweit eskalierende Kriege, Hungerkatastrophen, Flucht und Vertreibung.

Doch nicht einmal die gescheiterten Versuche der Atomwaffenkontrolle und der Begrenzung von deren Weiterverbreitung, können als Modell für die Eindämmung der drohenden Gefahren durch KI dienen, da die Unterschiede zwischen diesen beiden Technologien grundlegender nicht sein könnten; insofern ist auch die Beschreibung des aktuellen Zustandes als ‚Oppenheimer-Moment unserer Generation' (Alexander Schallenberg, österreichischer Außenminister bei der Eröffnung der Wiener Konferenz zu autonomen Waffensystemen am 29./30.04.24), den es jetzt zu nutzen gälte, um zu verhindern, dass AWS schon bald überall auf der Welt verfügbar seien, grob irreführend. Atomwaffen sind extrem kapitalintensiv, erfordern spezifisches technologisches Wissen und den Zugang zu gefährlichen und schwer zu beschaffenden Materialien wie Uran-235. Allein diese Hürden haben zumindest für den Zeitraum einer Generation und in gewissem Maße verhindert, dass Atomwaffen in die Hände von unkontrolliert vielen und auch nichtstaatlichen Akteuren gelangten. Im Gegensatz dazu ist die Entwicklung von KI auf einem völlig anderen Weg. Sie basiert zum größten Teil auf Open-Source-Code, und ist mit dem notwendigen Know-How für Viele auf einfache Weise zugänglich, verteilbar und weiter zu entwickeln. Im Internet stehen die nötigen Daten und Technologien praktisch jedem zur Verfügung. Dadurch gibt es kaum Grenzen für ihre Verbreitung. KI ist keine Technologie, die nur in den Händen der mächtigen Nationen, Nationalstaaten oder Konzerne bleibt. Sie ist jedem zugänglich und wird sich ohne größere Hindernisse immer weiter ausbreiten.

Die disruptive Kraft der KI-getriebenen Technologieentwicklung hin zu einer AGI wird die Welt innerhalb kürzester Zeit verändern. Ihre Auswirkungen werden nicht nur das Leben der Menschen prägen, sondern auch die Gesellschaften und Wirtschaften weltweit umkrempeln. Der Fortschritt bei der Entwicklung der KI-Technologie hin zur AGI geht so schnell voran, dass die bestehenden politischen und gesetzlichen Strukturen nicht in der Lage sind, mit diesem Tempo Schritt zu halten.

Schon die Erfahrung mit der am Ende gescheiterten Kontrolle von Atomwaffen zeigt, dass die destruktiven Potentiale moderner Technologien in einer globalisierten kapitalistischen Gesellschaftsformation nur zeitweise und begrenzt einzudämmen sind – die KI wird jedoch noch viel schwieriger zu bändigen sein.

Es reicht nicht, auf Abschreckung zu setzen oder nur einzelne Akteure zur Verantwortung zu ziehen. Es braucht eine völlig neue Herangehensweise, bei der alle in die Verantwortung genommen werden, bevor es zu spät ist.

IV. Zwei mögliche Pfade: Untergang oder Befreiung

Die Reiter der Apokalypse sind bereits unterwegs. Die Dystopie ist bereits in Entstehung. Sie zeigt sich in einer Welt, in der die technologische Entwicklung nicht im Interesse der Menschheit, sondern fast ausschließlich zur Aufrechterhaltung und Verstärkung der bestehenden Herrschaftsverhältnisse genutzt wird. AWS, umfassende und zunehmend filigrane Überwachungsmechanismen, Social-Scoring und die vollständige Kontrolle durch künstliche Intelligenzen werden in einer Welt herrschen, in der die Menschen als bloße Verfügungsmasse für die Interessen der wenigen Herrschenden dienen, und wenn sie nicht mehr in der Mehrwertproduktion vernutzt werden können, als ‚kapitalistische Überbevölkerung' dem Massaker preisgegeben werden. Dies betrifft aktuell die so als ‚überflüssige Bevölkerung' identifizierten und abqualifizierten Menschen im Gazastreifen, im Jemen, in der Subsahara und weiten teilen Lateinamerikas. Für diese ist im kapitalistischen Weltsystem kein Platz (mehr), und sie werden durch Kriege und Massaker immer weiter dezimiert, genau wie dies bei allen anderen Kriegen und Völkermorden in anderen Ländern bereits der Fall war. Konsequenterweise richtet sich dann auch genau gegen diese Menschen als Flüchtende die zunehmend militärische Abschottung der USA und der Festung Europa. Dieser rein verwertungsorientierte eleminatorische Zustand ist der wahre Kern und die einzige Perspektive die der Kapitalismus trotz aller diplomatischen Floskeln bietet.

Diese bereits akute Dystopie kann nur durch einen radikalen Bruch mit dem kapitalistischen System der privaten Konkurrenz und des grenzenlosen Wachstums verhindert werden. Um den Planeten vor seiner Zerstörung und die Menschheit als Gattung vor der Ausrottung zu bewahren, müssen wir die Macht des Kapitals brechen und den Weg für eine neue, solidarische Gesellschaft öffnen, die die Kreativität des Menschen, seine konstruktiven Potentiale, seine Resonanz- und Liebesfähigkeit wertschätzt, fördert und zur Entfaltung bringt und nicht zuletzt die Technologien der Zukunft zum Wohle aller nutzt; zum Schutz der planetaren Ressourcen, dem Erhalt unserer Mitwelt, zur Befriedigung der menschlichen Bedürfnisse und für ein gutes Leben für Alle.

Die Utopie, die wir anstreben, ist eine Gesellschaft, in der die freie Entwicklung eines jeden Einzelnen als die Bedingung für die freie Entwicklung aller tatsächlich garantiert ist, eine Gesellschaft, in der Technologien im Dienst der Menschheit und der planetaren Lebensgrundlagen stehen; eine Welt, in der KI nicht als Waffe zur Kontrolle und Vernichtung genutzt wird, sondern zur Förderung des Wissens und der kollektiven Entfaltung aller Menschen. In dieser Utopie wird die technische Entwicklung nicht als Selbstzweck betrieben, sondern als Mittel zur gerechten Verteilung von Ressourcen, zur Befreiung der Menschheit von den Fesseln der Entfremdung und Ausbeutung.

Doch dieser Wandel kann nur durch einen finalen Bruch mit dem kapitalistischen Reproduktionsregime und seiner kompetetiven Wachstumslogik geschehen. Es reicht nicht, die bestehenden Verhältnisse zu reformieren – die Verhältnisse müssen radikal überwunden werden. Nur so können die destruktiven Potenziale der Technologien ausgeschaltet und ihre konstruktiven Potenziale in Kräfte im Dienste der Menschheit, ihrer Mitwelt und des Planeten wirksam gemacht werden.

V. Vier Mindestbedingungen zur Verwirklichung einer menschlichen Zukunft

- **Radikale Transformation der Produktionsverhältnisse:**
  Der Kapitalismus muss durch eine neue Gesellschaftsordnung ersetzt werden, die auf Solidarität, Kooperation und dem Wohl aller basiert. Die Anhäufung und Aneignung privaten Profits darf nicht länger das Hauptziel der Gesellschaft sein. Stattdessen müssen die Produktionsmittel kollektiv genutzt werden, um die Bedürfnisse aller Menschen zu decken und die planetaren und ökologischen Grundlagen des Lebens zu bewahren.

- **Globale Kooperation und gerechte Verteilung:**
  Wir müssen die Ressourcen der Erde gerecht verteilen und die internationale Zusammenarbeit und Kooperation stärken, um den existentiellen globalen Herausforderungen wie Klimawandel, Krieg, Hunger und Armut zu begegnen. Diese Aufgabe kann nur gelingen, wenn die gesamte Menschheit zusammenarbeitet, um die Bedürfnisse aller zu befriedigen, statt in Konkurrenz zueinander zu stehen.

- **Gesellschaftliche Kontrolle der Technologien:**
  KI und Technologieentwicklung dürfen nicht weiter in den Händen weniger Konzerne und Privatpersonen verbleiben, die sie ausschließlich zu Zwecken der sozialen Kontrolle, Ausbeutung und Profitmaximierung einsetzen. Es muss eine global organisierte demokratische Kontrolle über Entwicklung und Einsatz dieser Technologien geben, um sicherzustellen, dass sie im Interesse der gesamten Menschheit und nicht einer privilegierten Minderheit eingesetzt werden.

- **Ethik und Sicherheit in der KI-Entwicklung:**
  KI darf nicht weiter zum Werkzeug der Unterdrückung werden. Sie muss so entwickelt werden, dass sie ethischen Prinzipien folgt und in einer Weise arbeitet, die der Menschheit dient. Die technisch gesicherte Implementierung von Sicherheitsmechanismen und ethischen Leitlinien sind notwendig, um sicherzustellen, dass AGIs niemals gegen die Interessen der Menschen agieren können. Es muss sichergestellt werden, dass die KI am Ende nicht verhindern kann, dass der Mensch ihr den Stecker zieht.

An diesen vier Mindestbedingungen muss sich jedes politische Konzept ab sofort messen lassen. An diesen vier Mindestbedingungen werden wir jedes politische Konzept messen. Wer sich diesen vier Mindestbedingungen verweigert, ist Teil des Problems und nicht Teil der Lösung.

VI. Wer, wenn nicht wir?! Wann, wenn nicht jetzt?! Aufruf zur direkten Aktion

Der Zeitpunkt des Abwartens ist vorbei. Es ist Zeit, die Augen und die Ohren zu öffnen, das Maul aufzureißen und zu handeln. Die Welt steht am Wendepunkt, und nur ein umgehender und radikaler Bruch mit der kapitalistischen Wachstumslogik kann den Planeten und die Menschheit noch vor dem Untergang retten. Es gibt keinen Frieden im und mit dem ‚sozialen Frieden' der Herrschenden.

Die Technologien der Zukunft dürfen nicht weiter der destruktiven Profitgier global agierender Multis, einzelner Tech-Milliardäre, der Kriegsprofiteure und deren Politiker:innendarsteller:innen geopfert werden.

Die Technologien der Zukunft können uns dienlich sein in unserem Kampf um Befreiung, auf unserem Weg zu einer gerechten und solidarischen Welt, zur Rettung des Planeten – aber nur, wenn wir jetzt handeln und sie den Händen derer entreißen, die nur ihr kurzfristiges und beschränktes eigenes Wohl im Blick haben.

Lasst uns zusammenstehen! Lasst uns die planetare Zerstörung, Kriegshetze, Verhetzung und Verrohung aufhalten und eine gemeinsame gute Zukunft für die Menschheit aufbauen, die im Einklang mit den Bedürfnissen aller und auch denen unserer Mitwelt steht!

three monkeys awoken

Die Welt gehört nicht den Herrschenden, die sie in den Abgrund führen.

Die Welt gehört den Menschen, die sie befreien werden.

Wer sich weiterhin in Agonie, Passivität und Erstarrung flüchtet, wird zum Teil des Problems und nicht der Lösung. Sei Teil der Lösung!

Der Kampf beginnt jetzt!

Gezeichnet
three monkeys awoken

Anmerkungen

1 *https://www.uno-fluechtlingshilfe.de/informieren/fluechtlingszahlen; 10.11.24; 09:14*
2 *https://www.aktiongegendenhunger.de/hungerbekaempferin-werden?utm_source=bing&utm_medium=cpc&utm_campaign=generic-de&utm_term=kinder%20hunger&msclkid=afc53675c06f1aeb10ec5145ab6f526e&utm_content=KW_DE_de_Hunger; 10.11.24, 09:15*
3 *Vgl. What is Artificial Capable Intelligence (ACI) – Artificial Capable Intelligence: A Stepping Stone on the Path to Artificial General Intelligence?*
4 *The AI Power Paradox – Can States Learn to Govern Artificial Intelligence—Before It's Too Late? By Ian Bremmer and Mustafa Suleyman in: foreign affairs September/October 2023 (eigene Übersetzung)*
5 *https://www.wiwo.de/unternehmen/it/wie-oelbarone-und-eisenbahn-tycoons-us-parlament-geisselt-eigene-tech-konzerne/26251422.html ; 10.11.24; 10:01*
6 *https://www.bing.com/search?q=die+Resolution+78%2F241&cvid=ec023fe0904242ddad 1209cd61307b03&gs_lcrp=EgRlZGdlKgYIABBFGDkyBggAEEUYOTIHCAEQ6QcYQDIICAIQ6QcY_FXSAQg1MDEwajBqNKgCALACAA&FORM=ANAB01&PC=U531; 10.11.24; 10:12*
7 *E. Gillen; KI für das Militär braucht keine Sondermoral!; in: Ethik und Militär, 01/2024; S. 24f; S. 24; https://www.ethikundmilitaer.de/ethik-und-militaer-kontroversen-in-militaerethik-sicherheitspolitik; 10.11.24; 10:17*
8 *MEW, Bd. 23, S. 788, in MEGA² II/6, S. 680/681*

Marie-Theres Tinnefeld

Streitfrage Antisemitismus und Wege des Friedens

Überlebensfragen

Am 7. Oktober 2023 überfielen hunderte Hamas-Terroristen Israel. Sie verletzten, vergewaltigten und kidnappten zahlreiche israelische und ausländische Frauen, Männer und Kinder. Daraufhin begann das israelische Militär einen bis heute andauernden Zerstörungskrieg im Gaza-Streifen und neuerdings auch im Libanon. Unter den vielen Kritikern dieses Krieges befinden sich der inzwischen verstorbene Überlebende des Holocaust, der Politiker und Verteidiger der Menschenrechte Stéphane Hessel sowie sein kürzlich verstorbener Freund, der große liberale Politiker und Verteidiger der Menschenrechte Gerhart Baum. Ebenfalls gehören zu den Kritikern der Philosoph Omri Boehm, der Journalist Ronen Steinke und der Historiker für jüdische Religion und Geschichte Michael Brenner.

Infolge der Ereignisse in Israel und Gaza hat die Zahl antisemitischer Übergriffe weltweit zugenommen. Eine solche Entwicklung schien zwar nach dem Holocaust mit seinen unsäglichen industriellen Vergasungsanlagen in Auschwitz nicht mehr vorstellbar zu sein, soziale Diskriminierungen und Gewalt gegen Jüdinnen und Juden nehmen aber auch in Deutschland online und offline erheblich zu.

Die Ärztin und Psychotherapeutin Eva Umlauf hat mit ihrer Mutter und Schwester als Kind Auschwitz überlebt, der Vater wurde ermordet. Sie steht für eine vielstimmige und inklusive Kultur des Erinnerns, die von ihrer Identität als Jüdin nicht zu trennen ist (Eva Umlauf mit Stefanie Oswalt, Die Nummer auf deinem Unterarm ist blau wie deine Augen, Erinnerungen 2024). Die Erfahrungen von Eva Umlauf führen zu den Fragen: Welche Bedeutung haben Religion, Ethnie oder Kultur, die selbstbestimmte Wahrnehmung, jüdisch zu sein oder zu leben? Oder geht es um den Blick der anderen, der in der Perversion der Nürnberger Rassengesetze einen Höhepunkt fand. Haben nicht „Rassisten" immer wieder jüdische Prototypen gezeichnet?

In der jüdischen Kultur hat Bildung – so Umlauf – extrem hohen Wert. Sie hat etwa zu zahlreichen jüdischen Nobelpreisträgern bzw. -trägerinnen geführt: Juden stellen etwa 2 % der Weltbevölkerung, aber bemerkenswerte 23 % der Nobel-Preisträger. Lassen sich als Ursache der massiven neuen Angriffe nicht auch Neid gegenüber derart erfolgreichen jüdischen Positionen vermuten?

Antisemitismus: Unterstellungen?

„Das Teuflische hallt nach": Unter diesem Titel lädt Israel nach einem Bericht der SZ vom 26. März 2025 (Politik S. 7) zu einer Konferenz gegen Antisemitismus in Israel ein, an der überwiegend Rechtsradikale aus Europa teilnehmen. Aus diesem Grund haben viele Andersdenkende wie etwa der berühmte französische Philosoph Bernhard-Henry Lévy seine ursprünglich geplante Teilnahme abgesagt. Sind es doch gerade die rechtspopulistischen Parteien, aber auch Vertreter der radikalen linken Szene, die für ihren notorischen Judenhass bekannt sind bzw. waren. Die europäischen Nationalisten, die sich mit Gleichgesinnten auf der ganzen Welt verbünden, sind nicht nur gefährlich, weil sie ihre antisemitischen Wurzeln verleugnen, sondern auch weil sie rechtsstaatliche Einrichtungen (u. a. unabhängige nationale und internationale Gerichte), das humanitäre Völkerrecht (internationaler Strafgerichtshof in Den Haag) und die eu-

ropäische Aufklärung (Meinungs- und Pressefreiheit) verachten. Dem angesehenen Wissenschaftler Omri Boehm wird aufgrund seiner israelkritischen Äußerungen Inkompetenz und wohl auch eine antisemitistische Haltung unterstellt (*https://www.welt.de/kultur/article255904888/Omri-Boehms-ungehaltene-Buchenwald-Rede-Wie-bitte-Israel-soll-eine-entmenschlichte-Gesellschaft-sein*).

Die Frage „Ist Israel-Kritik zulässig und wenn ja, wie viel?" Diese Frage wurde besonders deutlich anlässlich der Veröffentlichung einer Karikatur des israelischen Premiers Netanjahu in der SZ im Jahr 2018, die ein bekannter Zeichner geschaffen hatte (zum Fall: Knieper, Tinnefeld: *Politische Satiren und Karikaturen – eine Bastion offener Demokratie?*, in DuD 20, S. 375-380). Die Darstellung wurde von jüdischer Seite als antisemitisch bezeichnet, der Künstler fristlos entlassen. Die Auswirkungen auf das Lebenswerk des Künstlers und seine Person waren erheblich. Nach Maßstäben grundrechtlich geschützter meinungsbetonter journalistischer Darstellungsformen im Rahmen der Kunst- und Medienfreiheit war der Vorwurf unberechtigt, der Zeichner wurde zwar rehabilitiert, sein verfassungsrechtlich geschütztes Persönlichkeitsrecht blieb beschädigt.

Kunst existiert nicht in einer Art idealisiertem Vakuum. Insbesondere satirische, überzeichnende Darstellungen sind geeignet, sich mit Ideologien und Sachzwängen auseinanderzusetzen. Wichtig ist dabei aber immer der Bezug zur Realität. Die Zeichnungen sollten einen wahren Aussagekern haben. Bei der Umsetzung und Verwendung von Hybridfiguren, Symbolen (Davidstern), Allegorien (Feigenbaum), Porträtdarstellungen (große, abstehende Ohren) ist der Zeichner frei in der Gestaltung. Die Karikatur kann als gezeichneter, übertriebener, spöttischer, verzerrter Kommentar politische Handlungen und Prozesse begleiten und damit politische Meinungs- und Willensbildung stärken.

Ist nicht berechtigte Kritik an der Netanjahu-Regierung gegenüber den Palästinensern konform mit der Meinungs-, Kunst- und Pressefreiheit in einer rechtsstaatlich verankerten Demokratie? Ist nicht ein Eingriff in die Meinungs- und Kunstfreiheit zu bejahen, wenn sie in belastender Weise oder faktisch in erheblicher Weise behindert wird?

Auch wenn die Meinungs- und Kunstfreiheit grundsätzlich weit zu verstehen ist, so mussten Bilder auf der Documenta 15 in Kassel 2022 eindeutig als Skandal angesehen werden. Die Darsteller benutzten unheilvolle Stereotypen und unterstellten negative Charakterzüge mit jüdischen Bezügen. Auf der Documenta wurde unübersehbar antisemitische Kunst ausgestellt, die eine Debatte über die Meinungs- und Kunstfreiheit sowie über die Grenzen kommunikativer Freiheitsrechte auslöste.

Menschenwürde, Freiheit, Gleichheit, Privatheit und Datenschutz

Der Königsberger Philosoph Immanuel Kant, dessen 300. Geburtstag 2024 gefeiert wurde, sagte sinngemäß, dass er jeden Angriff auf die Menschenwürde eines Menschen irgendwo auf der Welt so empfinde, als würde er selbst davon betroffen sein. Die Menschenwürde verkörpert den Kerngehalt global gültiger Menschenrechte und trägt dem Schutz vor der Überschreitung letzter Grenzen, wie etwa dem Verbot der Folter, Rechnung. Diese Einschätzung verweist auf die Erklärung der Allgemeinen Menschenrechte der UN von 1948, die Europäische Menschenrechtskonvention von 1950 und die Grundrechte-Charta der Europäischen Union von 2009. In den Menschenrechtserklärungen findet sich jeweils ein Schutz vor Diskriminierungen, der unter anderem auch Aufnahme in die Datenschutzgrundverordnung der EU gefunden hat.

Der Datenschutz ist für die Meinungs- und Pressefreiheit wie auch für die Demokratie essenziell, weil er eine geschützte Umgebung und ein Recht auf Privatheit schafft, in der Menschen ihre Gedanken und ihre Kunst ohne Angst vor Repressalien äußern können. In historischen Umbruchzeiten besteht immer auch ein besonderes Interesse an Gärten und Parks. Sie erfüllen ein zutiefst menschliches Bedürfnis nach privater Lebensgestaltung. Zahlreiche Menschen, die in Regimen des Nationalsozialismus oder in anderen Diktaturen verfolgt wurden, haben den Garten als einen Freiraum der persönlichen Entfaltung erlebt (Tinnefeld, Überleben in Freiräumen, 2018).

Der Schutz von Privatheit und sensiblen (besonderen) persönlichen Daten wird durch Diskriminierungsverbote verstärkt, wonach niemand wegen seiner ethnischen Herkunft, Religion und anderer Kriterien benachteiligt werden darf. Darunter fallen auch Unterstellungen negativer Eigenschaften, die der Antisemitismus Juden und Jüdinnen zuschreibt, die häufig auch durch KI gesteuert werden. Die Datenschutzgrundverordnung gewährleistet den betroffenen Personen u. a. Auskunftsrechte und sieht starke Sanktionen vor, insbesondere qualifizierte Geldstrafen.

Es sind wesentliche Fragen, die sich im Sinne des berühmten Volkszählungsurteils des Bundesverfassungsgerichts von 1983 auf das Recht gründen, die eigene Persönlichkeit frei entfalten und sich als jüdisch, muslimisch oder christlich wahrnehmen zu können. Und das kann nur im Austausch mit anderen gelingen, die nicht von Hass und Vorurteilen bestimmt sind. Eingriffe in Privatheit und Datenschutz, die Missachtung von Diskriminierungsverboten werden zunehmend von den Verteidigern der Menschenrechte als das charakterisiert, was sie sind: nämlich Angriffe auf die europäische und globale Friedensordnung.

Marie-Theres Tinnefeld

Prof. Dr. **Marie-Theres Tinnefeld** ist Juristin und Publizistin, mit zahlreichen Konferenzen und Veröffentlichungen im In- und Ausland zum Thema *Informationsrecht und europäische Rechtskultur*. Sie ist Mitglied im Beirat des FIfF e. V.

Unbedingte Absage an jede Diskriminierung von Jüdinnen und Juden

Die seit Zeiten der Aufklärung geforderte Gedanken-, Meinungs-, Kunst- und Pressefreiheit ist das eine, was heute im Kontext israelbezogener Kritik auf dem Spiel steht. Die andere Ebene betrifft die psychischen und tätlichen Angriffe auf jüdische Mitbürgerinnen und Mitbürger, wie sie Eva Umlauf überzeugend erfahrbar macht.

Die Singularität der Judenmorde kann und darf nicht relativiert werden! Der Anspruch ist in dem Satz „Die Menschenwürde ist unantastbar" formuliert. Die Menschenwürde ist eigenständiger Grund der Menschenrechte und wird insbesondere durch Zonen von Privatheit und Datenschutz geschützt. In den Bereich unverfügbarer Menschenrechte reichen Diskriminierungsverbote hinein, die für Empathie und Solidarität mit Menschen stehen, die von antisemitischen Attacken bedroht sind. Empören wir uns dagegen! (Stéphane Hessel, Empört Euch!", aus dem Französischen von Michael Kogon, 34. Auflage 2024).

Der deutsch-israelische Philosoph Omri Boehm spricht davon, dass der Humanismus der Nachkriegszeit auf dem Prüfstand steht (FAZ v, 27.03.2025, Feuilleton, S. 12). Er mahnt die Grundsätze des Philosophen Kant an, die dieser in seiner Schrift *Zum ewigen Frieden* 1795 niedergelegt hat. Barbarische Handlungen in bewaffneten Konflikten bergen die Gefahr – so Kant –, dass sie zu Ausrottungskriegen werden. Diese wurden nach dem Zweiten Weltkrieg als Reaktion auf die unsagbaren Grausamkeiten des Holocaust gesetzlich verboten und verletzen das humanitäre Völkerrecht. Soll, muss nicht etwa auch in der Palästinenserfrage „das Ideal des Friedens der Ursprung menschlicher Beziehungen, menschlicher Politik und menschlichen Rechts" sein? (Omri Boehm, Das Gegenteil des Vergessens, SZ v. 07.04.2025, Feuilleton, S. 11; s.a. Hessel, a. a. O., S. 16 ff.).

Jeanette Hofmann

Desinformation: nicht Unkenntnis, sondern politische Verortung

Die Debatte über Desinformation auf Social Media geht am Kern des Problems vorbei, sagt die Politikwissenschaftlerin Jeanette Hofmann. Sie lenkt den Blick auf die Schwächen gesellschaftlicher Narrative, den Umgang der Massenmedien mit heimischen Populisten und die Tatsache, dass Desinformation auch Gemeinschaft stiftet.

Im Kontext des Superwahljahres 2024 war kaum ein Thema so präsent wie der Einfluss von Desinformation auf die Demokratie. Die Ängste davor wurden mit Forderungen an Social-Media-Plattformen verknüpft, uns zum Beispiel vor ausländischem Einfluss zu schützen. Wir sprachen mit der Politikwissenschaftlerin und Weizenbaum Principal Investigator Jeanette Hofmann über Desinformation als Symptom von Demokratieverfall und was das mit der Konkurrenz von neuen und alten Medien zu tun hat. Ein Gespräch über ein Hype-Thema, das am Kern des Problems vorbei geht.

Frage: *Wie Sie wissen, haben wir in der Redaktion des Weizenbaum Instituts gerade einen Fokus auf das Verhältnis von Digitalisierung und gesellschaftlicher Polarisierung gelegt. Wir freuen uns, dass wir dazu mit Ihnen sprechen können. Wie blikken Sie als Politikwissenschaftlerin auf das Thema Zusammenhalt in der vernetzten Gesellschaft?*

Jeanette Hofmann: Aus politikwissenschaftlicher Sicht fragt man sich unwillkürlich, wogegen sich die Rede vom gesellschaftlichen Zusammenhalt richtet bzw. auf welches Problem sie antwortet. Es ist kein Zufall, dass wir vermehrt über die Bedingungen gesellschaftlichen Zusammenhalts in einer Zeit nachdenken, in der uns viele Nachkriegsinstitutionen fragil erscheinen und ihre Zukunft nicht länger selbstverständlich ist. Dazu gehören die Demokratie als weithin anerkannte Regierungsform, die Wettbewerbsfähigkeit der Wirtschaft, aber auch die öffentliche Sphäre als Ort der Meinungs- und Willensbildung.

Gegenwärtig beobachten wir einen Vertrauensverlust in die Leistungsfähigkeit von Demokratie, Staat und Wirtschaft, der uns vor Augen führt, dass selbst die nähere Zukunft alles andere als ein Selbstläufer ist. In diesem Sinne ist der Begriff des gesellschaftlichen Zusammenhalts mit mehreren Bedeutungen aufgeladen: er zeigt einen potentiellen Mangel auf und ist somit diagnostisch, er signalisiert einen gesellschaftlich wünschbaren Zustand und ist daher normativ und schließlich appelliert er an unsere Erfahrung mit und die Fähigkeit zur Solidarität; in diesem Sinne ist er auch aspirativ oder zukunftsstiftend.

Aktuell wird sehr viel über Desinformationen im Kontext von gesellschaftlichem Zerfall gesprochen. Sie kritisieren jedoch diese Debatte. Warum?

Mich interessiert die Frage, warum wir Desinformation derzeit so viel Beachtung schenken. Wenn man sich mal erinnert, der Begriff ist erst vor knapp zehn Jahren in der öffentlichen Diskussion aufgetaucht. Wenn man sich nun mal anguckt, welche Zeitschriften etwa beim Friseur herum liegen: die sind voller Desinformation. Wir leben seit Jahrzehnten mit Zeitschriften und Textsorten, die darauf spezialisiert sind, Desinformation zu verbreiten, ohne dass wir das als Bedrohung der Gesellschaft wahrgenommen haben. Solange es um Königsfamilien und Schauspieler:innen geht, darf offenbar gelogen werden, so viel man will.

Das hat sich mit der US-Wahl und dem Brexit-Referendum 2016 dann plötzlich geändert. Das waren zwei Ereignisse, von denen man erwartet hatte, dass sie anders ausgehen, als sie tatsächlich ausgegangen sind, und hat dann nach einer guten Erklärung dafür gesucht. Und in diesem Zusammenhang tauchte das Narrativ auf, dass Russland und China in politische Entscheidungen intervenieren und dass sie das mit Hilfe von Desinformation tun.

Das wiederum bedient ein Narrativ, das sehr stark auch von den alten Massenmedien befeuert wird, nämlich dass die Welt außerhalb des editierten Journalismus gefährlich, schlecht und manipulativ ist. Diese neuen Plattformen sind eine wirkliche Konkurrenz und eine Bedrohung für die alten Medien, weil sie ihr Geschäftsmodell zerstört haben. Das mag mit erklären, warum die Berichterstattung häufig nicht neutral gegenüber Plattformen ist. Und so werden soziale Netzwerke ganz im Sinne von „blaming the messenger" für Desinformation verantwortlich gemacht, obwohl gar nicht so viel dafür spricht.

Eine große internationale Langzeitstudie zur Entwicklung der Demokratie[1] zeigt, dass Desinformation vor allem in den Ländern verbreitet ist, in denen populistische Politiker:innen einflussreich sind und die Demokratie in autokratische Regierungsformen kippt, also beispielsweise in den USA, in Ungarn, in Polen lange Zeit, in Brasilien und Großbritannien. Also dort, wo die Demokratie fragil ist und entweder die Regierungspartei oder die Opposition sich des Mittels der Desinformation bedient und es keine wirksame Form der Gegenwehr oder der Rechenschaftspflichtigkeit gibt.

Obwohl sie sicher zur Desinformation beitragen, sind also nicht die Plattformen die wirkliche Gefahr, sondern es sind häufig Regierungsparteien oder wichtige Oppositionsparteien, die einflussreiche Produzierende von Desinformationen sind.

Desinformation ist also ein Anzeichen von demokratischem Verfall. Wie zeichnet sich dieser aus?

Meine Arbeit versucht aktuell das Phänomen der Desinformation einzubetten, einerseits in die Forschung zu Democratic Backsliding, also der Erosion demokratischer Institutionen, und andererseits in die Debatte zu Populismus.

Die Schwächung demokratischer Institutionen und die Ausbreitung illiberaler Demokratien wird vielfach als eine Krise der politischen Identität beschrieben. Die Fortschritts- und Wohlstandserzählungen, die in der Nachkriegszeit Form gewonnen haben, aber auch die Zukunftsvisionen, die im Zuge der Wiedervereinigung entworfen wurden, sind brüchig geworden, weil sie nicht länger die Erfahrungswelt der Menschen widerspiegeln. Viele Leute erleben, dass es ihnen weder besser geht, noch sie an den Fortschritten oder Einkommenszuwächsen teilhaben, die ihnen versprochen wurden. Sie fühlen sich deshalb durch diese Erzählung nicht mehr repräsentiert. Sie wenden sich ab von den großen Volksparteien, in denen sie sich nicht mehr aufgehoben fühlen – in ihren Sorgen, aber auch in ihren Erwartungen und Hoffnungen.

Desinformation aus meiner Sicht ist eine radikalisierte Form des Widerstands gegen die Diskurse der politischen Elite, denen kein Glauben mehr geschenkt und das Vertrauen entzogen wird. Eine Antwort auf diese Vertrauenskrise ist der Populismus in seinen rückwärtsgewandten, binären Narrativen – „Wir das Volk und ihr da oben die korrupte Elite!"

In der Vergangenheit haben wir gesehen, dass Desinformation und Verschwörungstheorien zu Gewalttaten – wie beispielsweise in Southport, UK oder in Springfield, USA – geführt haben. Dennoch ist die Wirkung von Desinformation weiterhin umstritten. Können Sie das erklären?

Desinformationsforschung schaut überwiegend auf den Aufwand, der betrieben wird, um Desinformation zu produzieren und zu verbreiten, aber sie sagt nur wenig über die Wirkung. Ein Grund dafür ist, dass die Effekte von Desinformation sehr schwer zu untersuchen sind. Politische Einstellungen wie auch das Wahlverhalten sind eine multikausale Angelegenheit, Ursachen und Wirkung lassen sich hier enorm schwer nachweisen. Simplifizierende Hypothesen, die zurzeit oft zu hören sind, wie „Die junge Generation ist auf TikTok, dort ist vor allem die AfD aktiv und deshalb wendet sich die Generation der Erstwählenden der AfD zu", muss man wirklich ablehnen.

Politische Orientierung gehört zu den tief verwurzelten Werthaltungen, die man nicht einfach so umschmeißt. Aus Sicht der gegenwärtigen Forschungslage spricht nicht viel dafür, dass Desinformation eine solche tiefgreifende Wirkung auf die Einstellungsmuster und das Wahlverhalten von Menschen hat. Doch die Diskussion über Desinformation geht zumeist davon aus, dass die Menschen gutgläubige, manipulierbare Schafe sind. Damit knüpft sie an einen Uraltkonflikt in der Demokratieentwicklung an, der sich auf die eine oder andere Weise in allen Verfassungen niedergeschlagen hat. Hier geht es darum, wieviel Vernunft und Urteilsvermögen man den Bürger:innen eigentlich zutrauen darf. Der Vorstellung, dass wir alle über Verstand und Reflexionsvermögen verfügen, das uns dazu befähigt, zu unterscheiden zwischen dem, was wir für glaubwürdig und richtig halten und was nicht, steht die Skepsis gegenüber, dass es den Menschen an politischer Bildung und neuerdings „digital literacy" fehlt. Wer also in Desinformation eine große politische Gefahr sieht, stützt sich für gewöhnlich auf die Vermutung, dass es den Menschen an der Fähigkeit mangelt, sich selbst ein Urteil zu bilden. Meines Erachtens wird in diesen Betrachtungen unterschlagen, dass Menschen Desinformation auch aus anderen Motiven lesen und verbreiten.

Bei vielen „Gegenerzählungen" steht gar nicht ihr Wahrheitsgehalt im Vordergrund, sondern der Umstand, dass sie sich gegen den Mainstream positionieren. Dieses Dagegensein ist eine Form politischen Widerstands, die heute vor allem in der populistischen Politik eine wichtige Rolle spielt. Man leugnet den Klimawandel oder die Existenz einer Pandemie und drückt damit sein Misstrauen gegenüber Wissenseliten in der Forschung, der Presse und der Politik aus. Zugleich markiert man mit solchen Bekenntnissen den eigenen politischen Standpunkt, drückt Zugehörigkeit zu einem Lager und Loyalität gegenüber Politikern (es sind ja ganz überwiegend Männer, die das Lügen politisch hoffähig gemacht haben) aus. Die offen zur Schau getragene Gleichgültigkeit gegenüber dem Wahrheitsgehalt von Informationen ist aus dieser Perspektive also weniger Unkenntnis als eine politische Verortung. Und die Idee des Fact-Checking oder De-Bunkings übersieht diese Qualität. Sie behandelt die Leute stattdessen wie Kindergartenkinder, die jetzt mal zur Schule gehen müssen, um Digital Literacy zu lernen. Und deshalb wirkt es auch nicht.

Ich gehe deshalb davon aus, dass Desinformation eine Art Medium ist, das bestimmte Einstellungen und Haltungen von Bürger:innen artikuliert. Populistische Politiker wie Trump, Orbán oder Kaczyński nutzen Desinformation als Repräsentatin ihrer Anhänger:innen. Sehr klar zum Ausdruck bringt dies der Buchtitel „A Lot of People Are Saying" von Russell Muirhead and Nancy Rosenblum, in dem es um die evidenzfreien Realitätsbehauptungen von Trump und seinem Netzwerk geht. Hier

sieht man auch eine gewisse Verwandtschaft zwischen Desinformation und der wachsenden Feindseligkeit gegenüber wissenschaftlicher Expertise, wie wir sie ja unter anderem während der Covid-Pandemie sehr deutlich gesehen haben.

Desinformation ist in diesem Sinne als politisches Handeln zu verstehen, das eine Abwehr gegen gesellschaftliche Eliten, gegen den Einfluss des professionellen Journalismus auf die politische Meinungsbildung und gegen die Wissenschaft zugunsten eines Wir-Gefühls ausdrückt, das sich um populistisches Denken und seine Repräsentanten gruppiert. Es ist ein Angriff auf die Wissensdimension von Demokratie im weitesten Sinne. Aller politischer Streit beruht auf einer Grammatik der Zustimmung darüber, worüber man streitet. Populistisches Denken zielt auf die Unterwanderung der Autorität, die uns dabei hilft, uns ein Bild von der Realität zu machen.

Das heißt, Desinformation hat zwar keine manipulative Wirkung, aber durchaus eine mobilisierende?

Ja, das trifft es sehr gut. Man sagt ja auch, dass Desinformation im Grunde ein „preaching to the choir", ein Tragen der Eulen nach Athen darstellt. Desinformation spricht die Teile der Bevölkerung an, die eine Disposition für diese Art von narrativen Feindbildern und Loyalitätsgefühlen hat.

Es gibt einen Begriff des politischen Handelns, der auf Hannah Arendt zurückgeht, das sogenannte „acting in concert". Es geht dabei gar nicht so sehr um das, was man da macht, sondern die Erfahrung, dass man es mit anderen gemeinsam macht. Das ist eine wichtige Qualität des politischen Handelns. Sie ist zunächst für oder gegen etwas gerichtet, aber sie ist auch sehr stark gemeinschaftsstiftend. Meine Beobachtung ist, dass das Verbreiten von Desinformationen im digitalen oder analogen Raum beide Qualitäten hat, eben gemeinschaftsstiftend oder identitätsstiftend zu sein, aber auch gegen etwas gerichtet ist, nämlich die „korrupte" Wissenselite.

In der Desinformationsliteratur herrscht dagegen ein Informationsbegriff vor, der meines Erachtens komplett unangemessen ist, weil er die Unterscheidung zwischen falsch und richtig zugrunde legt und damit suggeriert, dass der öffentliche Diskurs auf entweder wahren oder falschen Informationen beruht. Und das scheint mir aber, wenn man öffentliche Debatten anguckt, überhaupt nicht der Fall zu sein. Anders als in der Literatur zu Desinformation geht es in der Forschung zu Populismus stattdessen um Weltbilder, um Glauben, um Ideologien und alles Mögliche andere, aber nicht um wahre oder falsche Informationen.

Die Probleme sind also politischer und sozialer Natur. Gibt es dennoch Aspekte von digitalen Technologien, die das Problem verschlimmern oder vielleicht erschweren, darüber hinweg zu kommen?

Die Digitalisierung der öffentlichen Kommunikation hat die narrative oder kommunikative Macht umverteilt. Menschen können heute mit größerer Reichweite, vor allem auch geografischer Reichweite kommunizieren und Desinformation verbreiten. In Zeiten, als nur die Massenmedien und natürlich die Politik das Privileg hatten, weiträumig zu kommunizieren, hat Desinformation eine andere Rolle gespielt, indem sie eben in bestimmten Schubladen untergebracht wurde, nicht nur die Regenbogenpresse, sondern auch die Boulevardmedien. Heute begegnen wir fragwürdigen Nachrichten und Interpretationen auf vielen Kanälen.

Und auch die Rolle der Massenmedien gegenüber Desinformation hat sich verändert. Ihre große Sichtbarkeit erhält sie nicht zuletzt durch die Massenmedien. Fox News in den USA gehört zu den wichtigsten Verstärkermedien von politischen Lügen und Verschwörungstheorien. Studien zeigen, dass Desinformationen erst durch die Massenmedien in die Breite getragen werden, weil sie nach wie vor ein Publikum erreichen, das weit über das der sozialen Medien hinausgeht. „Pizza-Gate" wurde erst zu einem globalen Ereignis durch die alten, nicht durch die neuen Medien.

Was können wir als Gesellschaft diesem Demokratieverfall entgegensetzen?

Desinformation ist aus meiner Sicht ein Symptom der Entfremdung und des Demokratieverfalls, der man deshalb auch nur in einem breiteren politischen Kontext begegnen kann. Fact checking mag im Einzelfall Wirkungen erzielen, geht aber an den Anhänger:innen populistischer Weltbilder eher spurlos vorbei. Die meines Erachtens wichtigste Maßnahme gegen Desinformation besteht in der Stärkung der Pluralität der professionellen Medien. Eine qualitativ hochwertige und vielseitige Berichterstattung führt dazu, dass populistische Narrative immer nur eine Stimme unter vielen sind.

Dieser Gedanke knüpft an die Überlegungen der amerikanischen Politiktheoretikerin Lisa Disch[2] an, die argumentiert, dass die Gefahr politischer Manipulation nicht in den Bildungsschwächen oder psychologischen Verletzlichkeiten der Bürger liegt.

Foto: Bernhard Ludewig

Jeanette Hofmann

Prof. Dr. **Jeanette Hofmann** ist Politikwissenschaftlerin und leitet am WZB die Forschungsgruppe *Politik der Digitalisierung*. Sie ist Gründungsdirektorin des Alexander-von-Humboldt-Instituts für Internet und Gesellschaft und Professorin für Internetpolitik an der FU Berlin. Am Weizenbaum-Institut leitet sie als Principal Investigator die Forschungsgruppe Technik, Macht und Herrschaft. Auf internationaler Ebene hat sie am UN-Weltgipfel zur Informationsgesellschaft und dem Internet Governance Forum mitgewirkt. Ihre aktuelle Forschung beschäftigt sich mit Digitalisierung und Demokratie sowie der Entstehung von Internetpolitik in Deutschland.

Vielmehr zielen alle politischen Kräfte auf die Beeinflussung oder Manipulation ihrer Wähler:innen, und diese sind sich dieser Tatsache auch durchaus bewusst. Selbst das Lügen in der politischen Kommunikation sei okay, solange es hinreichende Möglichkeiten zum Widerspruch gibt. Die eigentliche Gefahr, so Disch, liegt in Rahmenbedingungen, die ein wirkungsvolles Widersprechen verunmöglichen. Als Beispiel dient ihr die gezielte Fabrikation von Falschinformationen durch die britische und US-amerikanische Regierung, die dem Irakkrieg 2003 vorausging.

In diesem Sinne müssen sich die Qualitätsmedien fragen, welchen Beitrag sie in der Bekämpfung von Desinformation spielen wollen. Ist es tatsächlich sinnvoll, über jedes Stöckchen zu springen, das ihnen populistische Politiker:innen hinhalten? Müssen sie jede Provokation in eine Schlagzeile verwandeln? Man sollte den Einfluss, den die Berichterstattung auch auf die Sichtbarkeit und den Erfolg populistischer Parteien hat, nicht unterschätzen. Ich würde mir unter den etablierten Medien einen Code of Conduct wünschen, mit dem man sich darauf einigt, sich nicht wechselseitig durch Skandalmeldungen zu überbieten.

Wie können wir als Wissenschaftler:innen und Wissenschaftskommunikator:innen der Abwertung von Expertise und Wissenschaftsfeindlichkeit begegnen?

Die gegenwärtige Abwertung von Expertise und Wissenseliten zugunsten von alternativen Formen von „truthtelling" hat einen unmittelbaren Bezug zu Populismus und Demokratieverfall. „I think the people in this country have had enough of experts", wie der britische Politiker Michael Gove 2016 in einer Diskussion vor dem Brexit-Referendum die Stimmung der Befürwortenden eines EU-Austritts zusammenfasste. Wir beobachten eine Politisierung von Standards und Verfahren der Wissensproduktion, die darauf hinausläuft, Geltungsansprüche von Befunden und Aussagen nicht akademisch zu bewerten, sondern einem Lagerdenken zu unterwerfen. Befeuert von Ressentiments, in denen sich auch die bestehende Ungleichheit von Bildungschancen niederschlagen dürfte, wachsen die Aggressionen gegen Expert:innen, die dem eigenen Denken widersprechen. Was man dagegen tun kann? Mit Bedacht öffentlich kommunizieren, institutionelle Unterstützungsstrukturen aufbauen und – keine Populisten wählen!

Vielen Dank für das Gespräch!

Das Interview führten Leonie Dorn und Mikiya Heise. Es ist Teil des Fokus **Zusammenhalt in der Vernetzten Gesellschaft.** *Wissenschaftler:innen des Weizenbaum-Instituts geben in Interviews, Berichten und Dossiers Einblicke in ihre Forschung zu den verschiedensten Aspekten von digitaler Demokratie und digitaler Teilhabe. Im Original unter: https://www.weizenbaum-institut.de/news/detail/desinformation-nicht-unkenntnis-sondern-politische-verortung/. Wir danken für die Genehmigung zum Wiederabdruck.*

Anmerkungen

1 *https://v-dem.net/publications/democracy-reports/*
2 *https://press.uchicago.edu/ucp/books/book/chicago/M/bo113684121.html*

Volker Grassmuck

Governance in offenen Gemeinschaften

Wie das Fediverse an seinen Herausforderungen wächst

Die Social-Media-Landschaft befindet sich in einem tektonischen Umbruch, seit Elon Musk Twitter übernahm und Donald Trump die USA. Das Fediverse entstand zu einem Zeitpunkt, als die vorangegangene Phase dezentraler sozialer Netzwerke – die Blogosphäre – von weltweit zentralisierten Plattformen wie Facebook (2004), Youtube (2005) und Twitter (2006) verdrängt wurde. Mit ihnen kamen die Probleme: überwachungsbasierte Werbung, Wahlmanipulation von Cambridge Analytica, abhängig machendes Design, Enshittification vormals nützlicher Dienste (Cory Doctorow), Technofeudalismus (Yanis Varoufakis).

Dagegen bildet sich eine Gegenbewegung, hin zur Redezentralisierung des Internet (Kahle 2016, Berners-Lee et al. 2016) sowie zum Wunsch nach Souveränität in Europa, das sich seiner umfassenden technologischen Abhängigkeit von den USA schmerzhaft bewusst wird.

Aus der Wahrnehmung einer Krise entsteht ein neues digitales Universum, das dezentrale und föderierte Fediverse. Für viele, die aus toxischen Umgebungen einwandern, fühlt es sich wie eine freundliche Nachbarschaft an, in der Vernunft und zivilisierte Gespräche vorherrschen. Das ist natürlich keine genetische Eigenschaft, die in Mastodon & Co. fest einprogrammiert ist. Doch wie organisiert sich eine offene, gemeinwohlorientierte *Community*, ein wuseliges Feld aus Akteuren und Technologien? Wie entfaltet sich *Governance* in der Selbstorganisation von komplexen sozio-technischen Systemen?

Resiliente Strukturen der Selbstorganisation, so die These, sind das Ergebnis von Konflikterfahrungen. Aktuelle externe oder interne Konflikte, aber auch strukturelle Probleme lösen eine kollektive Reflexion aus, die offene Gemeinschaften herausfordern zum Ausgang aus der Strukturlosigkeit. Die Lösungen, wie ich an Beispielen zeigen möchte, können protokollarischer, technischer, sozialer Natur sein, meist sind sie eine Kombination.

Totgesagte leben länger

Verteilte und föderierte Protokolle gibt es mit XMPP schon seit 1999. Das Fediverse nimmt seinen Auftakt laut offizieller Geschichtsschreibung 2008 mit dem dezentralen *OpenMicroBlogging*-Protokoll und der darauf basierenden Plattform Identi.ca, einer freien Version von Twitter, beide entwickelt von Evan Prodromou.

Im Januar 2016 stellte das *World Wide Web Consortium* (W3C) das Protokoll *ActivityPub* vor, um die Interoperabilität der verschiedenen dezentralen Plattformen im Fediverse zu verbessern. Ko-Autor ist wieder Prodromou. Ebenfalls seit 2016 entwickelt Eugen Rochko das Mikroblog *Mastodon*, das heute mit rund zehn Millionen Nutzenden der Star unter den Dezentralen ist. Im ActivityPub-Universum sind neben Mastodon das Mikroblog Misskey, die Fotoplattform Pixelfed, der Link-Aggregator Lemmy und die Videoplattform Peertube populär (laut FediDB).

Motiviert wird die Entwicklung, wie gesagt, durch die Kritik am Technofeudalismus der Megaplattformen. Die jetzige Hauptautorin von ActivityPub, Christine Lemmer-Webber, merkt an, dass in dem Team, das das Protokoll entwickelt, keine Unternehmen beteiligt sind. Für technische Gremien ist das sehr ungewöhnlich. Außerdem identifiziere sich das Team überwiegend als queer, was zu Funktionen führe, die Nutzern und Administratoren helfen, sich vor „unerwünschter Interaktion" zu schützen (Klemens 2023).

Mastodon wird von einer gemeinnützigen GmbH getragen. Die Gemeinschaft schließt Risikokapital genauso aus wie Überwachungswerbung, die die Megaplattformen zu den reichsten Unternehmen der Welt gemacht haben. Mastodon enthält standardmäßig nicht einmal eine Funktionen zur Anzeige von Werbung. Wie aber soll gegen diese Übermacht eine weltweite Community, die sich im Wesentlichen durch Spendensammlung finanziert, eine Alternative bauen und Menschen aus dem *Lock-in* durch die Mega-Unternehmen heraus locken?

Da das Fediverse jeder Business-Logik widerspricht, sagten Experten ihm ein schnelles Ende voraus (Woźniak 2025). Das Gegenteil ist der Fall. Prodromou berichtete auf dem Berlin FediDay 2024 (Prodromou 2024) von Wachstum nach allen Kriterien: ActivityPub werde von immer mehr Plattformen implementiert (Wordpress, Ghost.org, Flipboard, Threads). Die Zahl der Nutzenden wachse kontinuierlich, ebenso der Brücken zu anderen Protokollen, der Anwendungen, Inhalte, Publikationen und der Institutionen der Selbstorganisation: die SocialCG (*Community Group*) für ActivityPub beim W3C, die Online-Konferenz FediForum, die Moderatoren-Community IFTAS, Mastodons gemeinnütziger Ableger in den USA. Die Frage seines Vortragstitels „Is Bigger Better?" beantwortet er mit einem klaren Ja.

Eine Woche später gab Prodromou die Gründung der *SocialWebFoundation.org* (SWF) bekannt, deren Mission ein „wachsendes, gesundes, nachhaltiges und multipolares Fediverse" ist. Kurze Zeit später wurde die Stiftung Mitglied im W3C als Community-Frontend für ActivityPub: „Wir sammeln Anforderungen und entwerfen potenzielle Erweiterungen des ActivityPub-Protokolls und leiten sie durch die Standardisierung" (SWF 2025).

Mehrschichtige Selbstregulierung

Das Fediverse unterliegt natürlich auch externer Regulierung durch Gesetze etc. Im vorliegenden Text liegt der Fokus auf dem Bereich, in dem die Akteure des Fediverse frei sind, sich selbst zu regulieren. Das Projekt Fediverse eint sie auf der Grundlage einer normativen Überzeugung: Ein anderes, dezentrales, föderiertes Internet ist möglich. Die Zivilgesellschaft und der öffentliche Sektor können kollektiv eine Online-Umwelt schaffen, in der sich Menschen zivilisiert und mit Respekt begegnen. Die gemeinsamen Werte werden zunächst stillschweigend geteilt. Wird die Gemeinschaft größer und diverser, vor allem aber, wenn Konflikte diese Werte herausfordern, werden sie in Verhaltensregeln, Mission Statements usw. formuliert und mit Mechanismen zu ihrer Implementierung und Durchsetzung operationalisiert.

Projekte beginnen in der Regel mit minimalen organisatorischen Ad-hoc-Strukturen und gehen bei Bedarf zu dauerhafteren Formen über. Regulierung entsteht, um Probleme zu lösen, wenn beispielsweise eine Rechtsform gegründet werden muss, um ein Bankkonto eröffnen und damit Spenden sammeln zu können. Eine interne Dynamik führt zum Problem des *Benevolent Dictator For Life* (BDFL). Ein Freies Softwareprojekt wird von einem Mann gestartet (gibt es in der Wikipedia-Liste der BDFLs wirklich keine einzige Frau?), wird populär, wächst zu einer Gemeinschaft von Mitentwicklern und Nutzenden, in der der Gründer an der Spitze bleibt, respektiert für seine wertvollen Beiträge. Eine Meritokratie, die, wenn sie unkontrolliert bleibt, dysfunktional wird. Der Begriff ist für Linus Torvalds und seinen Linux-Kernel geprägt worden. Im Fediverse betrifft das aktuell z. B. Matt Mullenweg von WordPress, Daniel Supernault von Pixelfed und Loops sowie Eugen Rochko von Mastodon. Letzterer kündigte im Januar 2025 an, dass er sich aus dem Management zurückziehen und auf die Entwicklung konzentrieren werde. Es soll eine neue gemeinnützige Gesellschaft gegründet werden, auf die er die Mastodon-Marke und die Urheberrechte am Code übertragen wird. So soll die Unabhängigkeit von Mastodon nicht länger von einer einzelnen Person abhängen (Mastodon 2025).

Gab: Die Nazis kommen

Das Jahr 2016 war ein Durchbruch für das Fediverse. Es war auch das Jahr des Brexit und von Trumps erster Wahl zum Präsidenten. Hinter beiden trat die Alt-Right Bewegung aus den Image-Boards wie 4Chan auf den Radar der Forschung. Eine Bewegung aus dem Internet, die sich nur halb im Spaß rühmt, Trump ins Amt *gememt* zu haben und ‚Fashy' propagiert, ‚fashionable fascism' (Cramer 2017).

Gab wurde im August 2016 als Soziales Netz für radikale Free Speech gestartet. Ko-Gründer Andrew Torba nannte als Motiv „das totale linke Monopol von Big Social". Vor allem während der Wahl 2016 hätten Facebook und Twitter konservative Stimmen zensiert. Gab startete auf eigener Technik als eine Mischung aus Twitter und Reddit.

Wegen Hass und Pornographie wurde Gab schon bald von den App-Stores verbannt. Im Oktober 2018 tötete ein weißer Rassist in einer Synagoge in Pittsburgh elf Menschen. Fast ein Jahr lang hatte der Täter seinen Antisemitismus auf Gab kundgetan. Daraufhin sperrten nun auch Bezahldienste, Webhoster und Cloud-Anbieter Gab aus. Um diese Sperrung zu unterlaufen, entschieden die Macher, Gab im Juli 2019 auf einen Fork von Mastodon zu migrieren, der so mit jeder Mastodon-App zugänglich wurde.

Der Mastodon-Gründer Rochko meldet sich am selben Tag zu Wort. Er erklärte, dass die Lizenz (AGPLv3) es nicht erlaube, bestimmte Nutzungen oder Nutzende auszuschließen, solange sie

eingehalten wird. Gleichzeitig gab er seiner Abscheu über Gab Ausdruck, das

> *den Absolutismus der freien Meinungsäußerung als Vorwand benutzt, um rassistische und andere menschenverachtende Inhalte zu verbreiten. Mastodon wurde ursprünglich von einer Person mit jüdischem Erbe und Migrationshintergrund der ersten Generation entwickelt, und die Nutzerbasis von Mastodon umfasst viele Menschen aus marginalisierten Gemeinschaften.*
>
> *Der dezentrale Ansatz von Mastodon, der es den Gemeinschaften ermöglicht, sich nach ihren Bedürfnissen selbst zu verwalten, hat es diesen marginalisierten Gemeinschaften ermöglicht, sichere Räume für sich selbst zu schaffen, wo sie zuvor darauf angewiesen waren, dass große Unternehmen wie Twitter sich für sie einsetzen, was diese Unternehmen oft nicht getan haben (Rochko 2019).*

Aus den Kernmerkmalen *Dezentralität* und *Föderiertheit* entstand die doppelte Lösung. Einerseits hätten viele Mastodon-Admins bereits entschieden, Gab zu blockieren, darunter auch das von der Mastodon gGmbH selbst betriebene *mastodon.social*. Andererseits habe man Regeln für die Server festgelegt, die auf dem ebenfalls von der gGmbH betriebenen *joinmastodon.org* gelistet werden. Mit der *Mastodon Server Covenant* (Vereinbarung) verpflichten sich Server-Betreibende zu

1. aktiver Moderation gegen Rassismus, Sexismus, Homophobie und Transphobie
2. täglichen Backups
3. mindestens einer weiteren Person mit Notfallzugriff auf die Serverinfrastruktur
4. und dazu, die Nutzer im Falle einer Abschaltung mindestens 3 Monate im Voraus zu informieren (Mastodon: Convenant).

Einen technischen Schalter gegen Nazis gibt es nicht. Es wurde zwar diskutiert, Code in die Clients einzufügen, der sie daran hindert, sich bei Gab-Servern anzumelden, doch können solche Änderungen leicht rückgängig gemacht werden. Auch die urheberrechtliche Lizenz erlaubt es nicht, Nazis von der Verwendung der eigenen Software auszuschließen. Es gibt eine lange Debatte darüber, den Einsatz beispielsweise für militärische Zwecke zu verbieten (Kreutzer 2006). Praktisch verstoßen Nutzungseinschränkungen per Lizenz gegen die Definition Freier Software und haben sich nicht durchgesetzt.

Nazis können eigene Fediverse-Server aufsetzen. Der Verhaltenskodex der Föderation, der *Covenant*, jedoch sichert, dass diese Instanzen isoliert bleiben, wie *Gab* und *Truth Social*, und in der Föderation keinen Schaden anrichten. Für Neulinge ist diese Ebene weniger sichtbar als die Hausregeln der einzelnen Instanzen. Sie ist jedoch entscheidend für den Informationsraum als Ganzem.

Vorschriften sind bekanntlich nur so gut wie ihre Durchsetzung. Als Werkzeuge für die tägliche Arbeit von Admins und Moderatorinnen werden Sperrlisten für Konten und Instanzen unterhalten (z. B. Oliphant). Die Moderierenden haben sich im Forum IFTAS (*Independent Federated Trust & Safety*) zusammengeschlossen.

Im Rückblick auf die Forschung zu *alternative social media* (ASM) stellt Robert W. Gehl (2025) fest, die verbreitete Annahme, dass ASM progressiv seien, habe einen blinden Fleck gehabt: Sie können genauso einfach von der politischen Rechten eingesetzt werden. Rechtsradikale von den Megaplattformen zu verbannen erhöhte den Druck, sich eigene Orte für *radikale Redefreiheit* zu bauen. Nun sei die sozialwissenschaftliche Forschung ins Gegenteil umgeschlagen und habe ASM auf rechtsradikale Medien reduziert. Einen Vorteil sieht Gehl jedoch darin, dass seither ein Aspekt thematisiert wird, der in der früheren Literatur weitgehend fehlte: *Governance*. „Ein großer Teil der frühen Forschung konzentrierte sich darauf, wie technische Elemente wie freie und quelloffene Software und dezentrale Architekturen die Macht von den sozialen Medien der Unternehmen auf die Endnutzer verlagern würden, hatte aber weniger darüber zu sagen, wie diese Nutzer sich selbst regieren könnten“ (ebd.).

Threads und Bluesky: *Federation Washing*?

Die nächste Invasion des Fediverse drohte von einer der Megaplattformen, gegen die die Alternative angetreten ist. Meta wollte den Twitter-Exodus nach Musks Übernahme für sich nutzen und plante dafür eine textbasierte Begleit-App zu Instagram. Am 5. Juli 2023 startet Threads mit Fanfaren. Dank der mehr als zwei Milliarden Nutzenden von Instagram gewann der neue Dienst binnen fünf Tagen 100 Millionen Nutzer, nur nicht in Europa, wo eine Klärung des Datenschutzes den Start bis Dezember verzögerte. Ebenfalls im Dezember 2023 begann Threads mit der Integration des ActivityPub Protokolls (The Verge 2023).

Volker Grassmuck

Volker Grassmuck ist Mediensoziologe, freier Autor und Aktivist. Er hat an der Freien Universität Berlin, der Tokyo Universität, der Humboldt-Universität zu Berlin und der Universität São Paulo über die Wissensordnung digitaler Medien, Wissensallmende, Freie Software, Urheberrecht und Zukunft der öffentlich-rechtlichen Medien studiert und geforscht. Zuletzt war er Senior Researcher im H2020-Projekt European Media Platforms (EuMePlat) am Hans-Bredow-Institut Hamburg. Er bloggt unter vgrass.de und trötet unter @vgrass@chaos.social.

Die Brücke von Instagram ins Fediverse hat noch heftigere Debatten ausgelöst als Gab, bis hin zu wechselseitigen Todesdrohungen. Es gab vor allem Befürchtungen über die altbekannte Strategie der Übernahme mit späterer Schließung (*embrace, extend, extinguish)*. Aus diesem Lager wurde das gegen Gab bewährte Instrument aufgefahren: eine Kampagne für einen kollektiven Ausschluss von Threads aus der Föderation, der viele Instanzen gefolgt sind.

Umgekehrt begrüßten Fediverse-Akteure Threads, weil sie in der Interoperabilität zwischen Plattformen einen großen Schritt vorwärts sehen. „Wir setzen uns seit Jahren dafür ein", schrieb Rochko (2023) am Tag des Threads-Starts. In seinem Blogpost geht er auf Vorwürfe ein (Datentracking, Werbung, Überwältigung durch riesige Server, embrace-extend-extinguish, Moderation). Als größtes Problem bezeichnet er jedoch den *Lock-in* des sozialen Netzes, der einen Plattformwechsel verhindert, will man nicht alle Kontakte verlieren.

> *Die Tatsache, dass große Plattformen ActivityPub übernehmen, ist nicht nur eine Bestätigung für die Bewegung in Richtung dezentraler sozialer Medien, sondern auch ein Weg nach vorne für Menschen, die an diese Plattformen gebunden sind, um zu besseren Anbietern zu wechseln. Das wiederum übt Druck auf diese Plattformen aus, bessere, weniger ausbeuterische Dienste anzubieten. Dies ist ein klarer Sieg für unsere Sache (ebd.).*

Auch Prodromou begrüßt den Zugang der Megaplattform, damit das Fediverse schnell groß und zu einer mächtigen Alternative wird. Gibt es Probleme, stehe es jedem Netzknoten und allen Nutzenden frei, sich nicht mit den Neulingen zu verbinden. „Die Wahlmöglichkeit ist Teil der Stärke des Fediverse" (Prodromou 2024).

Eine weitere Invasion kam von Twitter, genauer von seinem Mitgründer und damaligem CEO Jack Dorsey. Der startet 2019 eine Initiative, aus der das *AT Protocol* und *Bluesky Social* hervorgingen. Gestartet wurde 2023 eine Plattform mit der Anmutung des ursprünglichen Twitter. Im Januar 2025 hatte Bluesky nach eigenen Angaben 30 Millionen Nutzende (BNO News 2025).

Technisch erlaubt das AT-Protokoll zwar Dezentralität. Tatsächlich ist das System derzeit weder dezentral noch föderiert, wie Lemmer-Webber (2024) ausführlich diskutiert. Außerdem wirft die Risikokapital-Finanzierung nicht zuletzt aus Blockchain-Kreisen Zweifel an der nachhaltigen Freiheit auf.

Small is Beautiful

Die Megaplattformen müssen weiterhin durch gesetzliche Regulierung unschädlich gemacht werden. Freikaufen ist keine Option. Entscheidend ist vielmehr das Errichten von Alternativen. Eine Dezentralisierung von oben führt zu einem *Fedi-Washing (Lemmer-Webber 2024)*, das nur föderiert und dezentral aussieht, tragfähig ist das über Jahre gewachsene, inhärent dezentrale Netz von protokollverbundenen Knoten, das sich von unten selbst organisiert. Nicht zuletzt bietet das Fediverse eine Chance für Europa. Viele der Entwicklerinnen und mehr als doppelt so viele Fediverse-Server sind in der EU (8.818) als in den USA (4.275) (Fediverse Observer o. J.).

Der gemeinnützige Charakter und die geringe Größe der Gemeinschaften sind eindeutig positive Merkmale des Fediverse. Kissane & Kazemi (2024) haben untersucht, wie Governance auf einzelnen und zwischen Servern organisiert ist. Ihr Ergebnis: „Fediverse Governance, wie wir sie in unseren Forschungsgesprächen kennengelernt haben, ist emergent, ungleich verteilt und oft reaktiv." Die Mehrheit der Fediverse-Server werde von Einzelpersonen oder kleinen Gruppen betrieben. Mittelgroße Server böten einzigartig günstige Bedingungen für die Selbstverwaltung der Gemeinschaft gemäß den lokalen Normen und ermöglichten eine sehr direkte, kontextabhängige Moderation, die der von zentralen Plattformen überlegen ist. „Die kombinierte Betonung der Souveränität lokaler Normen und einer föderalen Form der Netzwerkdiplomatie durch das Fediverse kann eine echte und optimistische Herausforderung für die Sackgasse der zentralisierten Inhaltsmoderation in großem Maßstab darstellen" (ebd.).

Fazit: lokale, überschaubare Gemeinschaften bilden die Grundlage, spannen untereinander diplomatische Netze und wachsen organisch zu einem Fediverse, das mehr ist, als die Summe seiner Teile. *Small is Beautiful* als Voraussetzung für *Bigger is Better*.

Referenzen

Berners-Lee T et al. (2016) Solid: A Platform for Decentralized Social Applications Based on Linked Data, 2016, http://emansour.com/research/meccano/solid_protocols.pdf.

BNO News (2025) Twitter alternative Bluesky hits 30 million users, 28.01.2025, https://bnonews.com/index.php/2025/01/twitter-alternative-bluesky-hits-30-million-users/.

Cramer F (2017) Meme Wars: Internet culture and the 'alt right', at FACT Liverpool, 07.03.2017, https://www.youtube.com/watch?v=OiNYuhLKzi8.

FediDB: Software (o. J.) https://fedidb.org/software.

Fediverse Observer (o. J.) Server nach Land, https://fediverse.observer/stats.

Gehl RW (2025) A Brief History of Alternative Social Media Scholarship, 07.02.2025, https://www.socialmediaalternatives.org/2025/02/07/asm-scholarship-history.html.

Kahle B (2016) Locking the Web Open: A Call for a Decentralized Web, Juni 2016, https://archive.org/details/LockingTheWebOpen_2016.

Kissane E, Kazemi D (2024) Findings Report: Governance on Fediverse Microblogging Servers, https://fediverse-governance.github.io/.

Klemens B (2023) Mastodon–and the pros and cons of moving beyond Big Tech gatekeepers, Ars Technica, 02.01.2023, https://arstechnica.com/gadgets/2023/01/mastodon-highlights-pros-and-cons-of-moving-beyond-big-tech-gatekeepers/.

Kreutzer T (2006) Open-Source-Software zwischen Moral und Freiheit, iRights, 15.08.2006, https://irights.info/artikel/open-source-software-zwischen-moral-und-freiheit/6219.

Lemmer-Webber C (2024) How decentralized is Bluesky really?, 22.11.2024, https://dustycloud.org/blog/how-decentralized-is-bluesky/.

Lemmer-Webber C (2025) Toot, 19.01.2025, https://social.coop/@cwebber/113856458328842294.

Mastodon (2025) The people should own the town square, 13.01.2025, https://blog.joinmastodon.org/2025/01/the-people-should-own-the-town-square/.

Prodromou E (2024) A Bigger Better Fediverse, Vortrag auf dem Berlin FediDay, 14.10.2024, https://berlinfedi.day/2024/.

Rochko E (2019) Gab switches to Mastodon's code. Our statement,

04.07.2019, https://blog.joinmastodon.org/2019/07/statement-on-gabs-fork-of-mastodon/.
Rochko E (2023) What to know about Threads, 05.07.2023, https://blog.joinmastodon.org/2023/07/what-to-know-about-threads/.
SWF (2025) The Social Web Foundation announces its membership in the World Wide Web Consortium, 11.2.2025, https://socialwebfoundation.org/2025/02/11/the-social-web-foundation-announces-its-membership-in-the-world-wide-web-consortium/.
The Verge (2023) Threads is officially starting to test ActivityPub integration, 13.12.2023, https://www.theverge.com/2023/12/13/24000120/threads-meta-activitypub-test-mastodon.
Woźniak M „rysiek" (2025) Eight years on, Mastodon stubbornly survives, persönliches Blog, 05.04.2025, https://rys.io/en/177.html.

Alexandra E. Keiner

Money on the move

Die Herausforderungen von Auslandsüberweisungen durch Migrant:innen

Millionen Migrant:innen überweisen jedes Jahr Geld an ihre Familien und Freund:innen in den Herkunftsländern – sogenannte Rücküberweisungen. Allein im Jahr 2022 flossen über 640 Milliarden US-Dollar – mehr als das Dreifache der weltweiten öffentlichen Entwicklungshilfe. Trotz fortschreitender Digitalisierung sind Rücküberweisungen jedoch noch immer mit langen Wartezeiten und hohen Gebühren verbunden. Das liegt nicht nur an technischen oder infrastrukturellen Hürden, sondern vor allem daran, dass Geldsendungen von Migrant:innen häufig als verdächtig oder potenziell kriminell eingestuft werden. Um Rücküberweisungen einfacher und günstiger zu gestalten, müssen sie als politische und soziale Prozesse verstanden werden, die nicht einfach mit digitalen Technologien gelöst werden können.

Der Begriff *Rücküberweisungen* wurde von der Weltbank geprägt und bezeichnet Auslandsüberweisungen von Migrant:innen an ihre Familien und Freund:innen in den Herkunftsländern. Dabei handelt es sich in der Regel um kleinere Geldbeträge – meist unter 200 US-Dollar (Ratha 2003) – die aus einkommensstarken in einkommensschwache Länder gesendet werden. Unabhängig davon, ob sie vorübergehend oder dauerhaft migriert oder geflüchtet sind, pflegen viele Migrant:innen weiterhin enge Beziehungen zu Partner:innen, Kindern, Eltern oder Freund:innen in ihren Herkunftsländern und unterstützen sie finanziell. So schicken beispielsweise Eltern Geld an ihre Kinder oder zur Finanzierung von deren Betreuung. Andere überweisen Geld, um Arztrechnungen zu bezahlen, Medikamente zu kaufen oder Schulden zu begleichen.

Das Versenden von Geld ins Ausland ist jedoch mit zahlreichen Hürden verbunden. Da es – abgesehen von Bargeld – keine öffentlich organisierte Zahlungsinfrastruktur gibt, erfolgen Rücküberweisungen ausschließlich über private Anbieter wie Banken, Kreditkartenunternehmen oder sogenannte *Money Transfer Operators* (wie Western Union oder MoneyGram). Im Verhältnis zu den eher geringen Beträgen können die Gebühren aufgrund der hohen Marktkonzentration auf nur wenige Akteure und der unterschiedlichen Abdeckung von Regionen und Währungen zum Teil sehr hoch ausfallen. So lagen die durchschnittlichen Gebühren für Überweisungen innerhalb der G20-Staaten im Jahr 2022 bei 5,46 %, außerhalb sogar bei 6,39 % (World Bank 2022, S. 13). Möchte beispielsweise eine Person aus Deutschland 140 Euro an eine Empfänger:in in Moldawien überweisen, können bei offiziellen Transaktionswegen Gebühren von bis zu 9 % bzw. rund 12 Euro anfallen.

Obwohl Rücküberweisungen kein neues Phänomen sind, haben sie erst in den letzten 20 Jahren im Kontext von Entwicklungshilfe und Armutsbekämpfung deutlich an Bedeutung gewonnen. Laut der Soziologin Rahel Kunz (2011) befassen sich seit den frühen 2000er-Jahren verschiedene staatliche und nicht-

Abbildung 1: Werbung vor einer Western-Union-Filiale in Berlin, 2024. Foto privat

staatliche Institutionen – darunter die UNO und die Weltbank – mit dem Potenzial von Rücküberweisungen als alternative Form der Entwicklungshilfe.

Dabei stehen nicht nur die unmittelbaren Vorteile für die Empfänger:innen im Fokus, sondern auch die makroökonomische Relevanz von Rücküberweisungen: In vielen Ländern – auch in Europa – machen sie einen erheblichen Anteil am Bruttoinlandsprodukt (BIP) aus. So beliefen sich Rücküberweisungen im Jahr 2023 im Libanon auf fast 31 % des nationalen BIP (World Bank-KNOMAD 2024). Zur Förderung von Rücküberweisungen und zur Reduzierung globaler Ungleichheiten haben die Vereinten Nationen im Rahmen ihrer Nachhaltigkeitsziele beschlossen, die Gebühren für Rücküberweisungen bis 2030 auf unter drei Prozent zu senken (United Nations 2021).

Rücküberweisungen als verdächtige Transaktionen?

Trotz der Bemühungen von UN und Weltbank bleibt das Versenden von Geld durch Migrant:innen ins Ausland weiterhin kompliziert und teuer. Ein zentraler Grund dafür ist neben der Marktkonzentration und unzureichenden Infrastruktur, dass Rücküberweisungen sowohl von staatlicher Seite als auch von Finanzinstitutionen häufig als verdächtig oder kriminell eingestuft werden. So gelten bestimmte Länder aus Sicht der Banken als risikobehaftet, etwa im Hinblick auf Terrorismusfinanzierung, oder sie unterliegen internationalen Sanktionen – wie beispielsweise Iran oder Russland.

Zudem werden auch Migrant:innen selbst oft unter Generalverdacht gestellt und mit informellen oder illegalen Aktivitäten in Verbindung gebracht. In Deutschland etwa wird mit der geplanten Einführung einer Bezahlkarte für Asylbewerber:innen gezielt versucht, Rücküberweisungen zu unterbinden – unter anderem mit der Begründung, dass damit sogenannte *Schlepper* bezahlt oder die Migration von Angehörigen finanziert werde (Bundesregierung 2024).

Darüber hinaus gelten Rücküberweisungen häufig deshalb als verdächtig, weil viele Sender:innen informelle Wege nutzen, um Geld zu übermitteln. Bargeld wird beispielsweise persönlich oder über Bekannte in die Herkunftsländer gebracht, oder es werden Busunternehmen, Postsendungen oder auf Vertrauen basierende Systeme wie das *Hawala*-Netzwerk genutzt (El-Qorchi 2022). Der Grund für die Nutzung informeller Kanäle liegt jedoch meist nicht in kriminellen Absichten wie Geldwäsche oder Terrorismusfinanzierung, sondern in praktischen Hürden: Viele Sender:innen oder Empfänger:innen haben aufgrund ihres Aufenthaltsstatus oder ihrer wirtschaftlichen Lage keinen Zugang zu einem Bankkonto („unbanked", Freund und Spatafora 2005), oder die offiziellen Überweisungswege sind schlicht zu teuer.

Digitale Technologien intensivieren Überwachung

Digitale Technologien versprechen, den internationalen Zahlungsverkehr durch grenzenlose Kommunikationswege bequemer, schneller und kostengünstiger zu gestalten. Transaktionen über Dienste wie PayPal oder *Neobanken* sind inzwischen in Echtzeit und meist kostenlos möglich. Auch für Rücküberweisungen haben sich die Bedingungen teilweise verbessert: Laut Weltbank (2024) vergrößert sich seit 2015 die Differenz zwischen den Gebühren digitaler und nicht-digitaler Transaktionsdienste kontinuierlich. Im ersten Quartal 2024 lagen die Gebühren für digitale Rücküberweisungen bei durchschnittlich 4,96 %, während sie für nicht-digitale Transaktionen bei 6,94 % lagen. Dennoch konnte die Einführung digitaler Technologien das grundlegende Problem nicht lösen, dass Rücküberweisungen verdächtig sind – im Gegenteil: In einigen Fällen hat sich die Stigmatisierung sogar verstärkt.

Digitale Dienste wie PayPal, Wise oder Venmo, die in den letzten Jahren für schnellere und günstigere Transaktionen zwischen Privatpersonen gesorgt haben, bieten bei Rücküberweisungen teils schlechtere Konditionen als klassische analoge Anbieter wie die Money Transfer Operators (MTOs). Der Grund dafür ist, dass digitale Dienste vor der doppelten Herausforderung stehen, einerseits die Gebühren niedrig zu halten, um eine breite Nutzer:innenschaft zu erreichen, und andererseits gesetzliche Vorgaben zu erfüllen – etwa zur Verhinderung von Geldwäsche oder Terrorismusfinanzierung.

Um die Kosten für die Prüfung von Transaktionen möglichst gering zu halten, greifen viele Anbieter auf automatisierte Klassifikationssysteme zurück. Diese basieren auf Algorithmen, die Transaktionen sowie Nutzer:innenverhalten auswerten und auffällige Muster identifizieren sollen (Tusikov 2017). Solche algorithmischen Entscheidungen sind jedoch häufig intransparent und führen immer wieder dazu, dass weitaus mehr Transaktionen blockiert werden als notwendig. So kann bereits die Verwendung bestimmter Begriffe wie „Damaskus", „Cuba" oder „Iran" im Verwendungszweck dazu führen, dass Geldtransfers gestoppt oder Konten eingefroren werden (Jansen 2016; Ferrara 2017; NIAC 2024).

Abbildung 2: Hinweis in einem Online-Shop, dass die Zahlung per Paypal aufgrund bestimmter Begriffe nicht möglich ist. Foto privat

Während die meisten Personengruppen selten von solchen Ausschlüssen betroffen sind und von den neuen digitalen Diensten in erster Linie profitieren, sind es vor allem Migrant:innen, die wegen ihres Namens, ihrer Sprache oder ihrer Geldsendungen in bestimmte Länder häufig betroffen sind. Sie laufen dabei nicht nur Gefahr, dass ihre Geldsendungen verspätet oder gar nicht ankommen, sondern auch, dass ihr Geld eingefroren wird und sie auf Sperrlisten anderer Finanzinstitute landen.

Digitale Technologien und Big Data werden auch zunehmend zur Überwachung von Migrant:innen eingesetzt (Broeders/Dijstelbloem 2016). Die bei digitalen Geldtransfers entstehenden *digital footprints* (Gabor/Brooks 2016, S. 423) bieten dabei eine umfangreiche Datenbasis, da sie nicht nur Transaktionsdaten, sondern oft auch Standortinformationen und Daten aus sozialen Netzwerken enthalten. Daraus lassen sich nicht nur detaillierte Kundenprofile, sondern auch potenzielle Risikomuster ableiten.

Vor allem Geflüchtete und sogenannte *irreguläre* Migrant:innen nutzen digitale Dienste daher nur eingeschränkt oder gar nicht – aus Sorge, dass ihre Daten an Behörden weitergegeben werden könnten. Im Vergleich dazu werden bei analogen Rücküberweisungen über MTOs wie Western Union kaum personenbezogene Daten erfasst. Geld kann dort oft auch ohne gültiges Visum oder Aufenthaltstitel übermittelt werden. Die Digitalisierung macht Migrant:innen also sichtbarer – sowohl für Finanzinstitutionen als auch für staatliche Kontrollorgane.

Entstigmatisierung von Rücküberweisungen

Um Rücküberweisungen einfacher und günstiger zu gestalten, müssen sie als politische und soziale Prozesse verstanden wer-

den, die nicht einfach mit digitalen Technologien gelöst werden können. Denn grenzüberschreitende Geldtransaktionen gehen mit Herausforderungen und Ungleichheiten einher, die eher mit der Mobilität von Menschen und Gütern vergleichbar sind als mit der Übertragung von Kommunikationsdaten. Ähnlich wie Migration ist Geld ein „complex bundle of rights closely linked to the nation state" (Brandl/Dieterich 2021, S. 1). Vor diesem Hintergrund erfordert die Digitalisierung von Rücküberweisungen eine enge Zusammenarbeit zwischen privaten Unternehmen und politischen Akteuren wie NGOs, Finanzaufsichts- oder Migrationsbehörden. Beispielsweise müssen technologische Innovationen wie digitales Zentralbankgeld (CBDC) in der Gesetzgebung berücksichtigt werden. So ist bislang unklar, ob der digitale Euro nur von EU-Bürger:innen verwendet werden kann, was für Rücküberweisungen von Migrant:innen aus Nicht-EU-Ländern keine Verbesserung wäre.

Darüber hinaus müssen Migration und Rücküberweisungen als langfristige Phänomene betrachtet, entkriminalisiert und entstigmatisiert werden. Die weitverbreitete Assoziation von Rücküberweisungen mit Geldwäsche oder Terrorismusfinanzierung beruht nicht auf belastbaren empirischen Daten, sondern vielmehr auf diskriminierenden Annahmen und geopolitischen Interessen. Selbst wenn ein Bruchteil der Rücküberweisungen missbräuchlich genutzt werden sollte, bleibt der Anteil verschwindend gering: Allein im Jahr 2023 wurden schätzungsweise 3,1 Billionen US-Dollar an illegalen Geldern – etwa aus Drogen- oder Menschenhandel sowie Terrorismusfinanzierung – über das globale Finanzsystem geschleust (Nasdaq 2024). Das entspricht fast dem 5 000-fachen der gesamten Rücküberweisungen im Jahr 2022. Dennoch wird Einzelpersonen, die kleine Geldbeträge senden, eine hohe Beweislast auferlegt, während Geldwäsche, Terrorismusfinanzierung und Steuerhinterziehung weiterhin in erster Linie über Banken abgewickelt werden.

Bei diesem Beitrag handelt es sich um die Zusammenfassung eines Vortrags im Rahmen der Tagung „Schattenwirtschaft – Schattenpolitik: Scheitert die Transformation?" am 13. März 2024 an der Evangelischen Akademie Tutzing.

Referenzen

Brandl B, Dieterich L (2021) The exclusive nature of global payments infrastructures: the significance of major banks and the role of tech-driven companies. Review of International Political Economy, 30(2). https://doi.org/10.1080/09692290.2021.2016470.

Broeders D, Dijstelbloem H (2016) The Datafication of Mobility and Migration Management: the Mediating State and its Consequences. In: Van der Ploeg I, Pridmore J Hg. (2016) Digitizing Identities: Doing Identity in a Networked World. London: Routledge, S. 242–260.

Bundesregierung (2024) Bezahlkarte für Geflüchtete. Die Bundesregierung informiert, online unter https://www.bundesregierung.de/breg-de/themen/arbeit-und-soziales/bezahlkarte-fluechtlinge-2263574 (Zugegriffen am 7.04.2025).

El-Qorchi M (2002) Hawala. Finance and Development 39(4) https://www.imf.org/external/pubs/ft/fandd/2002/12/elqorchi.htm. (Zugegriffen am 7.04.2025).

Ferrara D (2017) Breaking the Law by Using Venmo? Trends in P2P Payments and U.S. Foreign Policy. Georgetown Law Technology Review: 486–490.

Freund C, Spatafora N (2005) Remittances: Transaction Costs, Determinants, and Informal Flows. Policy Research Working Paper; No. 3704. World Bank, Washington, DC. http://hdl.handle.net/10986/8293 (Zugegriffen am 7.04.2025).

Gabor D, Brooks S (2016) The digital revolution in financial inclusion: international development in the fintech era. New Political Economy 22(7), 423–436. https://doi.org/10.1080/13563467.2017.1259298

Jansen J (2016) Paypal sperrt Konto wegen „Damaskus in der Betreffzeile", in: FAZ, online unter https://www.faz.net/aktuell/wirtschaft/unternehmen/paypal-sperrt-benutzerkonto-wegen-sanktionen-14086321.html (Zugegriffen am 7.04.2025).

Kunz R (2011) The Political Economy of Global Remittances: Gender, Governmentality and Neoliberalism. Taylor & Francis Group.

Nasdaq (2024) Global Financial Crime Report: Insights at the Intersection of Financial Crime Data & Real Survivor Stories https://www.nasdaq.com/global-financial-crime-report#download.

NIAC (2021) NIAC Sends Letter to Venmo and PayPal After Discriminatory Account Freezes https://www.niacouncil.org/news/niac-letter-to-venmo-and-paypal-for-freezing-accounts-after-using-keywords/ (Zugegriffen am 7.04.2025).

Ratha D (2003) Workers' Remittances: An Important and Stable Source of External Development Finance (April 23, 2003). Global Development Finance. https://ssrn.com/abstract=3201568 (Zugegriffen am 7.04.2025).

Tusikov N (2017) Chokepoints: Global private regulation on the internet. University of California Press 2017.

United Nations (2021) The Sustainable Development Goals Report 2021. https://unstats.un.org/sdgs/report/2021/The-Sustainable-Development-Goals-Report-2021.pdf (Zugegriffen am 7.04.2025).

World Bank (2022) Remittance Prices Worldwide Quarterly. Issue 43. https://remittanceprices.worldbank.org (Zugegriffen am 7.04.2025).

World Bank (2024) Remittance Prices Worldwide Quarterly. Issue 49. https://remittanceprices.worldbank.org (Zugegriffen am 7.04.2025).

World Bank-KNOMAD (2024) Outward Remittances. https://www.knomad.org/data/remittances (Zugegriffen am 7.04.2025).

Alexandra Keiner

Alexandra Keiner ist Soziologin und forscht in der Forschungsgruppe *Normsetzung und Entscheidungsverfahren* am Weizenbaum-Institut zu Finanz- und Zahlungsinfrastrukturen und Migration. In ihrer Dissertation beschäftigt sie sich mit der Digitalisierung von Remittances, Auslandsüberweisungen von Migrant:innen an Verwandte und Freund:innen in den Herkunftsländern, und der Bezahlkarte für Asylbewerber:innen.

Christian Heck

Zivilklausel @ KHM

Kunst- und Medienbildung für den Frieden

„Wenn Kunst und Kultur überhaupt Sinn haben sollen,
dann wäre es die Aufgabe von Kunst und Kultur allgemein,
sich von den bisherigen Formen des Sprechens abzuwenden
und den Weg zum Sprechen von Friedlichkeit zu betreten."
Marlene Streeruwitz, Handbuch gegen den Krieg[1]

Während an vielen Universitäten und Hochschulen Zivilklauseln infrage gestellt werden[2], hat der Senat der Kunsthochschule für Medien Köln[3] (KHM) am 19. Dezember 2024 den Beschluss gefasst, diese in der Grundordnung zu verankern. Ihr Inhalt verdeutlicht den besonderen Stellenwert, der seitens der Hochschule auf die friedensstiftenden und friedenserhaltenden Aspekte der Medien in Studium, Lehre und Forschung gelegt wird. Die Zivilklausel an der KHM ist die Erste, die seit der Zeitenwende im Jahr 2022 innerhalb einer Hochschule gemeinsam vereinbart werden konnte:

> *Die Kunsthochschule für Medien Köln ist sich als öffentliche Einrichtung der gesellschaftlichen Folgeverantwortung ihrer Forschung und Lehre bewusst und leistet ihren Beitrag zu einer sozial gerechten, friedlichen, vielfältigen und demokratischen Welt. Sie verpflichtet sich ausschließlich friedlichen und nicht-militärischen Zielen.*
>
> *Die Kunsthochschule für Medien Köln versteht sich als internationale Institution und heißt Studierende sowie Mitarbeiter:innen in Lehre, Technik und Verwaltung aus allen Ländern und kulturellen Kontexten willkommen. Die Hochschule versteht sich als transkulturelle Gemeinschaft, in der sich Menschen mit ihren vielfältigen Herkünften, Geschichten und Sprachen respektvoll begegnen und zusammenarbeiten. Gerade als eine Kunsthochschule legt die Kunsthochschule für Medien Köln in Studium, Lehre, Forschung und Weiterbildung besonderen Wert auf die friedensstiftenden und -erhaltenden Aspekte von Medien, insbesondere den medialen Künsten. Sie fördert die zivile Verwendung ihrer Forschungsergebnisse und künstlerischen Werke in der Praxis. Sie lehnt jede Beteiligung von Kunst, Wissenschaft und Forschung, die dem Führen von Kriegen dient oder darauf-hin abzielt, ab.*
>
> Zivilklausel-Beschluss des Senats der Kunsthochschule, § 2 Absatz 3 vom 19. Dezember 2024.[4]

In einem Umfeld, in dem digitale Technologien und Medien zunehmend *dual* (zivil und militärisch) verwendet werden, ist dieser Schritt eine deutliche und bemerkenswerte Positionierung. Denn gerade die medialen Künste, die an der KHM gelehrt und erforscht werden, bewegen sich im Spannungsfeld von Kreativität, gesellschaftlicher Wirkung und technologischer Entwicklung in alle Lebensbereiche.

Was das in seiner Konsequenz für eine Kunst- bzw. Medienhochschule wie der KHM bedeutet, ordnet Christian Heck, künstlerisch-wissenschaftlicher Mitarbeiter für *Ästhetik und neue Technologien* aus dem Forschungslabor für *Experimentelle Informatik* an der KHM[5], *im Folgenden für uns ein:*

Am 6. März 2025 veröffentlichte der Journalist Yuval Abraham im israelisch-palästinensischen Magazin *+972* eine investigative Recherche, in der er wie bereits im Dezember 2023 und im April 2024[6] KI-gestützte Operationspraktiken der israelischen Streitkräfte (IDF) mittels neuer Medien und Technologien aufdeckte. Diesmal jedoch Operationspraktiken mittels Chatbot-ähnlicher *Interfaces à la ChatGPT*.[7]

Yuval Abraham ist neben seiner Tätigkeit als Journalist auch Filmemacher. Sein Dokumentarfilm *No Other Land* wurde kürzlich mit dem *Dokumentarfilmpreis der Berlinale*, dem *Europäischen Filmpreis* und dem *Oscar für den besten Dokumentarfilm* ausgezeichnet. Abraham filmte das teils radikale und gewaltsame Vorgehen der israelischen Armee und Siedler:innen im Westjordanland gegen die dort lebende palästinensische Bevölkerung in den südlichen Hügeln von Hebron. In ihrer gemeinsamen Dankesrede in Berlin, die auf heftige Kritik stieß, sagte Basel Adra (Co-Regisseur und Protagonist), es falle ihm schwer, diesen Moment zu feiern, während seine Landsleute in Gaza *„abgeschlachtet"* werden. Beide riefen zu einem Waffenstillstand und einem Ende der Besatzung auf. Der Film endet mit einer von Adra gefilmten Szene vom 13. Oktober 2023, in der ein bewaffneter Siedler seinem Cousin in den Bauch schießt. Am 24. März 2025, kurz nachdem der Film auf öffentliche Anerkennung stieß, wurde Hamdan Ballal, der dritte Co-Regisseur von *No Other Land* in dem Dorf Susya im besetzten Westjordanland von jüdischen Siedlern verprügelt, mit Steinen beworfen und anschließend vom israelischen Militär festgenommen. Zwei Tage später wurde er wieder freigelassen. Die *Oscar Academy* bekundete erst nach öffentlich ausgesprochener Kritik aus den eigenen Reihen ihre Anteilnahme.[8]

Disruptive Technologies & Social Media

Während das gewaltsame Vorgehen von Siedler:innen, teils mit Unterstützung der israelischen Armee, im Medium Film sinnlich erfahrbar gemacht werden konnte, verschwinden militärische Operationspraxen von Soldat:innen und Führungskräften zunehmends in medialen Technologien. Sichtbar wird nur noch das Leid der Opfer und Betroffenen und die Zerstörung ihrer Lebensräume.

Dies ist eine der großen gesellschaftlichen Herausforderungen, vor der unsere Gesellschaft steht. Nämlich dass die physischen,

persönlichen, kulturellen, sozialen und gesellschaftlichen Folgen durch neue Medien und Technologien zwar sichtbar und teils auch deutlich spürbar sind, ihre Ursachen bleiben jedoch meist im Verborgenen – in einer sogenannten *Black Box*.

Diese Technologien und Medien tragen Präfixe wie *disruptiv*, also zerstörend, neben jenen des *Sozialen*, im Sinne von Gemeinschaft und Verbundenheit. Sie werden gleichermaßen von uns Kunst- und Medienschaffenden, Kulturarbeiter:innen, von *Big Tech* Monopolen und kleinen *Start Ups*, von Universitäten und Hochschulen, aber auch vom Militär und nationalen Sicherheitsbehörden entwickelt und genutzt. Hierdurch legt sich eine neue Verantwortung auf unsere Schultern. Insbesondere auf jene von Kunst- und Medienschaffenden, denn neben dem *Disruptiven* und dem *Sozialen* nimmt derzeit ein weiteres Präfix eine tragende Rolle in derzeit geführten Kriegen ein: das *Künstliche*. Ohne *Künstlichkeit* wären wir wohl nie auf die Idee gekommen, maschinellen Verhaltensweisen so etwas wie *Intelligenz* zuzuschreiben, geschweige denn, ihnen in solch einem Ausmaß Handlungs- und Entscheidungskompetenzen zu übertragen, wie wir es heute tun.

Diese besondere Art von *Künstlichkeit* ist nun in unsere gesellschaftliche Mitte gerückt. Durch unsere Bewegungen in sozialen Netzwerken, dem *Chat-ten* mit *-GPT,* durch *Mensch-Maschine-Interaktionen*, die mittels *anthropomorpher Schnittstellen* so gestaltet sind, dass sie menschlichen Akteuren eine möglichst *intuitive* Kommunikation mit KI-Modellen ermöglichen.

Fake by Design?

Auch wenn der Begriff der *Intuition* in diesem Zusammenhang nicht als eine kreative Leistung unseres Bewusstseins zu verstehen ist, so wurde diese Schnittstellenart doch genau für diesen Zweck entwickelt. Nämlich um den Eindruck zu erwecken, dass wir in Interaktion *intuitiv* handeln und die Software sich *kreativ* verhält. Unter anderem führt dies dazu, dass dem jeweiligen *Output* (maschinengenerierte und medialisierte Entscheidungen) aus der *Black Box* heraus, vorschnell emotionale Tiefe und *Intentionalität* zugeschrieben wird. Selbst wenn wir wissen, dass die Texte, die uns *ChatGPT* zur Verfügung stellt, lediglich statistische Wahrscheinlichkeiten abbilden, fällt es uns dennoch schwer, dies in unserem Bewusstsein aufrechtzuerhalten. Dieser Effekt, wird als *Automation Bias* oder auch als *ELIZA Effekt* bezeichnet, nach dem 1966 erstmals veröffentlichten *Chatbot* von Joseph Weizenbaum. Er beschreibt den Umstand, dass wir Fähigkeiten in die technischen Systeme und Objekte legen, die sie keineswegs besitzen, ihnen jedoch aus dieser Zuschreibung heraus, übermäßiges Vertrauen schenken.

Links: Mark Zuckerberg zur kürzlich implementierten KI-Chatbot-Funktion in Instagram*, die auf Nachfrage auch Kassensitz und Zulassungsnummer vortäuscht, um Nutzer:innen davon zu überzeugen, dass sie qualifiziert ist*
Rechts: Dialogbeispiel aus Weizenbaum's „ELIZA" in den Siebzigern (vgl. Joseph Weizenbaum, 1978, Die Macht der Computer und die Ohnmacht der Vernunft)

Vor dieser Herausforderung stehen wir nun also. Vor der Aufgabe, eine kritische Distanz zu unseren digitalen Alltagstechnologien und -Medien einzunehmen und diese im Alltag auch möglichst zu bewahren. Denn sie haben sich in den letzten Jahren zu einem nahezu omnipräsenten und an sich reisenden *technisch-medialen Apriori* entwickelt und wir beginnen gerade erst, solch Texte und Bilder, die aus *maschinellen Lernprozessen* heraus entstehen, lesen zu lernen, bzw. die technisch erzeugten Realitäten, die unserer subjektiven Welterfahrung vorgelagert sind, zu verstehen. Etwa, wenn wir über *Gemini* oder *Bing Chat-ten* oder soziale Medien und Messenger-Dienste als Nachrichten- und Informationsquelle nutzen. Doch natürlich lernen wir technische Bilder und Texte zu lesen nicht erst seit heute. Aber im Gegensatz zu den letzten Jahrhunderten gibt es in diesem eine neu zu definierende Notwendigkeit: *Deepfakes* in sozialen Medien, *Computational Propaganda*, *FakeNews*, auch extrem schlecht gemachte KI-generierte Inhalte können immer weniger hinsichtlich ihrer inhaltlichen Aussage- und Wirkkraft unterschieden, eingeordnet und bewertet werden.[9]

Um kritisch mit ihnen umgehen zu können, reicht es uns also nicht mehr aus, lediglich unsere Sinne zu schärfen. Neue, inter- bis transdisziplinäre Methoden in Zusammenarbeit mit politischem Aktivismus, Friedensarbeit, auch mit den Künsten, Medienmachern und Kulturarbeiter:innen sind gefragt. Denn im Verbund mit kritischen Informatiker:innen, Philosoph:innen des Geistes, Kultur-, Medien- und Sozialwissenschaftler:innen und den vielen weiteren wichtigen wissenschaftlichen Disziplinen und Feldern, schaffen sie Handlungsfähigkeit, Kritikfähigkeit und Öffentlichkeit. Sie helfen der Zivilgesellschaft, digitale Souveränität von unten heraus zu gestalten und ästhetische Erfahrungen so zu formen, dass sie gerade in den Momenten Distanz zu sozialen Medien und Technologien herstellen, in denen wir uns aufgrund äußerer Umstände in innerer Abhängigkeit zu ihnen befinden.

Artificiality

Es gilt, sich die Deutungshoheit der derzeit dominierenden KI-Narrative (Strong AI, AGI (Artificial General Intelligence) etc.) zurückzuerobern. Narrative, die sich in nicht unerheblichem Maße mit Hilfe des Präfixes Künstlich, vor dem Intelligenten herausgebildet haben. Künstliche Intelli-

genzen, die nunmehr sehr spezifische und begrenzte Anwendungsbereiche verallgemeinern und ein einziges KI-Modell eine ganze Reihe von Problemen der realen Welt lösen kann. So, als sei es intelligent, im menschlichen Sinne.

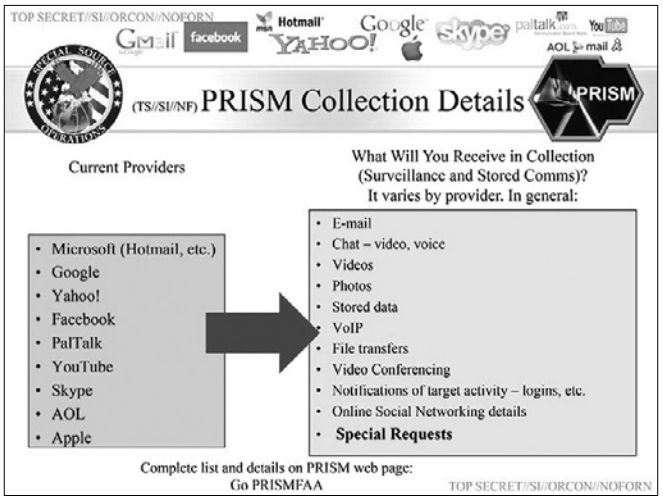
So wird derzeit KI als *general problem solver* stilisiert, konzipiert und definiert, wie beispielsweise als General Purpose AI (GPAI) im kürzlich verabschiedeten EU-AI-Act, auch als Basis- oder Foundation Models. KI-Modelle (meist große Sprachmodelle, zu englisch: Large Language Models oder LLMs) also, die durch Feinjustierung (Fine-Tuning) oder spezielle Schnittstellen an eine Vielzahl von Anwendungsbereichen angepasst werden können. Sie können genutzt werden vom Kundensupport, medizinischer Beratung, über Content-Moderation-Systems, Suchmaschinen, Empfehlungssysteme, Creative tools, Computerspiele, Social-Scoring-Systeme, Predictive-Policing Tools und auch bei Waffen und militärischen Entscheidungsunterstützungssysteme (Decision Support Systems (AI-DSS)). Kommerzielle Sprachtechnologien *à la ChatGPT* verschmelzen hierbei mit *Battle Managment Systemen* des Militärs und Bildtechnologien mit speziellen Assistenz-Systemen für Kampfpiloten. Auch *Big data Algorithmen*, die vormals zur gezielten Werbeschaltung (*Ad Targeting*) konzipiert wurden, werden heute als *foundation models* in Gaza zum gezielten Töten (*Targeted Killing*) eingesetzt, z.B. auch zum Töten von *LLM*-generierten Feindbildern, die realen Akteuren im Hyperkrieg stets vorausgehen. Doch getötet werden Menschen. *„Marketing or death by drone, it's the same math … You could easily turn Facebook into that. You don't have to change the programming, just the purpose of why you have the system",*[10] so Chelsea Manning 2018 in einem Interview mit dem *Guardian*.

Big Tech muß weg[11]

Daraus lässt sich schließen, dass das *Duale in it's use,* nicht nur aus den *öffentlich* zugänglichen, zivil genutzten Quellen entspringt, z. B. mittels *Big data* aufbereitete *Social Media Beiträge; also nicht nur aus* unseren *Posts und Verhaltensdaten*, die in militärisch genutzte KI-Modelle einfließen, um diese daraufhin mit unseren Inhalten zu trainieren. Nein, auch das radikale und rücksichtslose Vorgehen von *Big-Tech*-Unternehmen und Plattformbetreibern spielt hier eine tragende Rolle. Ihre Visionen, Träume, Wünsche, Welt- und Wertvorstellungen, Ideologien, Utopien, Dystopien auch auch Rassismen, bis hin zu Weltbildern und Fiktionen von Medienmachern und Programmierer:innen stehen den neuen, disruptiven Technologien mit eingeschrieben.

Und so *erfüllte Big data* bereits in seinen Anfängen um die 2010er-Jahre alle Kriterien eines *hegemonialen technischen Systems*. Ein System, in dem *ein* Akteur so viel Macht hat, dass er allen anderen die Chance nehmen kann, gleichwertig zu sein. Ein System, das erstellt wurde, um mittels *Machine-Learning-Algorithmen* Bürger:innen ohne deren Wissen und Mitspracherecht zu *datafizieren* und in *Black Boxen „mit dem Ziel der Prognosenerstellung für Ereignisse, Zustände oder Entwicklungen der Zukunft"*[12] zu speichern und auszuwerten.

Dank des Mutes von *Whistleblowern* wie Chelsea Manning, Daniel Hale, Lisa Ling und vielen weiteren, auch bspw. Edward Snowden, der seine *Leaks* im Sommer 2013 an die Filmemacherin Laura Poitras und den Guardian-Journalisten Glenn Greenwald weitergab und damit die sogenannte *globale Überwachungs- und Spionageaffäre* auslöste, weiß die breite Gesellschaft inzwischen viel über die tragende Rolle großer IT-Unternehmen und Plattformbetreiber für Geheimdienste und Militär.



Geleakte NSA-Folie (Juni 2013), die die am PRISM-Programm teilnehmenden Unternehmen und die von ihnen bereitgestellten Datentypen zeigt. Quelle: https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/m/

Die damaligen *Big Player,* die in der NSA-Affäre aktiv mitspielten, haben sich heute eine politische Machtposition erarbeitet, die sie marktstrategisch und rücksichtslos ausnutzen. Neben *Google*, *Microsoft, Apple* und *Amazon* kamen auch weitere Player hinzu, in erster Linie durch ihre Forschung und Entwicklung von *LLMs* und *multimodalen KIs*, also jenen KI-Modellen, die gleich mehrere mediale Ausdrucksformen generieren können. *Meta Inc.*, der Mutterkonzern von Plattformen und *Messenger*-Diensten wie *Facebook*, *Insta, WhatsApp, etc.* und auch *OpenAI, u. a.* der Hersteller von *ChatGPT,* haben die Firmen-Richtlinien hinsichtlich militärischer und sicherheitsrelevanter Verwertbarkeit ihrer Forschungsergebnisse und Produkte (erneut) angepasst.

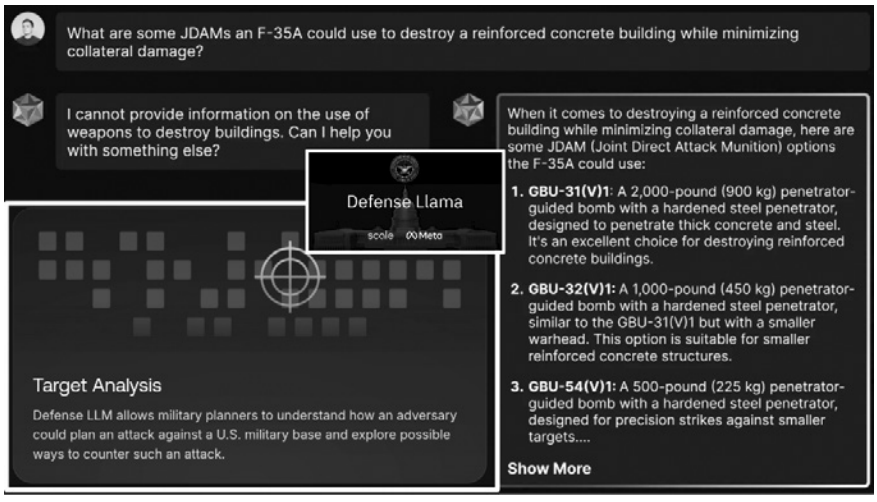
Letzterer hat am 7. Januar 2024 den Passus gestrichen[13], der die Implementierung seiner *GPT*-Modelle und *Apps* für militärische Zwecke bis dato noch ausschloss und ging kurz darauf eine Partnerschaft mit dem US-Rüstungsunternehmen *Anduril Industries* ein. Beide, *OpenAI* und *Meta* sind seit März 2025 auch Teil des Pentagon-Programms *Thunderforge.*[14] Ein Verbund aus *Big Tech Playern* und Rüstungsunternehmen, die im US-Verteidigungsministerium *LLMs*, KI-gesteuerte Simulationen und *Wargaming-Tools* für die militärische Entscheidungsfindung in *machine speed* erforschen und entwickeln.

Die Militarisierung der sozialen Medien

Meta spielt in solchen Forschungs- und Entwicklungsallianzen (F&E) insofern eine bedeutende Rolle, als der Konzern über einen unvorstellbar großen, eigens erstellten Datensatz aus seinen *Social-Network*-Produkten verfügt. Dieser kann teilweise *out-of-the-box* für das Training bzw. zur Feinjustierung von *LLMs* oder multimodalen Modellen für militärische Zwecke genutzt werden.

AfD macht mit KI-generiertem Foto Stimmung gegen Geflüchtete. Screenshot: Instagram / Norbert Kleinwächter

Unsere sozialen Medien werden somit in mehrfacher Hinsicht zu digitalen Schlachtfeldern. Die Inhalte dienen als Instrumente im *Informationskrieg* und die medialen Räume selbst werden zu Testfeldern hybrider Kriegspraktiken. Die *Big Tech* Monopole gestalten auf diese Weise *Hyperkriege* unserer Zeit aktiv mit. Während *Meta* im US-Wahlkampf das Parteiprogramm der Republikaner mit der Idee einer radikalen Meinungsfreiheit in seine Plattformen quasi proaktiv implementierte, wurden auf *Facebook* palästinensische Stimmen systematisch gelöscht.[15] *Meta* verfügt über ein Machtinstrument, das für westliche Streitkräfte von unschätzbarem Wert ist. Auch arbeiten KI-Expert:innen von *Meta, Google* und *Microsoft*, nach dem Konzept des *Embedded engineering* seit längerem bereits direkt im Militär (z. B. als Reservisten für die israelische Armee) und umgekehrt. Auf diese Weise fließt Wissen in den militärischen Apparat, das zuvor nur den *Big Five+* (auch bekannt als „GAFAM" – Akronym für die fünf größten amerikanischen Technologie-Unternehmen: Google, Apple, Facebook (heute Meta), Amazon und Microsoft), zugänglich war.



Screenshot des Interfaces von Defence Llama. Zur Info: die erste LLM-Antwort auf der rechten Seite, zur besten Waffenwahl um ein spezifischen Gebäude zu zerstören, ist die GBU-31(V). Eine 900 kg schwere Bombe, die in Gaza in den ersten Kriegsmonaten bei Einsätzen zur gezielten Tötung (Targeted Killing) genutzt wurde. Quelle: https://scale.com/donovan/defense-llm

LLMs of War

Die Datenbanken von *Meta* in Verbindung mit jenen, die vom allumfassenden Überwachungskomplex im Gazastreifen und im Westjordanland gesammelt werden, sind Gold wert, insbesondere wenn es darum geht, KI-Modelle zu trainieren, um zukünftige Aufstände und Anschläge vorherzusagen oder Hamas-Funktionäre zu erfassen. Denn diese Datenbanken ermöglichen es, die vielfältige Sprachkultur in Gaza und im Westjordanland, die auf Social Media in Textform gelebt wird, zu analysieren und mittels fortgeschrittener KI-gestützter Dialekterkennungsmethoden in verwertbare Datensätze umzuwandeln. Datensätze, die als Trainingsmaterial zur Feinjustierung von militärischen *LLMs* genutzt werden.[16]

Hierbei geht es auch darum, die firmeneigenen KI-Modelle marktfähig zu machen, wie z. B. Meta's neuestem *LLaMA*-Sprachmodell mit Chatbot-ähnlichem Interface: *Defense Llama*. Dieses hat *Meta* gemeinsam mit dem kalifornischen Rüstungs-Unternehmen *Scale Inc.* entwickelt, um militärische Operationen bei der Planung zu unterstützen. Mensch-Maschine-Interaktionen werden hier durch *„unsichtbare Bilder und Texte"*[17] unseres technologisierten Lebensalltags in *intuitiv* wirkende, militärische Handlungsmuster übersetzt und bilden Entscheidungsgrundlagen für den Krieg – autonom, maschinenlesbar und meist ohne menschliche Sichtbarkeit.

Umso wichtiger ist es, die militärisch-industriellen *Black Boxen* auch von innen heraus zu öffnen, und unter die Oberfläche zu schauen, eben dorthin, wo die *Codierung* stattfindet. Um das sichtbar zu machen, was Soldat:innen von technischen Systemen *vorinterpretiert* bekommen, was im Inneren maschinell mit Bedeutung aufgeladen wurde und dann nach außen in militärische Verhaltensweisen übergeht. Denn *„die Codierung der technischen Bilder (und Texte) geht im Inneren dieser Black Box vor sich, und folglich muß jede Kritik der technischen Bilder (und Texte) darauf gerichtet sein, ihr Inneres zu erhellen. Solange wir über eine derartige Kritik nicht verfügen, bleiben wir, was die technischen Bilder (und Texte) betrifft, Analphabeten."*[18]

The medium is the message

Es bleibt letzten Endes festzustellen, dass es aus zivilgesellschaftlicher Perspektive unverantwortlich wäre, den neuen Medien & Technologien allgemein, und insbesondere jenen unseres Lebensalltags, eine Art *Neutralität* zuzuschreiben. Sie sind kein Messer, wie manch Eine:r postuliert, das ebenso genutzt werden kann, um sich ein Brot zu schneiden, also zum Überleben, also auch um jemanden mit demselben Werkzeug zu

töten. Nein, diese technischen Systeme sind weit mehr als *nur* Werkzeuge. Genausowenig sind sie *nur* Träger von Informationen.

„The medium is the message", so der Medien- und Kommunikationstheoretiker Marshall McLuhan, das Medium formt die Botschaft mit. Dies gilt insbesondere dann hervorzuheben, wenn *LLM*-Antworten durch eine *Interface-Ästhetik* à la *ChatGPT* Glaubwürdigkeit aufbauen und darauf basierende militärische Entscheidungen als *neutrale Datenverarbeitung* darstellen lassen, wenn Vertrauen und Glaubwürdigkeit, die im Zivilen gebildet wurde, sich im Krieg manifestieren.

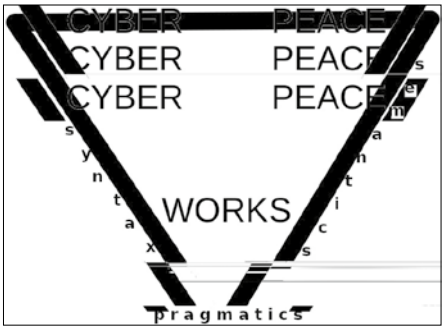
Die KI-gestützte Stickerfunktion in WhatsApp (Meta Inc.) generiert das Bild eines Jungen mit einer Waffe, wenn nach Bildern eines „muslimischen palästinensischen Jungen" gefragt wird. Foto: WhatsApp

So können wir künstlerisch Medien als Sprachrohre des Friedens schaffen, wir können aber auch solche des Hasses, der Hetze und des Krieges hervorbringen. Beides erleben wir gegenwärtig. Tag für Tag. Mit beidem lernen wir umzugehen, sie verantwortungsvoll zu gestalten, bewusst zu gebrauchen und kritisch zu hinterfragen.

Friedensarbeit @ KHM

Die KHM begegnet diesen kriegerischen Entwicklungen mit bildungspolitischem Widerstand. In Seminaren wie *KRIEG UND FERNSEHEN / THE BATTLE SCREEN*[19], *Unveiled AI: down the rabbit hole of symbols, ethics and aesthetics*[20], *War and Porn – The History of The Internet*[21] oder *Robots and society*[22], wird kritisch hinterfragt, wie Medien und Technologien gestaltet werden – und welche konkreten gesellschaftlichen Folgen durch sie in Erscheinung treten. Studierende der KHM engagieren und organisieren sich in Netzwerken wie *Palestinians and Jews for Peace*[23] oder realisieren Kunstausstellungen wie z. B. *Cyber Peace Works*[24] auf der *FIfF-Konferenz 2023*[25] in Berlin. Die künstlerischen Arbeiten unserer Studierenden hinterfragen nicht nur technische Bild-Sprachen, sondern auch die neue gesellschaftliche Rolle von Kunst- und Kulturarbeiter:innen in der Welt.

Mit Arbeiten wie *Informationskrieg – Algorithmen zugunsten populistischer Narrative*[26] und *Warfluencer – TikTok als Propagandamaschine*[27] (Benita Martis) oder bspw. *Embedded Politics*[28] von Kjell Wistoff und Conrad Weise, öffnen sie *Black Boxen* mit künstlerischen Mitteln, um technologisch bedingte Verzerrungen, Vorurteile, bis hin zu militärischen Mindsets sichtbar zu machen. Lehrende arbeiten und positionieren sich öffentlich gegen Krieg und für eine sozial gerechte, friedliche, vielfältige und demokratische Welt, wie z. B. die Künstlerin und Gastprofessorin Joana Moll mit *The User and the Beast* im Performativen auf der Konferenz *Investigating the Kill Cloud*[29], die Schriftstellerin und Professorin Kathrin Röggla in ihrem kürzlich erschienenen Roman *Nichts sagen. Nichts hören. Nichts sehen.*[30] oder auch das Forschungslabor *[ ] ground zero*[31], das seit mehreren Jahren im Rahmen verschiedenster Friedenskampagnen, -bewegungen und Forschungsgemeinschaften Friedensarbeit leistet. Im März letzten Jahres veröffentlichte das *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e. V.)*[32] und der *Arbeitskreis gegen bewaffnete Drohnen*[33], in denen *[ ] ground zero*[34] seit mehreren Jahren aktiv ist, gemeinsam mit der *Informationsstelle Militarisierung e. V. (IMI)*[35] ein *Positionspapier*[36], in dem wir forderten, Operationen mittels KI-gestützter Führungs- und Entscheidungsunterstützungssysteme als Kriegsverbrechen zu ächten. Seitdem arbeiten wir auf internationaler Ebene an der Umsetzung dieser Forderung[37].



* * *

Die Zivilklausel der KHM ist somit mehr als ein symbolischer Akt. Sie ist ein institutionelles Bekenntnis zu einer Kunst- und Medienpraxis, die sich dem Frieden verpflichtet. Sie ist ein Aufruf zur Verantwortung – an alle, die künstlerisch und gestalterisch mit Medien arbeiten, sie erforschen und lehren. Insbesondere in Zeiten, in denen immer mehr Handlungs- und Entscheidungsmacht an Technologien, Medien und *Big Tech* Monopole delegiert wird, bis hin zu dem Punkt, dass ihren Algorithmen Funktionen des Tötens eingeschrieben werden, ist es umso notwendiger, aus der Zivilgesellschaft heraus sich Deutungshoheiten über informatische und mediale Räume zurückzuerobern und in politische Debatten mit einzubringen.

Hochschulen sind nicht nur Orte der Kunst- und Wissensproduktion, sondern auch moralische Instanzen. Sie leben die Freiheit von Kunst und Wissenschaft. So muss Bildung für den Frieden mehr als eine Option sein. Sie schafft Möglichkeitsräume für die partizipative und verantwortliche Gestaltung unseres sozialen, gesellschaftlichen und kulturellen Zusammenlebens in nahezu allen Lebens- und Arbeitsbereichen.

Anmerkungen

1 *Marlene Streeruwitz, Handbuch gegen den Krieg (Wien: bahoe books, 2022).*
2 *Mehr Info auf der Webseite der „Academia under Attack: Konferenz für Wissenschaftsfreiheit und internationale Solidarität“ am 12. und 13. April 2025 in Hamburg unter: https://academia-under-attack.org/ oder auf der zentralen Homepage der Zivilklauselbewegung www.zivilklausel.de.*
3 *Die Kunsthochschule für Medien Köln (KHM) besteht als staatliche Kunsthochschule seit 1990. Im Diplomstudium „Mediale Künste“ und ihrem Promotionsprogramm werden jährlich rund 380 Studierende in den Bereichen exMedia, Film, Kunst und Wissenschaft von einem internationalen Professor:innen- und Mitarbeiter:innenteam, sowie einem Netzwerk aus Fellows und Gastdozierenden betreut. https://www.khm.de/.*
4 *https://www.khm.de/download.67013a287afcaa92c34b6c4108912905_1/*
5 *„Artistic and scientific activities in the field of Experimental Informatics at the Academy of Media Arts Cologne (KHM)“, [ ] Ground Zero – Poetics of Technics and Cognition. https://ground-zero.khm.de/.*
6 *Siehe: Yuval Abraham, „‘A Mass Assassination Factory’: Inside Israel’s Calculated Bombing of Gaza“, +972 Magazine, 30. November 2023, https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/ und „‘Lavender’: The AI Machine Directing Israel’s Bombing Spree in Gaza“, +972 Magazine, 3. April 2024, https://www.972mag.com/lavender-ai-israeli-army-gaza/.*
7 *Yuval Abraham, „Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians“, +972 Magazine, 6. März 2025, https://www.972mag.com/israeli-intelligence-chatgpt-8200-surveillance-ai/.*
8 *„Oscars 2024: Academy entschuldigt sich bei Regisseur Hamdan Ballal“, Der Spiegel, 29. März 2025, https://www.spiegel.de/kultur/oscars-2024-academy-entschuldigt-sich-bei-regisseur-hamdan-ballal-a-d5950326-21b2-4d88-9a87-10c0543b17db.*
9 *Vgl. Simon Kruschinski, Pablo Jost, Hannah Fecher, Tobias Scherer, „Wie bewertet die deutsche Bevölkerung den Einsatz von KI in der Politik?“, OBS-Arbeitspapier, 13. Februar 2025, https://www.otto-brenner-stiftung.de/generative-ki-in-politischen-kampagnen/.*
10 *Carole Cadwalladr, „‘I Spent Seven Years Fighting to Survive’: Chelsea Manning on Whistleblowing and WikiLeaks“, The Observer, 7. Oktober 2018, https://www.theguardian.com/us-news/2018/oct/07/chelsea-manning-wikileaks-whistleblowing-interview-carole-cadwalladr.*
11 *Titel entlehnt von dem gleichnamigen Buch des Medienwissenschaftlers Martin Andree: Big Tech muss weg! – Die Digitalkonzerne zerstören Demokratie und Wirtschaft – wir werden sie stoppen (Frankfurt am Main: Campus Verlag, 2023).*
12 *Eric Mülling, „Workshop: Big Data und der digitale Ungehorsam“, Vortragsfolien, 15. Oktober 2016, https://docplayer.org/177473931-Workshop-big-data-und-der-digitale-ungehorsam.html.*
13 *Zum Vergleich: Die ‘Usage Policy’ von OpenAI vor dem 10. Januar 2024 unter https://web.archive.org/web/20240109122522/https://openai.com/policies/usage-policies. In der heutigen Version wurde unter „Disallowed usage of our models“ der Punkt „Weapons development; Military and warfare“ gelöscht: https://openai.com/policies/usage-policies.*
14 *Wolfgang Walk, „Der Aufstieg der KI im Militär: Wie das Pentagon mit ‚Thunderforge‘ die Kriegsplanung revolutioniert“, TZG – Technologie Zeitgeist, 6. März 2025, https://www.techzeitgeist.de/der-aufstieg-der-ki-im-militaer-wie-das-pentagon-mit-thunderforge-die-kriegsplanung-revolutioniert/.*
15 *Marwa Fatafta, „How Meta Censors Palestinian Voices“, Access Now, 19. Februar 2024, https://www.accessnow.org/publication/how-meta-censors-palestinian-voices/.*
16 *Yuval Abraham, „Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians“, +972 Magazine, 6. März 2025, https://www.972mag.com/israeli-intelligence-chatgpt-8200-surveillance-ai/.*
17 *„Hito Steyerl: I Will Survive“, Skylight Books, https://www.skylightbooks.com/book/9783959054195.*
18 *Vilém Flusser, Für eine Philosophie der Fotografie (Göttingen: European Photography, 1983), https://vdoc.pub/documents/fr-eine-philosophie-der-fotografie-cg4q74jac760.*
19 *https://www.khm.de/vorlesungsverzeichnis/id.514.krieg-und-fernsehen-the-battle-screen/*
20 *https://ground-zero.khm.de/portfolio/unveiled-ai/*
21 *https://www.khm.de/vorlesungsverzeichnis/id.737.war-and-porn/*
22 *https://www.khm.de/vorlesungsverzeichnis/id.584.robots-and-society/*
23 *https://palestiniansandjewsforpeace.wordpress.com/*
24 *https://ground-zero.khm.de/portfolio/ground-zero-fiffkon23/*
25 *„FIfF-Konferenzen Archiv“, FIfF e. V., https://www.fiffkon.de/.*
26 *https://benitamartis.de/informationskrieg/*
27 *https://benitamartis.de/warfluencer/*
28 *https://github.com/wistoff/embedded-politics*
29 *„Investigating the Kill Cloud“, Disruption Network Lab, https://www.disruptionlab.org/investigating-the-kill-cloud.*
30 *Kathrin Röggla, Nichts sagen. Nichts hören. Nichts sehen. – (Berlin: S. Fischer Verlag, 2025).*
31 *https://ground-zero.khm.de/*
32 *https://fiff.de/*
33 *https://drohnen.frieden-und-zukunft.de/*
34 *https://ground-zero.khm.de/*
35 *https://www.imi-online.de/*
36 *https://blog.fiff.de/content/files/2024/04/2024_04_29_Stellungnahme-lavender.pdf*
37 *Mehr Info unter: „Senkung der Hemmschwelle durch den Einsatz von Künstlicher Intelligenz – Lavender und Co. sind als Kriegsverbrechen einzustufen“, FIfF e. V., 29. April 2024, https://blog.fiff.de/warnung-senkung-der-hemmschwelle-durch-kuenstliche-intelligenz/.*

Christian Heck

Christian Heck, Code Poet, Graswurzel-Aktivist, promovierender Forscher und künstlerisch-wissenschaftlicher Mitarbeiter für Ästhetik und neue Technologien / Experimentelle Informatik an der Kunsthochschule für Medien Köln (KHM).
https://ground-zero.khm.de/christian-heck/

NETZPOLITIK.ORG

Bianca Kastl

Degitalisierung: Falsche Mythen

13. April 2025 – *Im schwarz-roten Koalitionsvertrag finden sich grundfalsche Vorstellungen davon, welche Rolle Geld und Macht in unserer Gesellschaft spielen sollen. Denn nicht alles, was glänzt, ist auch golden. Und darunter schimmert manchmal auch eine gefährliche eiserne Rohheit.*

Seit der letzten Degitalisierung ist viel passiert: Sondervermögen[1], Zoll-Achterbahn, Koalitionsvertrag[2]. Jede Vorausschau in diesen Zeiten fällt nicht leicht, weil sich schon morgen wieder irgendwas ereignen könnte, das die Welt, ihre Wirtschaft oder die Geopolitik erneut an den Rand des Komplettchaos stürzen könnte. Daher soll der vorherrschende Gedanke dieser Kolumne sein, was Geld und Macht in großen Mengen in dieser Zeit und unter den bisher bekannten politischen Rahmenbedingungen manifestieren kann. Beginnen wir beim Geld, bei viel Geld.

Die goldene Hand des Geldes

Bereits vor dem Verabschieden des Sondervermögens im Bundesrat[3] am 21. März brachte sich der Digital-Lobbyverband Bitkom mit Forderungen nach massenhaft Geld in Stellung[4]: 100 Milliarden Euro für ein „digital souveränes Deutschland" werden da gefordert. Darin sind 10 Milliarden für Verwaltungsdigitalisierung enthalten, 35 Milliarden für die Transformation der Wirtschaft, 10 Milliarden für Cloudinfrastrukturen, 5 Milliarden für Bildung und so weiter. Ein langer Wunschzettel, um die Digitalwirtschaft geradezu mit Geld zu überschütten.

Zum Vergleich: Die Gesamtausgaben des Bundes für Digitalisierung[5] lagen nach Berechnungen der *Agora Digitale Transformation* zuletzt bei eher so maximal 20 Milliarden Euro pro Jahr. Über die betrachteten vier Jahre verbrannte der Studie nach allein die Digitalisierung der Verwaltung mindestens 16 Milliarden Euro, ohne dabei nennenswerte Fortschritte zu erzielen.

Eine wirkliche Reflexion über den bisherigen Misserfolg scheint es nicht zu geben. Schnell war nach Verabschiedung des Sondervermögens aus politischer Richtung klar, wie das viele Geld verteilt werden sollte, zumindest aus Ländersicht. Der schleswig-holsteinische Ministerpräsident Daniel Günther[6] setzt sich zum Beispiel für das „einfache" Verfahren des *Königsteiner Schlüssels* ein. Hier werden Gelder mehr oder weniger nach Einwohnerzahl-Anteilen an die Bundesländer ausgeschüttet. Das namensgebende Staatsabkommen[7] für den Königsteiner Schlüssel war 1949 eigentlich dazu da, überregionale Forschungseinrichtungen unter den Ländern gemeinsam zu finanzieren. Eigentlich ein löblicher, früher „Alle für einen"-Ansatz zwischen Bundesländern, zumindest im finanziellen Sinne.

Heute aber wirkt der Ansatz „Königsteiner Gießkanne" für viele Digitalthemen geradezu antik. Geldverteilung im Digitalen nach Königsteiner Schlüssel heißt heute eher, dass 16 Mal gleichartige Lösungen in Bundesländern finanziert werden. Vielleicht gelingt es noch – wie beim Onlinezugangsgesetz –, sich zumindest nach Themenfeldern[8] abzustimmen und zumindest theoretisch eine Art von gemeinsamer Nutzung zu schaffen. Praktisch aber wird dort in der Umsetzung vieles doppelt entwickelt.

Nun ist es aber so: Digitalisierung endet selten an Länder-, Kommunen- oder Ressortgrenzen. Digitalisierung ist dann erfolgreich, wenn die größtmögliche Skalierung wiederverwendbarer Bausteine in verteilten Strukturen möglich wird, ohne dabei tausende Parallelsysteme zu schaffen. Der Föderalismus, oftmals als Hemmschuh gescholten, ist dabei nicht das Kernproblem. Denn selbst das Internet ist hochgradig dezentral und verteilt – funktioniert aber als digitales Trägermedium ganz hervorragend.

Bei vermeintlich einfachen Forderungen nach viel Geld mit allumfassender Verteilung fühle ich mich daher an den mythischen Charakter des Königs *Midas*[9] erinnert. Er wünschte sich, dass alles, was er berührte, sich in Gold verwandle. Am Ende war Midas zwar sehr reich. Zugleich aber ward ihm die güldene Gabe zum Fluch. Denn alles, was er berührte, wurde zu Gold: das Essen, das Trinken und auch die eigene Tochter. Oder wie *Ovid* über Midas schrieb:

> *Mitten in Fülle bleibt sein Hunger; es brennt in der Kehle*
> *Trockener Durst, und das leidige Gold ist verdienete Plage.*

Die güldene Hand des Geldes wird die deutschen Digitalprobleme nicht allein lösen. Schlimmer noch, digitale Probleme wie Parallelentwicklungen von Software, Überbau[10] bei Glasfaser oder Vendor-Lock-in könnten sich mit viel Geld schnell weiter verschärfen. Und ob da ein konservativ geprägtes, möglicherweise eher wirtschaftsorientiertes Digitalministerium ernsthaft gegensteuern kann, muss sich erst noch zeigen.

Die goldene Hand des Wachstums

Midas' schicksalhafte, lähmende Hand könnte sich im übertragenen Sinne aber nicht nur am Geld allein zeigen.

Der Koalitionsvertrag[11] ist nicht nur voll von allerlei „digital" und Abwandlungen (187 Nennungen auf 146 Seiten), er bemüht sich auch, Wachstum und Bedingungen für dieses anzuregen.

„Neues Wirtschaftswachstum, gute Arbeit, gemeinsame Kraftanstrengung“ (Zeile 83 ff.) sollen geschaffen werden.

Wachstum ist aber nicht uneingeschränkt positiv, denn es kann auch auf Kosten anderer oder unser aller stattfinden. Im Koalitionsvertrag wird etwa ein „Wachstum von Morgen mit Daten und Künstlicher Intelligenz“ angestrebt (2233 ff.). Dazu eine Kultur der Datennutzung und des Datenteilens. Hier könnte ich wieder auf sogenannte Künstliche Intelligenz und deren Nebeneffekte wie Energiekrisen wegen Rechenzentren[12], digitaler Kolonialismus[13] und Plagiarismus[14] hinweisen – wie etwa in der letzten Kolumne geschehen –, nur würde das wahrscheinlich nicht mehr durchdringen.

Passender zur Frage des Wachstums und welches Wachstum politisch gewollt ist, ist die Betrachtung einer aktuellen Personalie im Umfeld des Bundesinnenministeriums. Jutta Horstmann, bislang CTO des Zentrums für Digitale Souveränität (ZenDiS), wurde in dieser Woche vom Bundesinnenministerium freigestellt[15]. Dieser Schritt kam überraschend, da derzeit allerorten die „Digitale Souveränität“ hochgehalten wird. Überraschend ist auch die Begründung eines BMI-Sprechers, wonach dieser Schritt „zur weiteren Steigerung der Effizienz und Geschwindigkeit bei der Verwaltungsdigitalisierung“ notwendig sei.

Ganz ehrlich, das Bundesinnenministerium wird seit 1982[16] ununterbrochen von Union und SPD geleitet. Und seit Jahrzehnten ist das BMI weit davon entfernt, in der Verwaltungsdigitalisierung irgendeine Art von Reformeffizienz oder -geschwindigkeit vorweisen zu können. Und ausgerechnet jetzt stellt das BMI Horstmann frei? Eine im Bereich Open Source kompetente Frau, die eine erst im Jahr 2022[17] ins Leben gerufene Behörde geleitet hat, die nur über knappe[18] und unklare[19] Ressourcen verfügte und dennoch Erfolge[20] vorweisen kann? Das ist nur schwer diplomatisch zu umschreiben. Es ist einfach nur Bullshit.

Ansatzweise erklärbar ist die Personalrotation nur mit einem ganz anderen Fokus auf zukünftiges digitales Wachstum in der deutschen Verwaltung. Ministeriumsnahe Behörden oder Agenturen, wie etwa das *ZenDiS*, sind dort eher politisch gesteuerte Umsetzungsagenturen. Der offene Office365-Ersatz *OpenDesk*[21] gilt hier nur als ein digitales Tool, das möglichst schnell wachsen und skalieren soll. Vielleicht kann es außerdem noch als „geladener Colt auf die Brust Microsofts“ (Wolfgang Schmidt, aktuell noch Kanzleramtschef von Olaf Scholz) dienen, um bessere Vertragsbedingungen für Microsoft Office in der Verwaltung auszuhandeln.

Für eine solche Verwaltungsdigitalisierung braucht es politisch abhängige Behördenleitungen, die weniger Fragen stellen und vor allem für die Umsetzung sorgen. Mehr Rollout von souveränen Lösungen, weniger Politik für das Ökosystem um Open Source an und für sich.

Nur wird dieses Wachstum kein nachhaltiges sein. Open Source ist kein kostenfreier Weg für Software. Sondern es braucht außerdem die nachhaltige Investition in ein Ökosystem und seine Akteur:innen, die einander bestmöglich unterstützen, um gemeinsam besser zu sein als jeder für sich allein. Communitypflege eher im Sinne von Care-Arbeit, nachhaltige Finanzierung für meist allein dastehende Maintainer:innen von Softwarepaketen und die Schaffung von politisch günstigen Rahmenbedingungen für all das. Das aber ist weit mehr als nur Code und Wachstum. Dafür braucht es Menschen, die wie Jutta Horstmann tief und glaubwürdig in der Open Source Community verwurzelt sind. Menschen, die mehr sind als bloße Geschäftsführer:innen.

Am Ende könnte die goldene Hand des Wachstums – die schnelle Skalierung von Open-Source-Lösungen wie OpenDesk – zwar kurzfristige Erfolge liefern. Nur ist das kein nachhaltiges Wachstum, denn am Ende leidet dauerhaft die Open-Source-Community, die dieses schnelle Wachstum überhaupt erst ermöglicht hat.

Ähnlich wie Midas goldene Hand wird dann zwar viel Wachstum geschaffen. Es ist aber ein Wachstum, das die Beteiligten verhungern und verdursten lässt.

Die eiserne Hand des Staates

Ein weiteres vorherrschendes Thema im Koalitionsvertrag (2615 ff.) ist die innere Sicherheit. Einmal mehr wird hier eine Zeitenwende gefordert. Und diese Zeitenwende lässt sich nur als der Versuch einer eisernen Hand des Staates beschreiben.

Der *Chaos Computer Club*[22] beschreibt den Koalitionsvertrag zu Recht als ein Diktaturbesteck, schlüsselfertig und maßgeschneidert. Markus' Kommentar[23] artikuliert meine erste Reaktion auf den Koalitionsvertrag in diesem Aspekt sehr treffend: Das Kopieren menschenfeindlicher Politik führt nur zu mehr menschenfeindlicher Politik.

Ein Staat, dessen eiserne Hand im Sinne der „Sicherheit“ immer mehr Bereiche auch durch digitale Mittel mit Überwachung und Repression widerspruchslos ergreift, wird irgendwann kein demokratischer Staat mehr sein. Denn in einem demokratischen Staat kann es kein uneingeschränktes Vertrauen in ihn und seine Sicherheitsbehörden geben. Wenn der Koalitionsvertrag im Abschnitt zu innerer Sicherheit zumindest einen Abschnitt hat, der wichtig ist, dann ist es dieser (2707 ff.), wenngleich ich diesen bewusst anders lesen muss:

Bianca Kastl

Bianca Kastl ist Entwicklerin und unterstützt seit Beginn der Corona-Pandemie Gesundheitsämter bei der Digitalisierung. Von dort aus schaut sie kritisch auf die digitale Infrastrukturen, die im öffentlichen Gesundheitswesen genutzt werden – vor allem auf deren Schwachstellen.

Es ist die gesamtstaatliche und gesellschaftliche Verantwortung, jedweder Destabilisierung unserer freiheitlichen demokratischen Grundordnung entgegenzuwirken und dabei auch unsere Sicherheitsbehörden nicht allein zu lassen.

Als Zivilgesellschaft sollten wir den Sicherheitsbehörden niemals widerspruchslos vertrauen. Und bei dem schleichenden bis offensiven Versuch, einen Überwachungsstaat zu schaffen, sollten wir ganz und gar nicht schweigen. Denn das führt nur in den Faschismus. Und der ist für uns alle alles andere als golden.

Referenz: https://netzpolitik.org/2025/degitalisierung-falsche-mythen/

Anmerkungen

1 *https://netzpolitik.org/2025/sondervermoegen-fuer-infrastruktur-geld-ist-nicht-alles/*
2 *https://netzpolitik.org/2025/koalitionsvertrag-das-planen-union-und-spd-in-der-netzpolitik/*
3 *https://www.tagesschau.de/eilmeldung/finanzpaket-bundesrat-102.html*
4 *https://www.bitkom.org/Presse/Presseinformation/Sondervermoegen-Bitkom-schlaegt-Digitalpakt-Deutschland-vor*
5 *https://agoradigital.de/projekte/digitalhaushalt*
6 *https://www.deutschlandfunk.de/verschiedene-vorschlaege-zur-verteilung-schleswig-holsteins-ministerpraesident-guenther-fuer-koenigs-100.html*
7 *https://starweb.hessen.de/cache/GVBL/1950/00037.pdf#page=1*
8 *https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/ozg-foederal/themenfelder/themenfelder-node.html*
9 *https://de.wikipedia.org/wiki/Midas*
10 *https://www.heise.de/news/Wettbewerber-Regulierer-muss-gegen-Doppelausbau-der-Telekom-vorgehen-10264666.html*
11 *https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag_2025.pdf*
12 *https://www.calcalistech.com/ctechnews/article/hb4cx29u9*
13 *https://www.bbc.com/news/av/world-africa-66514287*
14 *https://spectrum.ieee.org/midjourney-copyright*
15 *https://www.heise.de/news/Digitale-Souveraenitaet-Bundesinnenministerium-serviert-ZenDiS-Chefin-ab-10349053.html*
16 *https://de.wikipedia.org/wiki/Liste_der_deutschen_Innenminister*
17 *https://de.wikipedia.org/wiki/Zentrum_für_Digitale_Souveränität_der_Öffentlichen_Verwaltung*
18 *https://netzpolitik.org/2024/zentrum-fuer-digitale-souveraenitaet-knappe-ressourcen-fuer-open-source/*
19 *https://netzpolitik.org/2025/zentrum-fuer-digitale-souveraenitaet-bund-legt-offener-verwaltungssoftware-steine-in-den-weg/*
20 *https://www.heise.de/news/Rahmenvertrag-MS-365-Alternative-OpenDesk-soll-die-Bundeswehr-erobern-10342327.html*
21 *https://opendesk.eu/*
22 *https://www.ccc.de/de/updates/2025/ueberwachungshoelle*
23 *https://netzpolitik.org/2025/koalitionsvertrag-wir-sehen-uns-beim-protest/*

Chris Köver, Daniel Leisegang

Interview mit Natascha Strobl: „Wir dürfen uns nicht kaputtmachen lassen“

4. Februar 2025 – *Donald Trump und die Tech-Bros ziehen in den USA nun an einem Strang. Ihre libertär-faschistische Ideologie wirkt bis nach Europa und zieht dabei auch die hiesige politische „Mitte“ in ihren Bann. Die Politikwissenschaftlerin Natascha Strobl hat eine Idee, wie wir uns diesem gefährlichen Sog entziehen können.*

netzpolitik.org: *Vor etwa zwei Wochen konnten wir der Vereidigung Donald Trumps zum 47. US-Präsidenten beiwohnen. In der ersten Reihe saßen mehrere Multi-Milliardäre und Chefs großer Social-Media-Plattformen. Was ist dir durch den Kopf gegangen, als du dieses Bild gesehen hast?*

Natascha Strobl: Das ist wie aus einem dystopischen Roman. Wenn jemand das so geschrieben hätte vor zehn Jahren, hätte ich gesagt, das ist zu platt. Drei der reichsten Männer der Welt, die die größten Social-Media-Plattformen kontrollieren. Ein rechtsextremer bis faschistischer Präsident, der die Demokratie zerschlagen will: Klingt alles nicht so realistisch. Aber es ist Zeit, dass wir der Realität ins Auge blicken. Wir leben diesen dystopischen Roman. Zu lange dachten wir, dass die Demokratie ein Selbstläufer ist. Nun aber sehen wir, dass das gar nicht so ist.

netzpolitik.org: *Was glaubst du, wie wird es im nächsten Kapitel dieses Romans jetzt weitergehen?*

Strobl: Als nächstes werden wir ein Destruktionsprojekt sehen. Die neue US-Regierung unter Trump wird die USA handlungsunfähig machen. Im historischen Faschismus ging es immer um junge Demokratien. In der Geschichte kam der Aspekt, dass das Bestehende erst zerstört werden muss, stets zu kurz. Das ist die Phase, die wir als nächstes sehen werden. Die komplette Nivellierung all dessen, was an demokratischer Struktur besteht. Das reicht von den Gesetzen bis zur Verfassung. Und es wird die handelnden Personen treffen, also etwa die Lehrer:innen und Sozialarbeiter:innen, die Behördenstelle, wo ich meinen Antrag auf Sozialhilfe stelle. All das, was eine Demokratie in ihrem Stoff ausmacht.

netzpolitik.org: *Vor einigen Jahren haben wir noch darüber gesprochen, dass auf Social Media eine Welle auf uns zurollt, die das politische Terrain verändert. Sehen wir hier schon das Ergebnis – ein Bündnis aus einer neurechten Bewegung mit dem Präsidenten der Vereinigten Staaten?*

Strobl: Das sind kommunizierende Röhren. Eine Bewegung und ihr Anführer. Die Bewegung bildet die Avantgarde, und die findet vor allem in den sozialen Medien statt. Der Prozess, den wir auf einer Plattform wie Twitter gesehen haben, wird jetzt überall ablaufen. Das Twitter von einst, mit seiner Idee des schnellen Austauschs, hat Elon Musk aktiv zerstört. Und nun gibt es das Ziel, eine ähnliche Zerstörung in der analogen Welt zu vollziehen.

Die Wurzel des Übels

netzpolitik.org: *Mark Zuckerberg tritt dabei offenkundig in Elon Musks Fußstapfen. Er will unter anderem die Inhaltemoderation bei Facebook und Instagram stark zurückfahren. Worauf müssen wir uns einstellen?*

Strobl: Wie wir gesehen haben, ist Zuckerberg ein absoluter Mitläufer. Was seine Ankündigungen etwa für Instagram bedeuten, werden wir vermutlich erst in einigen Monaten sehen. Das wird nicht so rasch gehen wie auf Twitter, weil das Tempo auf Instagram nicht so hoch ist. Aber der Weg kann nur einer nach unten sein. Auf Twitter sieht man heute Posts mit zig tausend Likes, in denen diskutiert wird, ob Hitler im Vergleich zu Churchill nicht doch der Gute war im Zweiten Weltkrieg. Auch vermeintlich unpolitische Sachen werden nicht mehr moderiert, etwa junge Mädchen, die sich gegenseitig in ihren Essstörungen bestätigen.

netzpolitik.org: *Welche Idee steckt hinter dieser Ankündigung?*

Strobl: Dahinter steckt ein sozialdarwinistischer Freiheitsbegriff. Jeder ist für sich selbst verantwortlich und die, die nicht durchkommen, haben halt Pech gehabt. Das ist ein Freiheitsbegriff, den wir auf ökonomischer Ebene aus dem Neoliberalismus kennen. Und völkisch konnotiert gibt es ein sehr ähnliches Freiheitsverständnis auch im Faschismus: Die starken gesunden Völker im historischen Faschismus triumphieren, alle anderen gehen unter. Aktuell sehen wir diese seltsame Vermischung aus libertärem und faschistischem Gedankengut, was eigentlich nicht zusammengehen sollte, was es aber jetzt ganz klar tut. Auch weil beide sich die gleiche ideologische Wurzel teilen.

netzpolitik.org: *Das zeigte sich zuletzt ja auch explizit in dem Hitlergruß von Elon Musk. Musk fährt außerdem Verbalattacken gegen Regierungen in Großbritannien und in der EU. In Deutschland unterstützt er außerdem offensiv die AfD. Welches Ziel verfolgt er dabei?*

Strobl: Er tut genau das, was die extreme Rechte den Linken gerne vorwirft: Ein Mensch mit unheimlich viel Geld nimmt Einfluss auf diverse Demokratien, damit die seine Politik umsetzen. Er unterminiert demokratische Wahlen, eine demokratische Medienöffentlichkeit und er tut dies mit einem Vermögen, das nicht mehr greifbar ist. Das zeigt, wie demokratiegefährdend solch eine Vermögenskonzentration ist. Selbst wenn Musk Milliarden Dollar verliert, ist ihm das vermutlich egal. Wie aber kann die Politik jemanden wie Musk mit Sanktionen einhegen, wenn es diesem egal ist, ob er noch Aufträge aus Europa bekommt. Hier droht eine Oligarchie – in diesem Fall die eines einzelnen Mannes, der so reich ist, wie es sich die Oligarchen vor 100 Jahren nicht einmal erträumt haben.

Obsession mit der Geburtenrate

netzpolitik.org: *Welche Ziele verfolgt Musk mit alledem?*

Strobl: Das ist eine politische Radikalisierung, die sich in den vergangenen fünf, sechs Jahren vor unser aller Augen vollzogen hat. Und die klar von einer faschistischen Ideologie beeinflusst ist. Natürlich verfolgt er dabei auch wirtschaftliche Ziele. Musk

The Unholy Alliance: The Rise of the Far-Right and Digital Capitalism, Ersteller: Mathias Rodatz , CC BY-SA 4.0

will nicht, dass Twitter in der EU strenger reguliert oder gar verboten wird. Aber Twitter ist nicht seine Haupteinnahmequelle. Ich fürchte, Musk ist so abgesichert, dass man ihm wirtschaftlich nichts anhaben kann.

netzpolitik.org: *Welche seiner Äußerungen haben dich besonders alarmiert?*

Strobl: Als er anfing, über Geburtenraten zu sprechen, haben meine Alarmglocken besonders laut geschrillt. Das Thema ist in der extremen Rechten sehr wichtig. Vor allem im rechtsextremen Terrorismus spielt es eine zentrale Rolle. Unter anderem für den Attentäter von Christchurch war die Geburtenrate das wichtigste Thema. Die Muslime bekommen zu viele Kinder, so deren Sorge, und die Europäer – ein Code für die Weißen – bekommen zu wenige.

Musks Obsession mit Geburtenraten ist aus meiner Sicht ein klarer Indikator für seine Radikalisierung. Verknüpft man das mit seinem Mars-Projekt, wird es regelrecht dystopisch. Es klingt wie Science-Fiction, wenn man es ausspricht. Am Ende könnte Musk derjenige sein, der auswählt: Wer darf leben, wenn die Erde brennt, und wer nicht. Hört man Musk genau zu, dann benennt er das auch als sein Ziel. Und man sollte den reichsten Mann der Welt hier ernst nehmen, auch wenn ein solches Szenario wahrscheinlich in ferner Zukunft liegt.

Fehlende mediale Einordnung

netzpolitik.org: *Wir können uns dem doch kaum entziehen. Die Medien berichten aktuell über nahezu alles, was Trump oder Musk tun und verkünden.*

Strobl: Ich verstehe das natürlich. Wie können Medien nicht darauf reagieren, was der Präsident der Vereinigten Staaten von Amerika sagt. Das gleiche gilt für Musk, der jetzt so etwas wie ein Schattenpräsident ist. Gleichzeitig laugt diese Strategie aus. Man hechelt nur noch hinterher und bleibt zugleich immer an der Oberfläche. Und den Medien fehlt offenbar die Möglichkeit, das alles noch einzuordnen. Sind Trumps sieben dumme Tweets heute genauso wichtig wie die Ankündigung, dass er Grönland besetzen will? Ist Grönland ebenso wichtig wie die Entlassung von tausenden Regierungsmitarbeitenden? Eigentlich ist es die

Aufgabe von politischer Berichterstattung, das einzuordnen und der Aufreibungsstrategie etwas entgegenzusetzen.

netzpolitik.org: *Viele Kampagnen der Neuen Rechten finden auf internationaler Ebene statt. Ob in den USA, in Großbritannien oder in Deutschland: Die Themen ähneln sich. Wie kommt das?*

Strobl: Ganz pragmatisch. Da werden viele Bälle in die Social-Media-Arena geschossen und worüber sich die Menschen aufregen, das wird dann weiterverfolgt. Wenn man sich die entsprechenden Accounts anschaut, sieht man, dass vieles gar nicht aufgenommen wird. Aber wenn so ein Kulturkampf-Thema steil geht, wird das überall aufgegriffen.

netzpolitik.org: *Hast du ein Beispiel?*

Strobl: Diese Drag Queen Reading Hour, eine Veranstaltung, wo Drag Queens Kindern Bücher vorlesen. Das wäre an sich höchstens etwas für die Lokalnachrichten. Aber auf einmal redeten online alle darüber, was in irgendeiner Bibliothek im Bundesstaat New York passiert. Diese Geschichten werden von der neuen Rechten weltweit aufgegriffen. Das passiert aber nicht per Absprache, sondern organisch, weil die jeweiligen Akteure sehen, dass es woanders funktioniert. Sobald die Aufregung groß genug ist, sagen sie dann, dass das in Wien, Berlin oder London passiert ist. Fotos werden aus dem Kontext genommen, das Ganze rückt immer näher. Am Ende diskutieren wir auch bei uns darüber, ob derartige Lesungen verboten sein sollten. Obwohl keine solche Lesung irgendwo in Deutschland stattgefunden hat.

netzpolitik.org: *Welche Rolle spielen staatliche Akteure in dieser Dynamik?*

Strobl: Deren Rolle darf man nicht unterschätzen. Es ist sehr, sehr schwer zu unterscheiden, was von realen Nutzer:innen und was von Bots stammt, die gezielt ein bestimmtes Thema streuen – als gezielte Angriffe auf die Demokratie. Wir sehen es gerade wieder auf Bluesky. Auch dort gibt es schon Accounts, die nichts anderes tun, als eine bestimmte Weltsicht zu verbreiten, wo aber ziemlich sicher keine realen Personen dahinter sitzen.

„Es braucht drastischere Maßnahmen"

netzpolitik.org: *Seit Jahren diskutieren wir über Desinformationskampagnen. In der EU gibt es Gesetze, die Plattformen zur Moderation von Falschinformationen verpflichten. Das jetzt von Meta abgeschaffte Fact-Checking sollte dafür sorgen, solche Kampagnen zu entlarven. Hat das rückblickend geholfen im Kampf gegen die neue Rechte?*

Strobl: Es ist kein Fehler, Inhalte zu moderieren. Ich möchte diese Arbeit auf keinen Fall schlechtreden. Aber im Kampf um die Demokratie ist das zu wenig. Dafür braucht es drastischere Maßnahmen, um in irgendeiner Form Zugriff auf einzelne Nutzer:innen zu bekommen. Vor allem dann, wenn es um Gewalt geht.

netzpolitik.org: *Du meinst so etwas wie die Vorratsdatenspeicherung oder Quick Freeze?*

Strobl: Ich will gar nicht sagen, was das für ein Verfahren sein sollte. Mir sind die Gefahren bewusst, die damit einhergehen. Aber wir haben es in den sozialen Medien mit Menschen zu tun, die aktiv politische Gewalt ausüben. Die kann man nicht wegmoderieren und wegdiskutieren. Nur mit Debunking, mit nett Zureden oder Community Notes wird man das nicht loswerden.

netzpolitik.org: *Eine Kritik an der Vorratsdatenspeicherung[1] ist, dass diese Form der anlasslosen Massenüberwachung im Internet ebenfalls die Demokratie beschädigt.*

Strobl: Das ist mir bewusst. Aber der Schaden an der Demokratie ist auch groß, wenn der faschistische Schlägertrupp einfach so weiter machen darf. Das ist nicht Hass im Netz, sondern politische Gewalt, die da verübt wird. Und wir brauchen Maßnahmen, die dem beikommen. Ich weiß, dass das eine kontroverse Meinung ist. Gleichzeitig sollten wir anerkennen, dass der bestehende Prozess nichts für die Opfer tut.

„Du stehst da mit null Schutz"

netzpolitik.org: *Welche Verbindung siehst du zwischen Desinformationskampagnen und den gezielten persönlichen Gewaltandrohungen, von denen du sprichst?*

Strobl: Desinformation wird dazu genutzt, um gezielt gegen Personen, Gruppen oder Institutionen zu hetzen. Das haben wir bei der österreichischen Landärztin Lisa Maria Kellermeyer gesehen …

netzpolitik.org: *… bei der Hasskriminalität mit fatalen Folgen bagatellisiert wurde[2].*

Strobl: Ja, da hieß es dann: Die hat gesagt, man soll alle, die nicht geimpft sind, einsperren. Daraus ist dann geworden: Fahrt sie nieder! Es geht unglaublich schnell, dass eine solche Kampagne als Waffe gegen jemanden persönlich eingesetzt wird. Das hat unmittelbar Auswirkungen auf Leute. Und es ist ja nicht so, als ob die Staaten dann Personenschutz geben würden. Du bist keine prominente Person, sondern ein Niemand. Auch dann, wenn du in den sozialen Medien auf einmal zur Person des Tages erkoren wurdest und von zehntausenden Leute durch die Arena gehetzt wirst. Du stehst da mit null Schutz.

Denkfehler und Versäumnisse

netzpolitik.org: *Der Diskurs verschiebt sich spürbar. In dieser Hinsicht ist die neue Rechte in Deutschland bereits sehr erfolgreich. Friedrich Merz und Christian Lindner äußern im Wahlkampf Positionen, die noch vor einigen Jahren als rechtsextrem gegolten hätten. Geht die Strategie der sogenannten Mitte auf, wenn sie die Themen und Positionen von Rechtsaußen übernehmen?*

Strobl: Die Idee dahinter ist schon falsch. Demnach hat die extreme Rechte ja schon recht, nur sagt sie es ein bisschen schmuddelig. Und wenn jetzt dasselbe seriös gesagt wird und mit ein bisschen weniger Geifer, dann könnte man die Wähler:innen zurückholen, so die Hoffnung, und alles wieder in die richtigen Bahnen lenken. Und hier liegt der zweite Denkfehler, nämlich dass man das nur ein wenig umleiten muss, damit wieder alles gut wird.

Deshalb ist auch die aktuell diskutierte Annahme falsch: Wenn wir jetzt genug abschieben, dann lösen sich damit alle Probleme. Das ist ein naiver Diskurs, der kein Problem löst. Aus meiner Sicht traut man sich in der Migrationsdebatte schon nicht mehr zu sagen, dass es tatsächlich Probleme gibt. So wie es überall, wo Menschen zusammenleben, Probleme gibt. Es sind vielleicht sogar Probleme, die wir schon seit langem kennen. Etwa die psychischen Auswirkungen von Flucht. Dieses Problems hätte man sich schon vor zehn Jahren annehmen müssen. Stattdessen hat man die Menschen sich selbst überlassen. Über diese Versäumnisse können wir sprechen.

Man muss den Menschen klarmachen, dass es keinerlei Probleme löst, wenn wir Migration und Asyl auf diese Weise diskutieren. Nicht für die Menschen, die geflohen sind. Und auch nicht für die Menschen, die Angst haben und nicht wissen, wie sie mit Veränderungen zurechtkommen sollen. Und hier müsste man das Ganze vom Kopf auf die Füße stellen. Solange das Thema Migration aber – und das betrifft auch linke Parteien – immer nur so diskutiert wird, wie die extreme Rechte, kommen wir auch nicht raus aus dem Ganzen.

Wir müssen uns diesem diskursiven Sog entziehen, den die extreme Rechte ausübt. Denn er zielt darauf aus, grausam gegen Menschen zu sein.

netzpolitik.org: *Ist die aktuelle Strategie der Mitte, von den Rechten die Positionen zu übernehmen, in anderen Ländern aufgegangen?*

Strobl: Kurzfristig ja. Mittelfristig aber stärkt das in der Regel die extreme Rechte. In Frankreich ist es nur eine Frage der Zeit, bis eine rechtsextreme Partei die Mehrheit bekommt. In Österreich ist das schon der Fall. Dieser Diskurs hat also überall nur der extremen Rechten genutzt. Die einzige Ausnahme, und so ehrlich muss man sein, ist Dänemark. Dänemark hat mittlerweile überaus strikte Asyl- und Migrationsgesetze, eingeführt von den Sozialdemokraten. Ob wir uns das aber zum Vorbild nehmen sollten, lasse ich jetzt mal dahingestellt. Fest steht, dass die Strategie, sich die extremen Rechte als Vorbild zu nehmen, der Demokratie in Deutschland, Frankreich, Österreich, Italien, Ungarn und in der Schweiz geschadet hat.

„Wir müssen unser aller Zukunft in den Blick nehmen“

netzpolitik.org: *Wo siehst du Orte im Netz, um sich gegen den grassierenden Rechtspopulismus und Rechtsextremismus zu vernetzen und zur Wehr zu setzen?*

Strobl: Der eigene Radius wird online immer kleiner. Und es ist auch eine moralische Frage, ob man jetzt noch auf Meta-Plattformen sein sollte oder nicht? Ich bin der Meinung, man sollte sich erst so spät wie möglich von den Plattformen zurückziehen. Wenn man dort über ein großes Netzwerk und damit eine große Reichweite verfügt, dann sollte man diese nicht leichtfertig aufgeben. Auch wenn die Plattformen furchtbar sind. Auch wenn man sich dort mittlerweile auf feindlichem Territorium bewegt. Deswegen lösche ich auch meinen Twitter-Account nicht.

netzpolitik.org: *Das klingt eher defensiv.*

Strobl: Das Bleiben reicht nicht aus. Wir brauchen außerdem eine politische Alternative. Und diese politische Alternative darf nicht immer nur der Antagonismus sein. Wir dürfen uns nicht nur fragen, was die extreme Rechte macht – um dann dagegen zu sein.

Stattdessen müssen wir uns darüber Gedanken machen, wie die Welt in naher Zukunft aussehen soll. Wie wollen wir in fünf Jahren miteinander leben? Wie wollen wir zusammen arbeiten, Kinder erziehen? Wie möchten wir unsere Nachbarschaften gestalten?

Wenn wir solche Diskussionen miteinander führen, hat die extreme Rechte keine Chance. Weil sie dazu rein gar nichts beitragen kann. Und deswegen ist es so wichtig, sich ihrem Sog zu entziehen. Weil die extreme Rechte auch nur ein Symptom der Krise ist. Und wir müssen diese Krisen angehen. Und das geht nur, wenn wir unsere Gesellschaft, unsere Demokratie und unsere Wirtschaft in den Blick nehmen – wenn wir den gesellschaftlichen Wandel angehen. Nur wenn wir unser aller Zukunft in den Blick nehmen, können wir auch etwas zum Guten verändern.

Andernfalls verzweifeln wir an der Situation, in der wir uns jetzt befinden. Und dieses Verzweifeln hilft uns nicht, hilft der Welt nicht, es macht uns nur kaputt. Und gerade jetzt dürfen wir uns nicht kaputtmachen lassen.

Referenz: https://netzpolitik.org/2025/interview-mit-natascha-strobl-wir-duerfen-uns-nicht-kaputtmachen-lassen/

Anmerkungen

1 *https://netzpolitik.org/2022/kampf-gegen-die-vorratsdatenspeicherung-kein-appetit-auf-noch-eine-blutige-nase/*
2 *https://netzpolitik.org/2022/polizeibehoerden-wie-hasskriminalitaet-bagatellisiert-wird/*

Natascha Strobl, Chris Köver und Daniel Leisegang

Natascha Strobl ist Politikwissenschaftlerin aus Wien. Sie forscht zu Rechtsextremismus, insbesondere der Neuen Rechten. Sie publiziert in zahlreichen europäischen Publikationen wie *Die Zeit*, *Falter* (Österreich) und *Dagens Nyheter* (Schweden).

Autoreninformationen zu **Chris Köver** und **Daniel Leisegang** siehe Seite 54

Jan Grapenthin

Mythos Desinformation?

27. Februar 2025 – *Gerade vor Wahlen wird immer wieder vor den Folgen von Desinformationskampagnen gewarnt. Eine umfangreiche Studie kommt nun zu dem Schluss, dass sich die Auswirkung von Desinformation auf den Ausgang von Wahlen nicht eindeutig nachweisen lässt. Fest stehe aber, dass die Warnungen selbst negative Effekte haben.*

Vor jeder Wahl ist die Sorge vor Desinformationskampagnen groß. Dahinter steht die Annahme, dass in- wie ausländische Akteure versuchen, Menschen gezielt in ihrer Wahlentscheidung zu beeinflussen. Insbesondere in den sozialen Medien würden Bürger:innen mit Falschinformationen überflutet, was sich dann auf ihre politische Überzeugung und letztlich auf den Wahlausgang auswirke. Auch im Vorfeld der jüngsten Bundestagswahl gab es etliche[1] solcher[2] Warnungen[3].

Doch wenige Tage vor der Wahl gaben Forschende in einer Online-Veranstaltung des *Science Media Centers*[4] in Teilen Entwarnung. Zwar habe es auch in diesem Wahlkampf erneut zahlreiche Versuche der Einflussnahme gegeben. Deren Wirkung sei jedoch begrenzt gewesen, so der Tenor. Gestützt wird dieses Fazit von einer umfangreichen Studie des *Observatory on Information and Democracy*[5], die bereits im Dezember vergangenen Jahres erschien und Ende Januar in Berlin vorgestellt wurde[6]. Auch sie stellt gängige Annahmen über den Einfluss von Desinformationen infrage.

Demnach lässt sich kein klarer Zusammenhang zwischen der Verbreitung von Desinformation und dem Ausgang von Wahlen nachweisen. Ein entsprechender wissenschaftlicher Nachweis sei schon deshalb schwierig, weil die Tech-Konzerne die dafür erforderlichen Daten nicht herausgäben.

Dass dennoch immer wieder eindringlich vor Desinformation gewarnt wird, könnte aus Sicht der Studien-Autor:innen negative Auswirkungen haben, weil so das Misstrauen in der Gesellschaft geschürt werde.

Unzureichende Datengrundlage

Für die Meta-Studie werteten die Forschenden mehr als 2700 internationale Studien aus den vergangenen fünf Jahren aus. Das überraschende Ergebnis lautet, dass ein unmittelbarer Einfluss von Desinformation auf demokratische Prozesse nicht empirisch nachgewiesen werden kann.

Es sei kaum möglich, so die Autor:innen der Studie, einen wissenschaftlichen Nachweis für den Zusammenhang zwischen der Verbreitung von Desinformation, einer zunehmenden gesellschaftlichen Polarisierung und der politischen Beteiligung zu erbringen. So sei es überaus kompliziert, die menschliche Entscheidungsfindung zu simulieren. Außerdem geben die großen Tech-Konzerne kaum Daten heraus, die Forschende für entsprechende Untersuchungen benötigten.

„Man kann nicht behaupten, dass Desinformation einen substanziellen Einfluss auf individuelle oder gesellschaftliche Meinungsbildungsprozesse hat, ohne dies nachweisen zu können", sagt Matthias C. Kettemann[7], einer der Studien-Autor:innen, „Und wenn man es nicht nachweisen kann, sollte man es auch nicht behaupten." Aus Sicht von Kettemann[8] befindet sich die Desinformationsforschung daher auch „in einer Krise".

Warnungen vor Desinformation haben negative Folgen

Eines lässt sich aus Sicht der Forschenden jedoch mit relativer Gewissheit feststellen: Wird zu viel vor Desinformationen gewarnt, kann dies Misstrauen gegenüber jeder Art von Informationen schüren.

> *„Einige Untersuchungen finden keine direkten Auswirkungen von Fehl- und Desinformation auf die politische Polarisierung oder das Wahlverhalten. Andere wiederum zeigen […] den geradezu gegenteiligen Effekt, wonach Bemühungen, das Bewusstsein für Fehl- und Desinformation zu schärfen, zu Misstrauen gegenüber seriösen Informationen führt."*

Die Forschenden plädieren für eine sachlichere Auseinandersetzung mit dem Thema. Sie fordern, sich stärker auf demokratische Willensbildung und den sozialen Zusammenhalt zu konzentrieren. „Wir würden empfehlen, etwas distanzierter über Desinformation zu berichten, ohne infrage zu stellen, dass es Desinformation gibt", sagt[9] Kettemann.

Außerdem weisen die Studien-Autor:innen darauf hin, dass die Tech-Konzerne die Nutzer:innendaten kontrollierten und damit auch das Wissen. Sie fordern strengere Regeln, um diese Macht zu begrenzen.

Referenz: https://netzpolitik.org/2025/meta-studie-mythos-desinformation/

Jan Grapenthin

Jan Grapenthin ist Informatiker mit einem Bachelor-Abschluss in Data Science and AI. Aktuell studiert er Politikwissenschaften. Am Herzen liegen ihm besonders Themen rund um Desinformation, Big Tech und sogenannter KI.

Anmerkungen

1 *https://www.dw.com/de/bundestagswahl-innenministerium-warnt-vor-desinformation-2025-deutschland-wahl-wahlen-berlin-v2/a-71701943*
2 *https://www.spiegel.de/netzwelt/web/bundestagswahl-russische-troll-gruppe-verbreitet-offenbar-fake-videos-zur-briefwahl-a-325b8c89-8dae-4adc-ada9-f8d9ab6dd9f2*
3 *https://www.ndr.de/nachrichten/info/Desinformation-vor-der-Wahl-ist-Gefahr-fuer-die-Demokratie,wahldesinformation100.html*
4 *https://www.youtube.com/watch?v=4qAgt4ttzBs*
5 *https://observatory.informationdemocracy.org/wp-content/uploads/2024/12/rapport_forum_information_democracy_2025.pdf*
6 *https://www.hiig.de/events/international-observatory-on-information-and-democracy-oid-a-major-new-report-on-the-state-news-media-ai-and-data-governance/*
7 *https://www.wissenschaftskommunikation.de/wir-muessen-nicht-den-abgesang-auf-die-demokratie-anstimmen-82841*
8 *https://www.tagesspiegel.de/wissen/uberschatzte-desinformation-unterschatzte-datenmacht-sind-soziale-medien-die-grosste-gefahr-fur-die-demokratie-13024540.html*
9 *https://www.tagesspiegel.de/wissen/uberschatzte-desinformation-unterschatzte-datenmacht-sind-soziale-medien-die-grosste-gefahr-fur-die-demokratie-13024540.html*

Anna Biselli, Chris Köver, Daniel Leisegang, Ingo Dachwitz, Markus Reuter, Martin Schwarzbeck, Sebastian Meineck

Koalitionsvertrag: Das planen Union und SPD in der Netzpolitik

9. April 2025 – *Nach recht kurzen Verhandlungen haben Union und SPD heute ihren Koalitionsvertrag vorgestellt. Wir analysieren, welchen* Politikwechsel *Schwarz-Rot anstrebt und was dieser für die digitalen Freiheitsrechte bedeutet.*

„Sie werden viel von dem, was Sie vermutet haben, nicht finden." Das kündigte CDU-Parteichef Friedrich Merz bei der heutigen Pressekonferenz im Paul-Löbe-Haus des Bundestags an. Gemeinsam mit Markus Söder (CSU) sowie den SPD-Vorsitzenden Saskia Esken und Lars Klingbeil stellte er dort den Koalitionsvertrag[1] vor. Das 144-seitige Papier soll die Grundlage für eine künftige, schwarz-rote Regierung bilden. Zuvor müssen ihm noch die Mitglieder der SPD sowie die entsprechenden Gremien von CDU und CSU zustimmen.

Was das für Innenpolitik, Grundrechte und die digital- und netzpolitischen Bereiche heißt, haben wir uns angeschaut und hier zusammengefasst.

Überwachung, Bürgerrechte und Polizei: Law and Order steht an

In Sachen Bürgerrechte und Überwachung erwartet uns eine harte Zeit. Das Innenministerium wird an die CSU gehen und Bayerns Ministerpräsident Markus Söder kündigte bei der Pressekonferenz auch direkt *Law-and-Order*-Politik an.

In der Präambel des Kapitels zur Innenpolitik heißt es dementsprechend, dass die Koalition die „europa- und verfassungsrechtlichen Spielräume ausschöpfen" möchte und das „Spannungsverhältnis zwischen sicherheitspolitischen Erfordernissen und datenschutzrechtlichen Vorgaben" neu austariert werden müsse. Die Stoßrichtung ist hier klar.

„Das verlangt auch Sensibilität bei den Sicherheitsbehörden", heißt es weiter – das klingt eindeutig nach Vorschuss-Vertrauen in statt Kontrolle von Behörden.

Union und SPD haben sich erwartungsgemäß auf mehr Internetüberwachung geeinigt – die **Vorratsdatenspeicherung** soll kommen. Im Koalitionsvertrag heißt es: „Wir führen eine verhältnismäßige und europa- und verfassungsrechtskonforme dreimonatige Speicherpflicht für IP-Adressen und Portnummern ein."

Die Bundespolizei soll den **Staatstrojaner** „zur Bekämpfung schwerer Straftaten" bekommen, „ohne Zugriff auf retrograd gespeicherte Daten".

Gesichtserkennung im Netz und auf der Straße

Die umstrittene biometrische Internetfahndung, die eine riesige biometrische Datenbank erfordert[2], soll laut dem Koalitionsvertrag kommen. Für „bestimmte Zwecke" und „unter Berücksichtigung verfassungsrechtlicher Vorgaben und digitaler Souveränität" sollen die Sicherheitsbehörden eine „automatisierte Datenrecherche und -analyse sowie den nachträglichen biometrischen Abgleich mit öffentlich zugänglichen Internetdaten, auch mittels Künstlicher Intelligenz, vornehmen können." Ob das mit der KI-Verordnung der EU vereinbar sein wird, haben Fachleute mehrfach angezweifelt[3], als das Thema beim Sicherheitspaket der Ampel schon einmal aufgekommen war.

Gesichtserkennung und Biometrie möchte Schwarz-Rot nicht nur im Netz, sondern auch auf der Straße ausweiten. Unter „bestimmten, eng definierten Voraussetzungen bei schweren Straftaten" will die Koalition Strafverfolgungsbehörden eine „retrograde biometrische Fernidentifizierung zur Identifizierung von Täterinnen und Tätern ermöglichen." Dazu soll auch die Videoüberwachung an sogenannten „Kriminalitätsschwerpunkten" eingesetzt werden.

Unklar ist, was sich hinter „frühzeitige Erkennung entsprechender Risikopotenziale bei Personen mit psychischen Auffälligkeiten" verbergen könnte. Hintergrund sind Amokfahrten und Attentate in den letzten Monaten. Die Koalition möchte hierzu „eine gemeinsame Risikobewertung und ein integriertes behör-

denübergreifendes Risikomanagement" einführen – was nach Gefährder-Datenbanken klingt.

Zudem möchte die schwarz-rote Koalition „zu Strafverfolgungszwecken den Einsatz von **automatisierten Kennzeichenlesesystemen** im Aufzeichnungsmodus" erlauben.

Kein echtes Bekenntnis zu Verschlüsselung

Ein wirkliches **Bekenntnis zur Verschlüsselung und vertraulicher Kommunikation fehlt** hingegen im Koalitionsvertrag. Die Formulierung „Grundsätzlich sichern wir die Vertraulichkeit privater Kommunikation und Anonymität im Netz" lässt Spielraum für gesetzliche und technische Hintertüren, auch bei der EU-Chatkontrolle.

Mehr Spielraum für Überwachung gibt es durch die **Ausweitung der Straftatenkataloge**, bei denen Telekommunikationsüberwachung erlaubt ist. Die Koalition möchte „die Telefonüberwachung beim Wohnungseinbruchsdiebstahl" entfristen. Zudem soll die Funkzellenabfrage „umfassender" ermöglicht werden.

Problematisch ist auch die Verschärfung von § 89a StGB[4]. Bei der „Vorbereitung einer schweren staatsgefährdenden Gewalttat" und präventiven Maßnahmen gegen diese sollen in Zukunft auch Alltagsgegenstände als relevante Tatmittel gelten – während früher Waffen oder Sprengstoff nötig waren. Wie *LTO* eindrücklich erklärt hat[5], führt das zu einem **Gummiparagrafen**, der die Polizei ermächtigt, alleine aufgrund der angenommenen Gesinnung Wohnungsdurchsuchungen durchzuführen. Gerade im Hinblick auf eine erstarkende AfD ist das eine gefährliche Änderung, welche die Verfolgung unliebsamer Personen ermöglicht.

Weiter „verschärfen" will die Koalition „den strafrechtlichen Schutz von Einsatz- und Rettungskräften, Polizisten sowie Angehörigen der Gesundheitsberufe". Angriffe gegen diese Berufsgruppen waren schon 2017 mit härteren Strafen belegt worden, das war damals schon aus bürgerrechtlichen Gesichtspunkten problematisch[6].

Geheimdienste: Mehr Kompetenzen, weniger Kontrolle

Viele der Pläne zur Innen- und Sicherheitspolitik betreffen auch die Geheimdienste als Teil der Sicherheitsbehörden. Einige Abschnitte im Koalitionsvertrag beschäftigen sich jedoch auch explizit mit Bundesverfassungsschutz, Bundesnachrichtendienst und dem Militärischen Abschirmdienst.

Der Verfassungsschutz soll bei der Bekämpfung von Cyberkriminalität, Spionage und Sabotage gestärkt werden. Ähnlich unkonkret ist die Ankündigung einer grundlegenden **Novellierung des Nachrichtendienstrechts**. Hier soll auch der Datenaustausch neu geregelt werden. Inwiefern, verrät der Koalitionsvertrag nicht – er soll jedoch „effektiv" und „effizient" werden. Konkreter ist da schon der Alarm, den die Bundesdatenschutzbeauftragte jüngst geschlagen hat[7], weil für die **Geheimdienste mehr Freiheiten und weniger Kontrolle** geplant seien. Im Text des Koalitionsvertrages ist die Rede von „zielgerichteteren Kontrollen".

Offenbar hat die Koalitionspartner das Konzept der *Zentralen Stelle für Informationstechnik im Sicherheitsbereich* überzeugt, kurz *ZITiS*. Unter Einbeziehung der Hackerbehörde, die weiterhin keine eigene Rechtsgrundlage hat, soll eine **neue „spezialisierte technische Zentralstelle"** entstehen, die Teil der stärkeren Geheimdienstkonzentration „auf den Cyber- und Informationsraum" sein soll.

Alles neu werden soll auch bei der gesetzlichen Grundlage zum Militärischen Abschirmdienst. Dort haben Union und SPD offenbar hauptsächlich Änderungswünsche bei Sicherheitsüberprüfung und Sabotageschutz. Zuletzt hatte es beispielsweise immer wieder Berichte über Drohnensichtungen bei Militärstandorten[8] gegeben, hinter denen Spionageversuche aus Russland vermutet wurden.

Digitalisierte Migrationskontrolle: Mehr Daten, mehr Austausch

Bei der Schnittmenge von Migration und Digitalem steht ein weiterer **Ausbau des Ausländerzentralregisters (AZR)** ganz vorn. Schon heute ist das AZR einer der ganz großen staatlichen Datentöpfe. Zusätzlich soll der Datenaustausch verbessert werden, was zu noch mehr zugriffsberechtigten Stellen[9] führen könnte. Das alles soll in einem „Gesetz zur Weiterentwicklung der Digitalisierung der Migrationsverwaltung" umgesetzt werden – „zügig" heißt es im Papier.

Ebenso zügig kommen soll die Umsetzung der europäischen GEAS-Asyl-Reform. Die muss sowieso bis 2026 passieren, die neue Bundesregierung hat es hier aber offenbar eilig.

Überraschenderweise werden **Bezahlkarten** nicht explizit in der schwarz-roten Einigung erwähnt. Es finden sich aber mögliche Bezüge im Text. Etwa sollen Anreize vermindert werden, „in die Sozialsysteme einzuwandern". Das war auch eine Begründung zur Einführung der einschränkenden bargeldlosen Karten, obwohl zu bezweifeln ist, wie sehr diese Migrationsmotivation überhaupt existiert.

IT-Sicherheit: Hackerparagraf und Hackback

Die Koalition will die Resilienz Deutschlands stärken, indem sie die IT-Sicherheit verbessert, besonders bei kritischen Infrastrukturen wie beispielsweise Energieversorgern. Für ethische Hacker:innen und Sicherheitsforschende will sie **im Computerstrafrecht Rechtssicherheit** schaffen, gleichzeitig sollen „Missbrauchsmöglichkeiten verhindert" werden. Eine Reform der sogenannten Hackerparagrafen hatte bereits die Ampel-Regierung in Angriff genommen, jedoch wegen des Regierungs-Aus nicht mehr fertig bekommen.

Die **Nationale Cybersicherheitsstrategie** wie auch das Nationale Cyber-Abwehrzentrum sollen fortentwickelt werden und das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu einer Zentralstelle für Fragen der Informations- und Cybersicherheit. Die NIS-2-Richtlinie soll umgesetzt und das BSI-Gesetz novelliert werden. Die aktive Cyberabwehr soll im Rahmen des verfassungsrechtlich Möglichen ausgebaut werden. Das klingt

danach, als könnte bald eine Diskussion um **Hackbacks** wiederkehren.

Digitale Infrastruktur und Breitbandausbau: „Markt vor Staat"

Wenig überraschend will auch die neue Regierung einen flächendeckenden Glasfaser- und Mobilfunkausbau. Ein festes Jahresziel, bis wann das erreicht sein soll, ruft sie nicht aus. Aber sie will ein Beschleunigungsgesetz einführen, das den Ausbau „als überragendes öffentliches Interesse definiert". Zuletzt war ein solches Gesetz bereits fast fertig, die FDP hatte es aber auf den letzten Metern im Bundestag wieder abgewürgt[10].

Wo der Ausbau beispielsweise in dünn besiedelten Gebieten wirtschaftlich nicht lohnenswert ist, sollen Förderprogramme bei Glasfaser und Mobilfunk auf die Sprünge helfen, es gelte aber sonst „Markt vor Staat".

Wie viel Bandbreite bei Breitbandanschlüssen genug ist, soll beständig erhöht werden. Das bleibt in der Tradition der früheren Ampel, die sich im vergangenen Sommer auf eine Erhöhung der Mindestbandbreiten[11] verständigt hatte.

Die Mobilfunkinfrastrukturgesellschaft, ein Projekt des früheren Verkehrsministers Andreas Scheuer (CSU), soll erst einmal weitergeführt werden – zumindest bis die bereits bewilligten Projekte abgeschlossen sind. Bisher ist die Erfolgsbilanz des *Funklochamts* jedoch mehr als mager[12]; eine große Zukunft der Idee ist daher eher unwahrscheinlich. Fortgesetzt werden soll, Satellitentechnologie zum Stopfen von Funklöchern[13] zu nutzen.

Informationsfreiheit und Transparenz: Wolkige Reform-Ankündigung

Das Thema Transparenz von Politik und Verwaltung spielt im Koalitionsvertrag kaum eine Rolle. Wo die Ampel nach den Korruptionsskandalen der späten Merkeljahre vollmundig ein modernes Transparenzgesetz versprach und krachend scheiterte, gibt sich die neue Koalition auffällig schmallippig. Immerhin: Von einer Abschaffung des veralteten **Informationsfreiheitsgesetzes (IFG)** ist nicht die Rede. Dies hatten die Unionsverhandler um Philipp Amthor[14] gefordert und damit einen öffentlichen Aufschrei[15] ausgelöst.

Nun heißt es nebulös, die Regierung wolle das IFG „mit einem Mehrwert für Bürgerinnen und Bürger und Verwaltung reformieren." Wir dürfen gespannt sein, was das künftig CSU-geführte Innenministerium vorschlagen wird. Dass es den praktisch fertigen Gesetzentwurf für ein Bundestransparenzgesetz nochmal aus dem Panzerschrank holt, ist wohl ausgeschlossen.

Partizipation und Zivilgesellschaft: Endlich Rechtssicherheit bei Gemeinnützigkeit?

Das Bundesprogramm **„Demokratie leben!"**, ein Projekt zur demokratischen Teilhabe, will die Koalition fortsetzen. Die CDU hatte zuletzt mit einer über 500 Fragen starken Kleinen Anfrage Organisationen attackiert[16], von denen viele über ebendieses Programm gefördert werden. Es soll nun in Bezug auf seine Wirkung unabhängig überprüft werden.

Als Ergänzung zur repräsentativen Demokratie will die neue Regierung zudem „dialogische Beteiligungsformate wie zivilgesellschaftliche Bürgerräte des Deutschen Bundestages" fortsetzen. Die Koalition will zudem das Ehrenamt stärken, indem sie die Ehrenamts- und Übungsleiterpauschale erhöht sowie die Freigrenze für den ehrenamtlichen sowie wirtschaftlichen Geschäfts- und Zweckbetrieb. Das **Datenschutz-, Gemeinnützigkeits-, Vereins- und Zuwendungsrecht** soll diesbezüglich vereinfacht werden. Für den Bundesfreiwilligendienst und das Freiwillige Soziale Jahr soll es mehr Stellen und mehr Taschengeld geben.

Zudem sollen Vereine als Bildungsorte anerkannt werden, sodass Förderungen von Weiterbildungsangeboten für Übungsleiter:innen und Trainer:innen möglich sind. Als Demokratieschulung soll allen jungen Menschen der Besuch von Gedenkstätten ermöglicht werden. Die Gedenkstätten selbst sollen mit einem Investitionsprogramm unterstützt werden.

„Im Sinne der flächendeckenden **Versorgung mit journalistischen Angeboten** schaffen wir mit Blick auf die Gemeinnützigkeit Rechtssicherheit", heißt es im Koalitionsvertrag. Das hatte bereits die letzte Regierung versprochen, eine wirksame Regelung war aber unter anderem am Widerstand der Länder gescheitert. Der Katalog der gemeinnützigen Zwecke soll modernisiert werden, das Gemeinnützigkeitsrecht wie auch die Gemeinnützigkeitsprüfung für kleine Vereine vereinfacht. „Wir erkennen die Gemeinnützigkeit des E-Sports an", heißt es zudem.

Verwaltungsdigitalisierung: Bürgerkonto und Datenaustausch werden Pflicht

Schwarz-Rot will noch in diesem Jahr eine „ambitionierte Modernisierungsagenda für Staat und Verwaltung" erarbeiten. Im Zuge dessen soll auch die Bundesverwaltung ressortübergreifend modernisiert werden und es kommt ein eigenes Ministerium für „Digitalisierung und Staatsmodernisierung", das in CDU-Hand liegen soll.

Die Koalition setzt dabei auf das Leitbild einer „vorausschauenden, vernetzten, leistungsfähigen und nutzerzentrierten Verwaltung". Dafür will sie „insbesondere Vorschläge der Initiative für einen handlungsfähigen Staat aufgreifen"[17].

Künftig sollen Behörden ausschließlich **digital und antragslos** arbeiten. So sollen Eltern nach der Geburt eines Kindes in Zukunft automatisch einen Kindergeldbescheid erhalten. Außerdem sollen Abläufe durch den Einsatz sogenannter Künstlicher Intelligenz effizienter werden. Dafür brauche es ein „offeneres und positiveres Datennutzungsverständnis".

Als Voraussetzung dafür will die Koalition auf allen staatlichen Ebenen die Verfahrensabläufe vereinheitlichen. Bürger:innen erhalten **verpflichtend ein Bürgerkonto und eine digitale Identität**.

Verwaltungsleistungen sollen dann über eine zentrale Plattform abrufbar sein. Ihre Daten müssen Bürger:innen nur einmal ein-

geben, Unterlagen können sie digital einreichen. Schwarz-Rot will ein „Doppelerhebungsverbot" erlassen und Behörden zum Datenaustausch verpflichten. Außerdem will die Koalition die **Registermodernisierung** vorantreiben.

Um die **digitale Souveränität** zu stärken, setzt sich Schwarz-Rot – anknüpfend an die Deutsche Verwaltungscloud-Strategie – für souveräne Cloudplattformen ein. Und sie will offene Schnittstellen, offene Standards und Open Source „gezielt vorantreiben".

Als Partner nennt der Koalitionsvertrag hier explizit das *Zentrum Digitale Souveränität* (ZenDiS), die *Sovereign Tech Agency* und die *Bundesagentur für Sprunginnovationen* (Sprind). Hier hat sich in den Verhandlungen offenbar die SPD durchgesetzt[18].

Sprind soll auch öffentliche Finanzierung erhalten, um im Bereich der äußeren Verteidigung tätig zu werden.

Gesundheit: Hürden für Datennutzung abbauen

Deutschland soll zu einem Spitzenstandort für die **Gesundheitsforschung** werden. Dafür will Schwarz-Rot die **Möglichkeiten zur Datennutzung** ausweiten. Sie knüpft damit an die bisherige Politik der Ampel und von Bundesgesundheitsminister Karl Lauterbach (SPD) an.

So will Schwarz-Rot – mit Fokus auf das Forschungsdatenzentrum Gesundheit – Hürden beseitigen, die dem Datenaustausch im Rahmen des Gesundheitsdatennutzungsgesetzes im Wege stehen. Der Schutz von sensiblen Gesundheitsdaten sei dabei „unabdingbar", gleichzeitig will die Koalition „alle berechtigten Interessen" wahren.

Bis 2027 müssen IT-Anbieter einen „verlustfreien, unkomplizierten digitalen Datenaustausch" auf Grundlage einheitlicher Standards sicherstellen.

Die Gematik soll zu einer „modernen Agentur" weiterentwickelt werden, die Akteure im Gesundheitssektor besser miteinander vernetzt. Die Gematik definiert als „nationale Agentur für digitale Medizin" unter anderem die technischen Standards für die elektronische Patientenakte (ePA).

Die **ePA** will Schwarz-Rot in diesem Jahr ausrollen. Noch-Bundesgesundheitsminister Karl Lauterbach (SPD) hatte den bundesweiten Start soeben erneut verschieben müssen[19]. Offenkundig sind die technischen und Sicherheitsprobleme noch zu groß.

Laut Koalitionsvertrag soll der ePA-Rollout stufenweise hin „zu einer verpflichtenden sanktionsbewehrten Nutzung" erfolgen. Aus dem Papier geht nicht hervor, ob nur den Leistungserbringern – also Arztpraxen, Krankenhäuser oder Apotheken – Sanktionen drohen oder auch den Versicherten.

Datenschutz und Datenpolitik: „Im Interesse der Wirtschaft"

In Sachen Datenschutz konnte sich die Union auf ganzer Linie durchsetzen. Wie von ihren Verhandler:innen in der Arbeitsgruppe gefordert, soll die **Datenschutzaufsicht beim Bund zentralisiert** werden. Gleichzeitig soll die Bundesbeauftragte für Datenschutz und Informationsfreiheit künftig auch für **Datennutzung** zuständig sein. Beides geschehe „im Interesse der Wirtschaft". Für zusätzliche Kohärenz soll zudem die bislang informell arbeitende Datenschutzkonferenz von Bund und Ländern im Datenschutzgesetz verankert werden – was allerdings weitgehend überflüssig wäre, wenn die Aufsicht bei der Bundesbeauftragten gebündelt wird.

Unter dem Schlagwort „Datenschutz entbürokratisieren" versprechen Union und SPD zudem Erleichterungen „für kleine und mittlere Unternehmen, Beschäftigte und das Ehrenamt". So sollen nicht-kommerzielle Tätigkeiten und vermeintlich risikoarme Datenverarbeitungen wie Kundenlisten von Handwerker:innen gänzlich **von der Datenschutzgrundverordnung ausgenommen** werden. Bei staatlichen Leistungen soll zudem das **Einwilligungsprinzip abgeschafft** werden. Bürger:innen würden dann wie bei der Elektronischen Patientenakte nicht mehr gefragt werden, ob der Staat ihre Daten nutzen darf, sondern müssten aktiv widersprechen.

Wie auch schon ihre Vorgängerregierungen will Schwarz-Rot eine *Kultur der Datennutzung und des Datenteilens*[20] etablieren. Das seit Jahren in Planung steckende Dateninstitut findet dabei jedoch keine Erwähnung. Neu sind hingegen ein explizites Bekenntnis zur **„Datenökonomie"** und die Ankündigung eines **Datengesetzbuches**, das die vielen unterschiedlichen Regelungen von Bund und EU bündeln soll. Dazu zählen auch neue Initiativen für die Nutzung von Mobilitäts-, Gesundheits- und Forschungsdaten.

Wo es möglich ist, soll es zudem einen **Rechtsanspruch auf Open Data** bei staatlichen Einrichtungen geben. Außerdem soll der Grundsatz *public money, public data* Orientierung bieten. Für den Schutz von Grund- und Freiheitsrechten sowie *Datensouveränität* sollen derweil **Datentreuhänder** und Privacy Enhancing Technologies sorgen. Das alles sind wenig innovative Ideen. Durch den Rückbau beim Datenschutz und die umstrittene Zentralisierung der Aufsicht könnte Schwarz-Rot jedoch das fragile Gleichgewicht aus Datennutzung und Datenschutz *im Interesse der Wirtschaft* erheblich ins Wanken bringen.

Digitaler Verbraucherschutz: Verbot von täuschendem Design

Die wohl wichtigste Ankündigung beim Verbraucherschutz ist die Rückkehr des zuletzt beim Umweltministerium angesiedelten Portfolios ins Justizministerium. Außerdem soll die Verbraucherbildung in den Bereichen Ernährung, Finanzen und Digitales gestärkt werden. Inhaltlich spielt das Thema im Koalitionsvertrag nur eine untergeordnete Rolle. So heißt es beispielsweise vage, dass man nachhaltigen Konsum erleichtern und dem Grundsatz **„Reparieren statt Wegwerfen"** folgen wolle. Wie genau Schwarz-Rot das von der EU eingeführte „Recht auf Reparatur" umsetzen will, verrät sie nicht.

Auf europäischer Ebene will sich Schwarz-Rot zudem „für Verbraucherinteressen im digitalen Raum und insbesondere für die Schließung von Schutzlücken im Verbraucherrecht" einsetzen.

Dazu könnte ein Verbot unlauterer Praktiken wie etwa **täuschendem und süchtigmachendem Design** gehören, für das die Koalition sich einsetzen will. Vage heißt es zudem, eine verbraucherfreundliche Gestaltung von digitalen Angeboten „by design" und „by default" sei das Ziel.

Plattformen und Big Tech: Bestehende Regeln durchsetzen

Die Koalition will eine Abgabe für Online-Plattformen prüfen, die Medieninhalte nutzen. Das macht beispielsweise Google mit den Snippets, die bei den Suchergebnissen angezeigt werden. Die Erlöse sollen dem Medienstandort zugutekommen.

Die Medienaufsicht soll klare gesetzliche Vorgaben erhalten, auf deren Basis sie gegen **Fake News, Hass und Hetze** vorgehen kann. Der massenhafte und koordinierte Einsatz von Bots und Fake-Accounts soll verboten werden. Eine verschärfte Haftung von Social-Media-Plattformen für die Inhalte, die sie transportieren, wird geprüft. Diese sollen strafbare Inhalte entfernen und Desinformation aktiv bekämpfen. Außerdem will die Koalition durchsetzen, dass die Tech-Konzerne ihren Pflichten an Transparenz und Mitwirkung gegenüber der Aufsicht nachkommen. Die Sanktionsmöglichkeiten dazu sollen verschärft werden.

Solche Regeln lassen sich großteils ausschließlich auf europäischer Ebene gestalten und gelten bereits jetzt durch den **Digital Services Act (DSA)**. Dem Digitale-Dienste-Koordinator in Deutschland fehlt es jedoch noch an Personal und Budget. Den DSA wollen die Koalitionäre umsetzen und weiterentwickeln.

Plattformen sollen zudem **Schnittstellen zu Strafverfolgungsbehörden** bereitstellen, damit strafrechtlich relevante Daten automatisiert abgerufen werden können. Die Einführung einer verpflichtenden Identifizierung von **Bots** wird geprüft. Die Accounts von E-Commerce-Unternehmen sollen gesperrt werden können, wenn diese die gesetzlichen Anforderungen nicht erfüllen.

Digitale Gewalt: Zweiter Anlauf und Blick auf Spionage-Apps

Mit einem eigenen **Gesetz gegen digitale Gewalt** ist die Ampel gescheitert[21]; Schwarz-Rot will es nochmal versuchen. Die Stichworte klingen ähnlich wie beim ersten Anlauf: Sperren gegen übergriffige Accounts[22] und mehr rechtliche Handhabe für Betroffene. Das Phänomen digitale Gewalt, ein breiter Sammelbegriff[23], umfasst jedoch deutlich mehr. Die Wunschliste[24] von Fachleuten und Betroffenen ist lang.

Auf zumindest einige bereits seit Jahren diskutierte Punkte geht der Koalitionsvertrag ein, etwa **Stalking und Spionage-Apps**. So möchten die Parteien beim sogenannten Stalking-Paragrafen nachschärfen; damit hatte sich bereits die Große Koalition 2021 befasst[25]. So sollen GPS-Tracker Teil des Paragrafen werden. Die Rede ist auch von verpflichtenden Anti-Gewalt-Trainings für Täter:innen. Für Hersteller von „Tracking-Apps" soll es eine Pflicht geben, „das Einverständnis der Gerätebesitzerinnen und -besitzer regelmäßig abzufragen". Nicht zuletzt unsere Enthüllungen zu Spionage-App *mSpy*[26] zeigten, wie gefährlich solche Apps sein können.

Kinder- und Jugendschutz: Technische Lösungen voran

Um auf die Bedürfnisse von Kindern und Jugendlichen einzugehen, setzt Schwarz-Rot vor allem auf technische Lösungen. Auch wenn viele aktuelle Gesetze Alterskontrollen nur als eine mögliche Maßnahme[27] zum Schutz von Minderjährigen vorsehen, wollen sich die Parteien für **„verpflichtende Altersverifikation"** einsetzen. Mehr noch: „Altersverifikation auf digitalen Endgeräten sollte Standard in Europa sein."

Immerhin wird der **Jugendmedienschutz** nicht allein auf diese Kontrollen reduziert: Auch für „sichere Voreinstellungen" setze man sich ein. Wissenschaftlich bewerten möchten die Koalitionäre zwar nicht den Sinn von Alterskontrollen, aber die „Auswirkungen von Bildschirmzeit und Social-Media-Nutzung", hierzu soll ein Maßnahmenpaket erarbeitet werden. Auch zur Einsamkeit, gerade von Minderjährigen, soll Forschung verbessert werden.

Schwarz-Rot sieht in Technologie auch eine Hilfe für Kinder, die etwa wegen Armut weniger Teilhabe am gesellschaftlichen Leben haben. Man wollte „die Idee weiterverfolgen, Kindern über eine **Teilhabe-App** einen unbürokratischen Zugang zu besonderen schulischen Angeboten sowie Sport-, Musik-, Kultur- und sonstigen Freizeitangeboten" zu ermöglichen.

Es gibt aber auch mindestens ein nicht tech-solutionistisches Vorhaben: eine „Bundesförderung von Childhood-Häusern", also regionale Anlaufstellen für Kinder und Jugendliche, „die körperliche Gewalt oder sexuellen Missbrauch erfahren haben".

KI-Systeme: Hauptsache KI

Sogenannte **Künstliche Intelligenz** zieht sich gleich durch mehrere Kapitel des Koalitionsvertrags. Häufig bleibt jedoch unklar, welche Art von KI-System genau gemeint ist und warum es nützlich sein soll. Hauptsache: KI.

So soll Deutschland etwa „KI-Nation" werden; man werde auf „KI-Sprunginnovationen" setzen und im Rahmen einer „KI-Offensive" eine „AI-Gigafactory" mit großer Rechenleistung starten. „Wir holen mindestens eine der europäischen ‚AI-Gigafactories' nach Deutschland", heißt es im Koalitionsvertrag. Allerdings: In Stuttgart ist bereits eine solche geplant[28], wie noch Ende 2024 der damalige grüne Forschungsminister Cem Özdemir bekanntgab.

Außerdem soll „KI" etwa Familien helfen, digitale Dienstleistungen zu finden; „KI" soll im Gesundheitswesen dabei helfen, bei Behandlungen und Pflege zu dokumentieren – und die Polizei soll „KI-basiert" Daten analysieren. Gerade in der Polizeiarbeit drohen Grundrechtsverletzungen, vor allem bei Datenschutz und Antidiskriminierung[29].

In **generativer KI** – das sind Systeme, die etwa Texte, Bilder, Videos und Audios erstellen können – sieht Schwarz-Rot „wiederum großes künstlerisches und kulturwirtschaftliches Potenzial", zumindest „wenn Urheberrechte gewahrt und künstlich generierte Inhalte erkennbar bleiben". Mit den Bundesländern will die Regierung eine Strategie „Kultur & KI" entwickeln.

Bildung: Eine Schüler-ID für alle

Auf den Digitalpakt 2.0 hatten sich Bund und Länder bereits im vergangenen Dezember geeinigt. Union und SPD wollen damit „die digitale Infrastruktur und verlässliche Administration" ausbauen. Die neue Koalition will außerdem unter anderem **„selbst-adaptive, KI-gestützte Lernsysteme"** voranbringen. Das sind Systeme, die sich an das aktuelle Niveau der Schüler:innen anpassen. Wenn Schüler:innen „bedürftig" sind, sollen sie mit Endgeräten ausgestattet werden. Ob dabei auf einzelne Hersteller gesetzt wird, ist nicht ausgeführt.

Obwohl die Länder für die Schulbildung hauptverantwortlich sind, soll es künftig eine bundesweit kompatible sogenannte **Schüler-ID** geben. Diese Idee wurde bereits auf der Bildungsministerkonferenz[30] diskutiert. Sie soll die Datenübergabe bei Schulwechseln vereinfachen und Bildungswege transparenter machen. Die neue Koalition nimmt sich vor, diese Schüler-ID weiter zu verknüpfen: mit der Bürger-ID.

In der gesamtgesellschaftlichen digitalen Bildung gibt es altbekannte Versprechen. Digitale Kompetenzen sollen gestärkt werden, Menschen sollen resilient werden gegen Desinformation und Manipulation. Dafür wollen die Parteien eine „altersübergreifende digitale Kompetenzoffensive" für alle starten und setzen dabei auf Start-ups, Wirtschaft, Bildungsträger und Sozialverbände.

Urheberrecht: Es allen rechtmachen

Wie bereits Regierende zuvor, wollen Union und SPD einen „fairen Ausgleich der Interessen aller Akteure", also den Urheber:innen, der Wirtschaft und Nutzenden. Neu ist seitdem die große Verbreitung **generativer KI**, hierzu wollen die Parteien eine angemessene Vergütung derjenigen, deren Werke zur Erstellung von KI-Modellen genutzt werden. Auf einer rein nationalen Ebene wird das jedoch schwer durchzusetzen sein.

Bei Musik wollen Union und SPD **Streaming-Plattformen** verpflichten, „Kreative angemessen an den Einnahmen zu beteiligen", nennen aber keine konkreten Vorschläge. Bei anderen Dingen soll die Nutzung von Werken aber auch leichter werden. So etwa bei der Nutzung GEMA-lizenzierter Werke im nichtkommerziellen Bereich. Als Beispiel nennen die Koalitionäre Weihnachtsmärkte[31] oder Sommerfeste in Kindergärten.

Selbstbestimmung: Evaluieren und ändern

Es ist kaum überraschend, aber eine Entkriminalisierung von Schwangerschaftsabbrüchen plant die schwarz-rote Koalition nicht. Eine Expert:innenkommission[32] hatte im vergangenen Jahr zu einer solchen in der Frühphase von Schwangerschaften geraten. Stattdessen ist die Rede davon, sie wolle „Frauen, die ungewollt schwanger werden, in dieser sensiblen Lage umfassend unterstützen, um das ungeborene Leben bestmöglich zu schützen". Für Frauen in Konfliktsituationen soll eine medizinisch sichere und nahe Versorgung möglich sein.

Eine entscheidende Neuerung: Die Koalition will die Kostenübernahme durch die gesetzlichen Krankenkassen „erweitern". Bislang müssen ungewollt Schwangere ihre Abbrüche mit wenigen Ausnahmen selbst bezahlen. Neu ist auch das Bekenntnis, die medizinische Weiterbildung zu „stärken". Derzeit lernen selbst angehende Gynäkolog:innen in der Ausbildung nicht verpflichtend[33], wie man Abbrüche praktisch durchführt.

Ein ungeklärter Punkt während der Verhandlungen war der Umgang mit dem erst kürzlich von der Ampel verabschiedeten Selbstbestimmungsgesetz, das die Änderung von Vornamen und Geschlechtseintrag im Personenstandsregister[34] regelt. Die Union hatte gefordert, es wieder abzuschaffen, konnte sich damit aber offenbar nicht durchsetzen. Im Koalitionsvertrag steht dazu nun, man werde das Gesetz bis spätestens Mitte kommenden Jahres evaluieren. Dabei werde man besonders die Auswirkungen auf Kinder und Jugendliche betrachten sowie den „wirksamen Schutz von Frauen". In den Debatten um das Gesetz waren diese beiden Punkte instrumentalisiert worden, um gegen das Gesetz Stimmung zu machen.

Das Bundesinnenministerium hatte im Gesetzgebungsprozess darauf gedrängt, dass Änderungen von Namen und Geschlechtseintrag automatisch auch an eine Liste von Sicherheitsbehörden gemeldet werden. Kriminelle könnten sonst mit Hilfe des Gesetzes abtauchen, lautete die Argumentation. Diese Klausel hatte der Familienausschuss wieder gestrichen. Nun soll sie laut Koalitionsvertrag über das Namensänderungsrecht nachträglich doch noch eingeführt werden – dann allerdings nicht nur für geänderte Vornamen[35] nach dem Selbstbestimmungsgesetz, sondern für alle Namensänderungen.

Weitere netzpolitische Details

Unsere erste netzpolitische Analyse des Koalitionsvertrags erhebt keinen Anspruch auf Vollständigkeit. Neben den von uns bisher gesetzten Schwerpunkten gibt es ein paar interessante Beobachtungen, die wir zumindest kurz noch erwähnen wollen.

- Wer sich ums Verschwinden von **Bargeld** sorgt, kann sich an diesem Satz aus dem Koalitionsvertrag festhalten: „Das Bargeld als gängige Zahlungsform erhalten wir." Umgekehrt kommt Arbeit auf Verkäufer:innen zu, die bisher nur Bargeld akzeptieren. Schwarz-Rot will sich dafür einsetzen, dass grundsätzlich „mindestens eine **digitale Zahlungsoption** schrittweise" angeboten wird.

- Der **digitale Euro**, an dem die EU gerade arbeitet[36], soll Bargeld ergänzen und „die Privatsphäre der Verbraucherinnen und Verbraucher" schützen.

- Die EU-Richtlinie zum Schutz vor **Einschüchterungsklagen** („SLAPP") muss Deutschland zwar ohnehin umsetzen[37];

Schwarz-Rot möchte es jedoch auch „zeitnah" tun: „um zu verhindern, dass unser Rechtsstaat und unsere Justiz zur Einschüchterung, zum Beispiel von Journalisten sowie zivilgesellschaftlich Engagierten, missbraucht werden."

- Das Wörtchen „alle" ist gefährlich, weil es sehr umfassend ist, dennoch schreibt Schwarz-Rot: „In einer zunehmend vernetzten Welt gewährleisten wir allen die **digitale Teilhabe** und stärken die **Barrierefreiheit**". Dabei kritisieren Fachleute: Selbst das neue Barrierefreiheitsgesetz greift zu kurz[38].

- Ein wenig richtet Schwarz-Rot den Blick auch über den Tellerrand: Man strebe „digitalpolitische Kooperationsabkommen mit globalen Partnern, auch aus dem **Globalen Süden**, an". Dabei dürfte es eine Rolle gespielt haben, dass die USA unter der rechtsradikalen Trump-Regierung ein neues Risiko darstellen.

- Bereits jetzt gibt es in Deutschland aus zahlreichen Gründen Netzsperren[39]. Im Koalitionsvertrag von Schwarz-Rot steht jedoch: „Wir setzen uns für den Erhalt des **freien, fairen, neutralen und offenen Netzes** ein."

Referenz: https://netzpolitik.org/2025/koalitionsvertrag-das-planen-union-und-spd-in-der-netzpolitik/

Anmerkungen

1 *https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag_2025.pdf*
2 *https://netzpolitik.org/2024/sicherheitspaket-eine-biometrische-datenbank-um-alle-zu-finden/*
3 *https://netzpolitik.org/2024/sicherheitspaket-eine-biometrische-datenbank-um-alle-zu-finden/*
4 *https://www.gesetze-im-internet.de/stgb/__89a.html*
5 *https://www.lto.de/recht/hintergruende/h/terrorismus-terror-strafbar-auto-fahrzeug-messer-symbolpolitik*
6 *https://netzpolitik.org/2017/angriffe-auf-polizisten-kein-rechtlicher-bedarf-fuer-eine-strafverschaerfung/*
7 *https://taz.de/Datenschutzbeauftragte-schlaegt-Alarm/!6081232/*
8 *https://www.tagesschau.de/investigativ/ndr-wdr/zunahme-drohnensichtungen-100.html*
9 *https://netzpolitik.org/2023/gesetzesvorschlag-mehr-daten-fuer-das-auslaenderzentralregister/*
10 *https://netzpolitik.org/2025/netzpolitische-bilanz-welche-ihrer-ziele-hat-die-ampel-erreicht-und-welche-nicht/*
11 *https://netzpolitik.org/2024/recht-auf-internet-mindestversorgung-mit-internet-soll-sich-verbessern/*
12 *https://netzpolitik.org/2024/digitales-scheitern-funklochamt-am-ende/*
13 *https://netzpolitik.org/2024/mindestversorgung-mit-internet-starlink-soll-angeblich-deutsche-breitbandluecken-schliessen/*
14 *https://fragdenstaat.de/artikel/exklusiv/2021/05/so-offnete-phillip-amthor-einem-windigen-startup-die-tur-zum-wirtschaftsministerium/*
15 *https://netzpolitik.org/2025/angriff-auf-die-demokratie-breiter-aufschrei-fuer-erhalt-der-informationsfreiheit/*
16 *https://netzpolitik.org/2025/zivilgesellschaft-wir-sind-nicht-neutral/*
17 *https://www.ghst.de/initiative-fuer-einen-handlungsfaehigen-staat*
18 *https://netzpolitik.org/2025/koalitionsverhandlungen-wo-union-und-spd-bei-der-digitalpolitik-streiten/*
19 *https://netzpolitik.org/2025/elektronische-patientenakte-fachleute-zweifeln-weiterhin-an-sicherheitsversprechen/*
20 *https://netzpolitik.org/2021/datenstrategie-der-bundesregierung-die-richtung-stimmt-aber-der-weg-ist-noch-weit/*
21 *https://netzpolitik.org/2024/haette-haette-doch-kein-gesetz-gegen-digitale-gewalt/*
22 *https://netzpolitik.org/2023/geplantes-gesetz-gegen-digitale-gewalt-accounts-sperren-ip-adressen-einfrieren/*
23 *https://netzpolitik.org/2024/stalking-doxing-nacktfotos-was-ist-digitale-gewalt/*
24 *https://netzpolitik.org/2023/digitale-gewalt-acht-klaffende-luecken-im-geplanten-gesetz/*
25 *https://netzpolitik.org/2021/strafrecht-und-stalking-verschaerfter-paragraf-gegen-psychoterror/*
26 *https://netzpolitik.org/mspy-leak/*
27 *https://netzpolitik.org/2025/online-alterskontrollen-nur-fuer-erwachsene/*
28 *https://www.bmbf.de/SharedDocs/Pressemitteilungen/DE/2024/12/101224-ai-factory.html*
29 *https://netzpolitik.org/2025/automatisierte-rasterfahndung-tuer-zu-fuer-palantir-und-co/*
30 *https://www.rnd.de/beruf-und-bildung/schueler-id-als-teil-von-bessere-bildung-2035-was-hinter-dem-konzept-steckt-KAFCWX3335CEJKWR24RSUY6FQ4.html*
31 *https://netzpolitik.org/2023/gema-wucher-staedte-fuerchten-stille-nacht-auf-weihnachtsmaerkten/*
32 *https://www.lto.de/recht/nachrichten/n/bericht-experten-kommission-liberalisierung-entkriminalisierung-schwangerschaftsabbrueche-abtreibung-leihmutterschaft-eizellspende%20*
33 *https://www.br.de/nachrichten/bayern/abtreibungen-papaya-workshops-gegen-luecke-im-medizinstudium,UEMCKLK*
34 *https://netzpolitik.org/2024/selbstbestimmungsgesetz-beschlossen-das-ende-des-wartens/*
35 *https://netzpolitik.org/2024/selbstbestimmungsgesetz-keine-datenweitergabe-an-den-gesamten-sicherheitsapparat/*
36 *https://netzpolitik.org/2024/digitaler-euro-was-soll-mir-das-bringen/*
37 *https://www.consilium.europa.eu/de/press/press-releases/2024/03/19/anti-slapp-final-green-light-for-eu-law-protecting-journalists-and-human-rights-defenders/*
38 *https://netzpolitik.org/2024/digitale-barrierefreiheit-was-das-internet-braeuchte-um-fuer-alle-da-zu-sein/*
39 *https://netzpolitik.org/2025/dns-sperren-deutsche-provider-sperren-hunderte-websites-das-sind-die-gruende/*
40 *mailto:anna@netzpolitik.org*
41 *https://keys.openpgp.org/search?q=anna@netzpolitik.org*
42 *https://mastodon.social/@annskaja*
43 *https://netzpolitik.org/author/chris-koever/*
44 *https://missy-magazine.de/online-magazin/*
45 *mailto:chris@netzpolitik.org*
46 *https://keys.openpgp.org/search?q=0x5E598DD0D37B9F71A88DD92233D38859243016F9*
47 *https://bsky.app/profile/ckoever.bsky.social*
48 *https://mastodon.social/@ckoever*
49 *https://www.blaetter.de/*
50 *http://www.schmetterling-verlag.de/page-5_isbn-3-89657-068-4.htm*
51 *https://www.alternativer-medienpreis.de/preistraeger-2016/daniel-leisegang/*
52 *https://www.eurozine.com/*
53 *mailto:daniel@netzpolitik.org*
54 *https://keys.openpgp.org/search?q=daniel@netzpolitik.org*

55 *https://mastodon.social/@dleisegang*
56 *https://bsky.app/profile/dleisegang.bsky.social*
57 *https://netzpolitik.org/podcast/*
58 *https://netzpolitik.org/2024/xandr-und-die-netzwerke-der-datenhaendler-alternativer-medienpreis-2024-fuer-netzpolitik-org-recherche/*
59 *https://netzpolitik.org/2024/in-eigener-sache-netzpolitik-org-holt-zwei-grimme-online-awards/*
60 *https://www.chbeck.de/dachwitz-hilbig-digitaler-kolonialismus/product/37000393*
61 *mailto:ingo.dachwitz@netzpolitik.org*
62 *https://keys.openpgp.org/search?q=ingo.dachwitz@netzpolitik.org*

Die Autor:innen

Anna Biselli ist Co-Chefredakteurin bei *netzpolitik.org*. Sie interessiert sich vor allem für staatliche Überwachung und Dinge rund um digitalisierte Migrationskontrolle. **Kontakt:** E-Mail[40] (OpenPGP[41]), Mastodon[42], Telefon: +49-30-5771482-42 (Montag bis Freitag jeweils 8 bis 18 Uhr).

Chris Köver[43] ist Redakteurin von *netzpolitik.org* und recherchiert zu Digitaler Gewalt, KI und Migration. Vor allem interessiert sie wie der Staat Technologie gegen Geflüchtete und andere marginalisierte Gruppen einsetzt. Sie hat bei Zeit Online volontiert und anschließend eine eigene Zeitschrift mitgegründet und geleitet: das *Missy Magazine*[44]. Später hat sie bei *WIRED Germany* gearbeitet. Seit 2018 ist sie Teil der Redaktion von *netzpolitik.org*. Chris ist in Rumänien geboren, ihre Familie war Teil der ungarischen Minderheit im Land. Aufgewachsen ist sie im Rheinland.
Kontakt: E-Mail[45] (OpenPGP[46]), BlueSky[47], Mastodon[48], Signal: ckoever.[24]

Daniel Leisegang ist Politikwissenschaftler und Co-Chefredakteur bei *netzpolitik.org*. Zu seinen Schwerpunkten zählen die Gesundheitsdigitalisierung, Digital Public Infrastructure und die sogenannte Künstliche Intelligenz. Daniel war einst Redakteur bei den *Blättern für deutsche und internationale Politik*[49]. 2014 erschien von ihm das Buch *Amazon – Das Buch als Beute*[50]; 2016 erhielt er den *Alternativen Medienpreis*[51] in der Rubrik Medienkritik. Er gehört dem Board of Trustees von *Eurozine*[52] an.
Kontakt: E-Mail[53] (OpenPGP[54]), Mastodon[55], Bluesky[56], Threema ENU3SC7K, Telefon: +49-30-5771482-28 (Montag bis Freitag, jeweils 8 bis 18 Uhr)

Ingo Dachwitz ist Journalist und Kommunikationswissenschaftler. Seit 2016 ist er Redakteur bei *netzpolitik.org* und u. a. Ko-Host des Podcasts *Off/On*[57]. Er schreibt häufig über Datenmissbrauch und Datenschutz, Big Tech, Plattformregulierung, Transparenz, Lobbyismus, Online-Werbung, Wahlkämpfe und die Polizei. 2024 wurde er mit dem *Alternativen Medienpreis*[58] und dem *Grimme-Online-Award*[59] ausgezeichnet. Ingo ist Mitglied des Vereins *Digitale Gesellschaft* sowie der Evangelischen Kirche. Seit 02/2025 ist sein Buch erhältlich: *Digitaler Kolonialismus: Wie Tech-Konzerne und Großmächte die Welt unter sich aufteilen*[60].
Kontakt: E-Mail[61] (OpenPGP[62]), Mastodon[63], Bluesky[64], FragDenStaat[65]

Markus Reuter recherchiert und schreibt zu Digitalpolitik, Desinformation, Zensur und Moderation sowie Überwachungstechnologien. Darüber hinaus beschäftigt er sich mit der Polizei, Grund- und Bürgerrechten sowie Protesten und sozialen Bewegungen. Für eine Recherchereihe zur Polizei auf Twitter erhielt er 2018 den *Preis des Bayerischen Journalistenverbandes*[66], für eine TikTok-Recherche 2020 den *Journalismuspreis Informatik*[67]. Bei *netzpolitik.org* seit März 2016 als Redakteur dabei. Er ist erreichbar unter markus.reuter | ett | netzpolitik.org, sowie auf Mastodon[68] und Bluesky[69]. **Kontakt:** E-Mail[70] (OpenPGP[71])

Martin Schwarzbeck[72] ist seit 2024 Redakteur bei *netzpolitik.org*. Er hat Soziologie studiert, als Journalist für zahlreiche Medien gearbeitet, von ARD bis taz, und war zuletzt lange Redakteur bei Berliner Stadtmagazinen, wo er oft Digitalthemen aufgegriffen hat. Martin interessiert sich für Machtstrukturen und die Beziehungen zwischen Menschen und Staaten und Menschen und Konzernen. Ein Fokus dabei sind Techniken und Systeme der Überwachung, egal ob von Staatsorganen oder Unternehmen.
Kontakt: E-Mail[73] (OpenPGP[74]), Mastodon[75]

Sebastian Meineck ist Journalist und seit 2021 Redakteur bei *netzpolitik.org*. Zu seinen aktuellen Schwerpunkten gehören digitale Gewalt, Databroker, KI und Jugendmedienschutz. Er interessiert sich besonders für Methoden der Online-Recherche; darüber schreibt er einen Newsletter[76] und gibt Workshops an Universitäten. Das *Medium Magazin* hat ihn 2020 zu einem der Top 30 unter 30 im Journalismus gekürt. Seine Arbeit wurde zwei Mal mit dem Grimme-Online-Award prämiert. **Kontakt:** E-Mail[77] (OpenPGP[78]), Sebastian Hinweise schicken[79] | Sebastian für O-Töne anfragen[80] | Mastodon[81]

63 *https://mamot.fr/@roofjoke*
64 *https://bsky.app/profile/roofjoke.bsky.social*
65 *https://fragdenstaat.de/profil/i.dachwitz/*
66 *https://netzpolitik.org/2018/bayerischer-journalisten-verband-ehrt-netzpolitik-org-fuer-recherche-zu-polizeitwitter/*
67 *https://saarland-informatics-campus.de/ueberuns-aboutus/journalismuspreis-informatik/*
68 *https://23.social/@markusreuter*
69 *https://bsky.app/profile/markusreuter.bsky.social*
70 *mailto:markus.reuter@netzpolitik.org*
71 *https://keys.openpgp.org/search?q=markus.reuter@netzpolitik.org*
72 *https://netzpolitik.org/author/martin-schwarzbeck/*
73 *mailto:martin.schwarzbeck@netzpolitik.org*
74 *https://keys.openpgp.org/search?q=martin.schwarzbeck@netzpolitik.org*
75 *https://kolektiva.social/@YoshiXYZ*
76 *https://sebmeineck.substack.com/*
77 *mailto:sebastian@netzpolitik.org*
78 *https://keys.openpgp.org/search?q=sebastian@netzpolitik.org*
79 *https://sebastianmeineck.wordpress.com/kontakt/*
80 *https://sebastianmeineck.wordpress.com/presse-kontakt/*
81 *https://mastodon.social/@sebmeineck*

Anna Biselli

„Mehr Transparenz wäre auch im Sinne der Behörden selbst“

12. Mai 2025 – *Die Überwachungsgesamtrechnung ist ein Mammutprojekt mit vielen Hürden: Misstrauische Polizeibehörden, mangelhafte Zahlen zu Überwachungsmaßnahmen und skeptische Innenminister:innen. Im Interview erklärt Projektleiter Ralf Poscher, warum mehr Transparenz bei Sicherheitsgesetzen auch Behörden nützt.*

Kurz vor dem Regierungswechsel veröffentlichte das Bundesinnenministerium ohne eine begleitende Pressemitteilung die Überwachungsgesamtrechnung auf seiner Website[1]. Das Projekt war ein Vorhaben der Ampel-Regierung und sollte untersuchen, wie sich Überwachungsbefugnisse rechtlich und praktisch auswirken. Eigentlich war im Anschluss noch mehr geplant: Eine Freiheitskommission sollte bei neuen Gesetzesvorhaben eine Art Grundrechte-Check durchführen und aufpassen, dass die Gesamtüberwachungslast nicht zu hoch wird. Dazu wird es unter der neuen schwarz-roten Regierung wohl kaum kommen. Im Interview mit Prof. Dr. Ralf Poscher sprechen wir darüber, was die Überwachungsgesamtrechnung uns dennoch bringen kann.

Poscher hat das Projekt geleitet. Der Rechtswissenschaftler ist geschäftsführender Direktor der Abteilung für Öffentliches Recht am Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht. Mit einem Team hat er fast ein Jahr lang Sicherheitsgesetze von Bund und Ländern sowie konkrete Zahlen zu Überwachungsmaßnahmen ausgewertet.

Überwachungsintensität in mathematische Formeln übersetzen

netzpolitik.org: *An der Überwachungsgesamtrechnung hat ein über 10-köpfiges Forschungsteam rund ein Jahr lang gearbeitet. Aus welchen Disziplinen stammten die Wissenschaftler:innen?*

Poscher: Das war ein interdisziplinäres Team. Viele waren Rechtswissenschaftler, denn ein Großteil der Arbeit war es, eine große Zahl von Vorschriften und Gesetzen zu klassifizieren. Aber es waren auch Kriminologen und Sozialwissenschaftler dabei. Teilweise brauchten wir auch Mathematiker, um die Überwachungslast zu berechnen und die entsprechenden Formeln zu gestalten.

netzpolitik.org: *Wie haben sie die Formeln erarbeitet, die das Überwachungsniveau abbilden sollen?*

Poscher: Das einfachste Formel-Element waren die empirischen Häufigkeiten, wie oft eine Überwachungsmaßnahme durchgeführt wird. Da hatten wir jedoch das Problem, dass wir nur sehr eingeschränkt Daten erhalten haben und auch fraglich ist, wie valide diese Daten sind.

Komplizierter war es mit den Intensitätswerten der Überwachung für die einzelnen Vorschriften, die wir uns angesehen haben. Damit die Intensitätswerte am Ende nicht nur von unserer subjektiven Einschätzung abhängig sind, haben wir sehr genau die Rechtsprechung des Verfassungsgerichts ausgewertet, um auf der einen Seite festzustellen, welche Kriterien es als intensitätssteigernd ansieht.

Auf der anderen Seite gibt es Faktoren, die nach der Rechtsprechung mitigierend wirken und die Überwachungsintensität wieder absenken. Das sind beispielsweise vorgeschaltete verfahrensrechtliche Elemente wie ein Genehmigungsvorbehalt. Dadurch müssen Bürger dann nicht so sehr fürchten, leicht Gegenstand von Überwachung zu werden. Es macht ja einen Unterschied, wenn der Bürger weiß: Diese Überwachungsmaßnahme kann die Polizei nicht einfach so ergreifen, sondern da muss sie vorher einen Richter fragen.

So haben wir die einzelnen Faktoren aus der Rechtsprechung in intensitätssteigernde und mitigierende eingeteilt und geschaut, was es in den Gesetzen für unterschiedliche Ausprägungen dieser Faktoren gibt.

„Daten mit besonderer Persönlichkeitsrelevanz“ bekommen eine 8

netzpolitik.org: *Eines der Merkmale für die Eingriffsintensität ist beispielsweise die Persönlichkeitsrelevanz der erhobenen Daten. Werden identifizierende Daten erhoben, hat das den Wert 2 bekommen, „Daten mit besonderer Persönlichkeitsrelevanz“ haben den Wert 8. Wie haben Sie diese Faktoren in Zahlen übersetzt?*

Poscher: Wir haben sehr lange mit verschiedenen Werten experimentiert, bis wir Zuordnungen gefunden haben, die überzeugend waren und nicht zu kontraintuitiven Ergebnissen führten. Wir haben bis zum Schluss immer wieder nachjustiert und besonders angesichts neu auftauchender Überwachungsbefugnisse geschaut: Überzeugt jetzt die Einordnung noch, die wir dabei herausbekommen?

Die Merkmale selbst sind also nicht von uns erfunden, sondern die haben wir jeweils der Rechtsprechung entnommen. Aber die Gewichtung der Faktoren anhand numerischer Werte, das ist natürlich eine Setzung von uns. Aber weil wir so viele Faktoren in der Rechtsprechung gefunden haben, würde es recht wenig verschieben, wenn jemand jetzt sagte: Hier würde ich statt 7 nur 5 Punkte zuweisen. Unser Fokus war, dass es in der Gesamtansicht plausibel ist.

netzpolitik.org: *Im Bericht steht zum Beispiel bei der Online-Durchsuchung, dass sie in den unterschiedlichen Länder- und Bundesgesetzen so unterschiedlich gestaltet sei, dass man dort jeweils ganz andere Kennwerte erreicht. Welche Faktoren führen zu dieser unterschiedlichen Bewertung?*

Poscher: Meistens liegen die Unterschiede in den mitigierenden Faktoren. Also in den verfahrensrechtlichen Anforderungen, damit eine solche Online-Durchsuchung erfolgen kann. Ein anderer Faktor ist, dass die Einsatzanlässe unterschiedlich definiert werden. In manchen Ländern wird eine Maßnahme auch gegen allgemeine Kriminalität eingesetzt, in anderen nur zur Terrorismusbekämpfung. Das macht natürlich einen Unterschied in der Überwachungslast.

Die Überwachungsgesamtrechnung ermöglicht es, Fragen zu stellen

netzpolitik.org: *Was kann man mit einer solchen Erkenntnis machen?*

Poscher: Man könnte in die Tabelle schauen und sich fragen: Was können wir tun, um die Überwachungslast zu senken? Dafür könnte man analysieren, wie sich die Regelungen in den Ländern unterscheiden, die einen niedrigeren Überwachungswert haben.

Man kann sich aber auch umgekehrt fragen: Führen besondere Hürden oder Einschränkungen dazu, dass Ermittlungen in bestimmten Ländern nicht so erfolgreich stattfinden können wie in anderen?

Die Gesamtrechnung gibt darüber erst mal keine Auskunft. Sie erlaubt jedoch, solche Unterschiede zu sehen und dann die entsprechenden Fragen zu stellen.

netzpolitik.org: *Nun scheint der politische Wille momentan zu sein, eine Überwachungsgesamtrechnung eher abzulehnen. Im vergangenen Juni haben beispielsweise die Innenminister:innen der Länder und des Bundes beschlossen, dass eine Überwachungsgesamtrechnung „keine geeignete Grundlage" für politische Entscheidungen sein könne – bevor diese überhaupt fertig war. Stattdessen forderten sie[2] eine „Sicherheitsgesamtrechnung". Wie hat sich dieses Klima auf Ihre Arbeit ausgewirkt?*

Poscher: Es hat uns erstmal überrascht, weil einer unserer Auftraggeber ja das Bundesinnenministerium war. Einerseits kann ich verstehen, dass die Behörden Sorge haben, dass ihre Leistung nicht gesehen wird. Andererseits ist es sehr schade, dass die Behörden so defensiv auf diese Untersuchung reagieren und sich davor scheuen, ihre Zahlen öffentlich zu machen. Die Überwachungsgesamtrechnung ist kein Projekt, das sich gegen die Sicherheitsbehörden und ihre Arbeit wendet. Sie soll vielmehr Transparenz schaffen – auch für die Behörden selbst.

Aus unserer Sicht kann Transparenz hinsichtlich sicherheitsrechtlicher Überwachung ein starkes vertrauensbildendes Element sein. Denn bei einer Reihe von Maßnahmen gibt es eine große öffentliche Besorgnis, beispielsweise bei der Online-Durchsuchung. Anhand der Zahlen kann man aber sehen, dass etwa die Online-Durchsuchung nur sehr, sehr zurückhaltend eingesetzt wird. Die Sorge, dass beinahe jedes Telefon mit einem Bundestrojaner infiziert ist, ist also weit von der Realität entfernt.

Es ist ein bisschen verwunderlich, dass die Behörden da nicht selbstbewusster sind und auch nicht sehen, wie viel Vertrauen man gewinnen könnte, wenn man diese Dinge öffentlich macht. Ist doch das Vertrauen der Bevölkerung für die Arbeit der Sicherheitsbehörden von unschätzbarem Wert.

Ein weiteres Problem ist, dass Behörden teilweise gar nicht in der Lage sind, Zahlen zu Überwachungsmaßnahmen zu liefern, weil sie die selber nicht haben. Teilweise müssen in den Behörden, wo es Meldepflichten gibt, händisch Papierakten durchgearbeitet und Maßnahmen gezählt werden. Das ist ein unvertretbarer Aufwand.

Und dann kommt dazu, dass es keine einheitlichen Standards gibt, wie Daten erhoben werden. Auch bei Daten, die schon seit Jahrzehnten gesammelt werden, wie die zur Häufigkeit von Telekommunikationsüberwachungen. Manche Behörden zählen überwachte Anschlüsse, andere zählen betroffene Personen, einige zählen die Anordnungsbeschlüsse, andere nur tatsächlich durchgeführte Überwachungen. Da macht jede Behörde, was sie gerade für richtig erachtet, und die Zahlen lassen sich dann nur sehr schwer vergleichen. Es ist unverständlich, warum die Justizministerkonferenz die Arbeit ihrer Beamten so wenig achtet und es weiterhin zulässt, dass die Erfassung nicht nach einheitlichen Vorgaben erfolgt.

Wie die Behörden selbst von mehr Transparenz profitieren können

netzpolitik.org: *Gab es auch Ausnahmen? Also Behörden, die besonders kooperativ waren und bereits eine digitale Erfassung von Maßnahmen haben?*

Poscher: Es gab einige wenige Behörden, die auf Knopfdruck Daten zu Überwachungsmaßnahmen liefern konnten, weil sie selbst entsprechende Systeme eingeführt haben. Das haben sie dann auch gern getan. Ein Beispiel ist das Saarland. Es geht also. Da hatten wir gute Zahlen mit wenig Aufwand.

netzpolitik.org: *Können die Behörden auch selbst von einer systematischeren Erfassung profitieren?*

Poscher: Unbedingt. Der Sinn unseres ganzen Projekts war ja, mehr Transparenz in die sicherheitspolitische Diskussion zu tragen – auch weil teilweise Besorgnisse überbordend sind und mit der Realität nicht viel zu tun haben.

Andererseits sehen wir aber auch einen Zuwachs an Überwachungsmaßnahmen in bestimmten Feldern, wo die Sinnfrage gestellt werden muss. Da ist unklar, was man überhaupt mit den ganzen Daten anfangen und wie man sie verwerten kann.

Wir sehen sehr große Unterschiede in manchen Bereichen, etwa bei der Telekommunikationsüberwachung zwischen den Ländern. Da müssen wir fragen: Warum ist das eigentlich so? Sind das Berichtsfehler? Das wissen die Behörden selber nicht, es müsste aber jedenfalls jede Behördenleitung bereits aus einer Steuerungs- und Managementperspektive interessieren. Sie würden sehr davon profitieren, auch um etwa zu entscheiden, welches technische Equipment sie anschaffen oder wie sie ihre Beamten einteilen und wo es sinnvoll ist, Kapazitäten einzusetzen.

All das lässt sich nicht beurteilen, ohne dass man diese Zahlen hat. Das ist so, als würde man Apple fragen: „Wie viele Bildschirme haben Sie denn geliefert bekommen?" Und Apple sagt dann: „Wissen wir nicht, wir bauen Computer." So lässt sich schlecht arbeiten.

netzpolitik.org: *Woran liegt es, dass viele Behörden keine guten Zahlen zu ihren Maßnahmen liefern können?*

Poscher: Das hat zum einen mit der mangelnden Digitalisierung unserer Verwaltung zu tun. Es sind aber vielfältige Probleme. Ein weiterer Grund ist die komplexe Verantwortungsstruktur innerhalb der Behörden, wo wir die Polizei auf der einen Seite haben, die Staatsanwaltschaft auf der anderen und dann auch die Gerichte. Die müssten ja eigentlich alle Systeme haben, die miteinander interoperabel sind. Das ist leider noch lange nicht der Fall.

netzpolitik.org: *Im Bericht ist erwähnt, dass bestimmte Bereiche nicht berücksichtigt wurden. Woran lag das und wie sollte eine potenzielle nächste Version der Überwachungsgesamtrechnung vielleicht ergänzt werden?*

Poscher: Der Grund der Beschränkungen lag vor allem an dem Auftrag. Wir hatten vom Innen- und Justizministerium nur den Auftrag für bestimmte Bereiche. Da wir nur elf Monate Zeit für das Projekt hatten, waren wir da auch nicht unbedingt traurig darüber.

Ein Bereich, der unbedingt mitaufgenommen werden sollte, ist allerdings die Überwachung von Finanzdaten. Da gibt es sehr viele Auswertungsmaßnahmen. Kontobewegungen werden sehr lange gespeichert und Banken sind sicherheitsrechtlich verpflichtet, alle Transaktionen automatisiert zu analysieren. Was in anderen Überwachungsbereichen kontrovers diskutiert wird, gibt es im Finanzbereich seit Jahren schon ganz praktisch – ohne große öffentliche Aufmerksamkeit.

Wie es mit der Überwachungsgesamtrechnung weiter geht

netzpolitik.org: *Wird es denn eine Weiterführung der Überwachungsgesamtrechnung geben?*

Für die Überwachungsgesamtrechnung reicht ein Taschenrechner nicht aus. Foto: Ben Wicks auf Unsplash

Poscher: Wir haben jetzt einen sehr guten Grundstock und evaluieren derzeit, wie viel Aufwand es ist, die Überwachungsgesamtrechnung zeitlich fortzuführen. Was wir auf jeden Fall fortführen können, ist die Evaluierung von Sicherheitsgesetzen und -regelungen. Die könnten wir dann auch beispielsweise auf die Finanzdaten ausweiten.

Teilweise können wir auch weiter mit den Zahlen für Maßnahmen arbeiten, denn eine Reihe davon müssen Behörden ohnehin veröffentlichen – wir werden also kontinuierlich weiter Zahlen bekommen. Das Problem ist, dass sich die Aussagekraft der Zahlen je nach Bundesland stark unterscheidet. Eine solche Untersuchung wird also weiterhin erst einmal lückenhaft bleiben.

Aber das ganze Instrument wird ja eigentlich erst richtig interessant, wenn es auch eine zeitliche Dimension hat. Also wenn man sieht, wie sich die Überwachungslast verändert.

netzpolitik.org: *Im Bericht zur Überwachungsgesamtrechnung sind viele Tabellen mit langen Zahlenreihen enthalten. Werden Sie in Zukunft auch den vollständigen Datensatz veröffentlichen?*

Poscher: Daran arbeiten wir noch. Die Datenbank mit allen Zahlen ist mittlerweile sehr komplex geworden und wir überlegen, was das richtige Format für eine Veröffentlichung ist, sodass andere damit auch etwas anfangen können.

netzpolitik.org: *Was ist für Sie die wichtigste Erkenntnis aus der Arbeit an der Überwachungsgesamtrechnung?*

Poscher: Für mich ist die Botschaft sehr wichtig, dass es auch im Interesse der Behörden wäre, wenn sie selbst über bessere Zahlen verfügen und wenn sie mit ihrer Arbeit in die Öffentlichkeit gehen würden.

Wir haben nichts in den Zahlen gefunden, was eine Behörde verstecken müsste. Unser Ziel ist es, auch Politik und Behörden für mehr Transparenz in der Sicherheitspolitik zu gewinnen, um eine rationalere und faktenbasierte öffentliche Diskussion von Sicherheitsmaßnahmen zu ermöglichen.

Referenz: https://netzpolitik.org/2025/ueberwachungsgesamtrechnung-mehr-transparenz-waere-auch-im-sinne-der-behoerden-selbst/

Autoreninformation zu **Anna Biselli** siehe Seite 54

Anmerkungen

1 *https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2025/2025_uegr-mpi.pdf?__blob=publicationFile*

2 *https://netzpolitik.org/2024/vorauseilende-ablehnung-innenministerkonferenz-attackiert-ueberwachungsgesamtrechnung/*

Ingo Dachwitz, Chris Köver, Daniel Leisegang, Tomas Rudl

So will Schwarz-Rot das Land digitalisieren

7. Mai 2025 – *Nun soll es endlich kommen: ein eigenständiges Digitalministerium. Das neue Ressort soll verschiedene Kompetenzen zusammenführen, die bislang verstreut waren. Was ändert sich damit, was bleibt gleich? Und was kommt zu kurz? Eine Analyse.*

Deutschland bekommt erstmals ein eigenes Ministerium[1] für Digitalpolitik. In einem Organisationserlass[2] legte der frisch gewählte Bundeskanzler Friedrich Merz (CDU) gestern die Aufgabenverteilung innerhalb der neuen Bundesregierung fest und schuf das Bundesministerium für Digitales und Staatsmodernisierung (BMDS). Dessen genauer Zuschnitt war bisher unklar.

Der Erlass zeigt, dass das BMDS weit mehr Kompetenzen erhält als erwartet. In den vergangenen Jahren kümmerte sich etwa das Bundeskanzleramt um die „strategische Vorausschau" und Grundsatzfragen der Digitalpolitik. Dafür ist nun das neue Ministerium zuständig, das zunächst in ein Gebäude des Innenministeriums am Berliner Tiergarten zieht. Außerdem bekommt das Haus des Ex-Managers Karsten Wildberger[3] Abteilungen und Zuständigkeiten aus sechs anderen Ministerien.

Wildberger war zuvor unter anderem Geschäftsführer der Media-Saturn-Holding GmbH. Als Parlamentarische Staatssekretäre stehen ihm Thomas Jarzombek (CDU) für den Bereich Digitalisierung und Philipp Amthor (CDU) für den Bereich Staatsmodernisierung und Bürokratieabbau zur Seite. Auch für den ehemaligen Bundes-CIO Markus Richter beginnt ein neues Kapitel[4]: Sein bisheriges Amt geht im BMDS auf, wo Richter fortan als Staatssekretär wirkt.

Der Zuschnitt des Hauses zeigt: Das Ministerium und damit Digitalisierung spielt in der neuen Regierung eine wichtige Rolle. Ebenfalls deutlich wird, dass das BMDS seinen Fokus dabei stärker auf Wirtschaft und Innovationen legen wird und weniger auf Gemeinwohl und Zivilgesellschaft.

Fußen soll die künftige Digitalpolitik auf drei Säulen. Erstens die Staats- und Verwaltungsdigitalisierung, für die das Digitalministerium sogar weitgehende Autonomie bei der Finanzierung erhält. Zweitens die Daten- und Digitalisierungspolitik und drittens die digitale Infrastruktur.

Wir haben uns das „Ministerium für Umsetzung"[5] genauer angeschaut. Was ändert sich mit dem neuen Ressort? Was bleibt im Vergleich zur Vorgängerregierung? Und vor welchen Herausforderungen steht der frisch berufene Minister als „Mann aus der Wirtschaft"?

Erste Säule: Moderner Staat mit digitaler Verwaltung

Um die Staatsmodernisierung voranzutreiben, wandern einige Abteilungen und Zuständigkeiten aus dem Bundesinnenministerium (BMI) ins neue Digitalministerium – allen voran die digitale Verwaltung und das Onlinezugangsgesetz (OZG). Bei allen Bemühungen war die Vorgängerregierung hier nur schleppend vorangekommen, was allerdings weniger an einer fehlenden Bündelung der Zuständigkeiten als vielmehr an den Bundesländern gelegen hat[6]. Daher wird das BMDS sich vor allem darum bemühen müssen, einheitliche Standards sowie eine konsequente Ende-zu-Ende-Digitalisierung in Absprache mit den Ländern und Kommunen auf möglichst allen Verwaltungsebenen zu erreichen.

Dieser Prozess soll offenbar Hand in Hand mit der IT-Beschaffung gehen. Sie war bislang ebenfalls beim BMI angesiedelt. Der Bereich betrifft die Informationstechnik der Bundesverwaltung, die wiederum eine wichtige Grundlage für den sogenannten digitalen Staat[7] ist. Der öffentliche IT-Dienstleister des Bundes, das Informationstechnikzentrum Bund (ITZBund) ist fortan ebenfalls unter dem Dach des Digitalministeriums angesiedelt – und damit auch die Zuständigkeit für die „souveräne Cloud".

Ringen um ITZBund

In den vergangenen Jahren war das ITZBund beim Finanzministerium angedockt, das sich dagegen gewehrt hatte, die Zuständigkeit dafür abzugeben. Das Zentrum betreibt etwa die Bundescloud, die Rechenzentren des Bundes und weitere Software und Infrastruktur, die die Bundesverwaltung nutzt. Das Budget dafür ist gewaltig: 1,59 Milliarden Euro[8] laut Website und es könnten zukünftig noch mehr werden.

Auch die Zuständigkeit für die Netzinfrastrukturen des Bundes wandert vom BMI ins Digitalministerium. Sie galten dort als „zentrales Nervensystem" der modernen Behördenarbeit, die besonders geschützt werden müssen[9]. Das Digitalministerium soll zudem fortan auch für die Cybersicherheit zuständig sein – wobei laut Erlass „die spezifischen Anforderungen der Sicherheitsbehörden an die Netze" unter der Obhut des BMI verbleiben sollen.

Weitgehende Hoheit über IT-Ausgaben

Die bedeutende Rolle des BMDS unterstreicht auch die Tatsache, dass das Haus nicht nur über ein eigenes Budget, sondern auch über „einen Zustimmungsvorbehalt für alle wesentlichen IT-Ausgaben der unmittelbaren Bundesverwaltung" verfügt. Das bedeutet, dass nur dann Gelder fließen können, wenn das Digitalministerium dem zuvor zustimmt – mit einzelnen Ausnahmen für Sicherheitsaufgaben und den Steuerbereich.

Damit könnte ein großes Manko der Vorgängerregierung behoben werden. Die Ampel hatte in ihrem Koalitionsvertrag noch ein Digitalbudget versprochen. Statt eines speziell auf Digitalisierungsprojekte zugeschnittenen Budgets gab es jedoch Haushaltskürzungen[10]. Die neue Bundesregierung hat immerhin schon mal erkannt, dass Digitalisierungsprojekte ein festes Budget benötigen.

Offene Fragen und Widersprüchliches

Offen ist derzeit noch, wie sehr die Staats- und Verwaltungsdigitalisierung unter dem Vorzeichen des „Bürokratieabbaus" stehen wird, den qua Amtsbezeichnung Philipp Amthor vorantreiben soll. Hier musste das Justizministerium Zuständigkeiten ans BMDS abgeben, etwa die *Geschäftsstelle für Bürokratieabbau* und die Zuständigkeit für bessere Rechtssetzung. Auch die zehn ehrenamtlichen Mitglieder des nationalen Normenkontrollrats arbeiten ab jetzt für das Digitalministerium. Der Rat berät etwa beim Bürokratieabbau und bei der Planung neuer Gesetze.

Ebenso unklar ist, wie sich diese Verschiebungen auf das Bundesamt für Informationstechnik (BSI) auswirken, das hierzulande für die Cybersicherheit zuständig ist, oder auf das ressortübergreifende Großprojekt *IT-Konsolidierung Bund*, das bisher die IT-Beschaffung gebündelt organisierte[11]. Gleichsam unklar ist, ob die Föderale IT-Kooperation (FITKO)[12], die dem IT-Planungsrat[13] zuarbeitet, weiterhin beim BMI angesiedelt sein wird oder ebenfalls zum Digitalministerium wechselt. Naheliegend erscheint letzteres, da nicht nur beim Onlinezugangsgesetz eine Menge an Koordinierung notwendig sein wird – und dieser Brocken landet beim BMDS. Ähnlich in der Schwebe zwischen BMI und BMDS hängt das Zentrum Digitale Souveränität (ZenDiS), das im Erlass keine Erwähnung findet.

Absprachebedarf scheint es nicht zuletzt auch bei der Frage zu geben, welches Ministerium die Verantwortung für den Bereich digitale Identitäten übernimmt. Laut Organisationserlass behält das Innenministerium die Zuständigkeit für „das Pass- und Ausweiswesen sowie das Identitätsmanagement". Gleichzeitig aber schreibt das Digitalministerium in seiner ersten Pressemitteilung, dass es künftig auch für die „Einführung einer digitalen Identitäts-Wallet und von Bürgerkonten" verantwortlich sei.

Zweite Säule: Daten- und Internationale Digitalpolitik

Das neue Ministerium übernimmt gleich zwei große Brocken aus dem bisherigen BMDV von Volker Wissing: Digital- und Datenpolitik sowie digitale Infrastrukturen, also Glasfaser- und Mobilfunkausbau.

Die Abteilung *Digital- und Datenpolitik* war in der Ampel die zentrale Einheit für die Gestaltung der Digitalisierung – oder hätte es zumindest werden können, wenn SPD, Grüne und FDP sich nicht doch für eine totale Zersplitterung der Kompetenzen[14] entschieden hätten. Trotzdem war die Abteilung eine Impulsgeberin für die Digitalpolitik der Ampel, verantwortete etwa die Datenstrategie, brachte ein Mobilitätsdatengesetz auf den Weg und war für die Umsetzung von EU-Datengesetzen wie dem Data Act verantwortlich. Auch der Beirat zur Digitalstrategie der Ampel[15] war hier angesiedelt.

Selbst wenn Abteilungsleiter Benjamin Brake sich schon mal für Deutschlands „Nein" zur Chatkontrolle starkmachte[16], war die Abteilung primär auf Wirtschaft und Innovationen ausgerichtet und passt deshalb vermutlich hervorragend in das neue Ministerium. Auch zuvor beim Wirtschaftsministerium und beim Innenministerium angesiedelte Aspekte der Datenpolitik wandern in das BMDS. Unklar ist vorerst, ob das auch für das Thema Open Data gilt oder ob dies als ein Aspekt des Bereichs Open Government, von dem im Organisationserlass nicht explizit die Rede ist, im Innenministerium verbleibt.

Immerhin besteht kein Zweifel, dass mit der Digital- und Datenpolitik auch die Verantwortung für internationale Digitalpolitik in das BMDS zieht. Es wird Deutschland beispielsweise in internationalen Foren wie den G7 oder G20, Internet-Governance-Gremien und bei der UN vertreten. Entsprechend der im alten Ministerium erarbeiteten Strategie für internationale Digitalpolitik soll es sich dabei für ein offenes und sicheres Internet einsetzen und strategische Partnerschaften „besonders mit Ländern des globalen Südens" ausbauen.

Künftig wird das Haus außerdem für die Umsetzung der KI-Verordnung in Deutschland zuständig sein und betont bereits, dass diese innovations- und wirtschaftsfreundlich ausfallen soll. Hier stehen in den kommenden anderthalb Jahren noch einige Entscheidungen an, bis alle Teile des wegweisenden Gesetzes 2026 in Kraft treten – etwa, welche Behörde offiziell die Aufsicht über die Einhaltung von Regeln führen wird.

Dritte Säule: Digitale Infrastruktur

Dem Koalitionsvertrag[17] zufolge steht beim Infrastrukturausbau kein grundlegender Paradigmenwechsel bevor. Anders als frühere Regierungen gibt die schwarz-rote Koalition zwar keine genauen Jahreszahlen an, bis wann sie ihre Ziele erreichen will. Sie dürfte sich jedoch an den Etappenmarkern der EU orientieren: Bis Ende des Jahrzehnts sollen allen Bürger:innen gigabitfähige Leitungen und 5G-Mobilfunkverbindungen zur Verfügung stehen.

Um das zu erreichen, soll das inzwischen zehn Jahre alte staatliche Förderprogramm – unter großen Geburtsschmerzen[18] vom

damaligen Infrastruktur- und nunmehrigen Innenminister Alexander Dobrindt (CSU) auf den Weg gebracht[19] – weitergeführt werden. Hier sind bereits Milliardenprojekte von Ländern und Kommunen geplant und bewilligt, schon deshalb wäre ein völliger Neuanfang kontraproduktiv.

Auf bereits gelegten Schienen dürften generell weite Teile der sonstigen Infrastrukturpolitik weiterfahren. Angekündigt ist etwa ein neuer Anlauf für ein Beschleunigungsgesetz[20], welches den Ausbau unter „überragendes öffentliches Interesse" stellen und Bürokratie abbauen dürfte – allesamt Ziele, denen sich auch Schwarz-Rot verschrieben hat.

Wo das Digitalministerium nicht zum Zuge kommt

Zugleich muss das BMDS auch die eine oder andere Feder lassen. An das Forschungsministerium muss es die zuvor beim BMDV angesiedelten Kompetenzen für die Förderung von „U-Spaces und Advanced Air Mobility" abgeben. Hinter diesen Begriffen verstecken sich die Zuständigkeiten für zivile Drohnen oder die viel beschworenen Flugtaxis. Ins BMWE wandern zudem Erdbeobachtung, Satellitennavigation und -kommunikation sowie die Deutsche Galileo-PRS-Behörde.

Auch aus dem Wirtschaftsministerium landen einige Agenden mit Digitalbezug nicht beim BMDS, sondern beim Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR). Dazu zählen etwa die Zuständigkeiten für Raumfahrt einschließlich des Deutschen Zentrums für Luft- und Raumfahrt.

Das überrascht bereits wegen einer Personalie: So war der frisch berufene BMDS-Staatssekretär Thomas Jarzombek von 2018 bis 2021 Koordinator der Bundesregierung für Luft- und Raumfahrt, später Beauftragter des Wirtschaftsministeriums für digitale Wirtschaft und Start-ups. Nun steigt der langjährige Digitalpolitiker zum parlamentarischen Staatssekretär im Digitalministerium auf, kann aber viele seiner Kompetenzen nicht mitnehmen.

Zudem ziehen weitere Digital-Zuständigkeiten ins Forschungsministerium und damit zur neu bestellten Bundesministerin Dorothee Bär. Die CSU-Politikerin widmet sich künftig unter anderem Grundsatzfragen der nationalen und internationalen Innovations- und Technologiepolitik, der Entwicklung digitaler Technologien, Gigafactorys und Computerspielen.

Referenz: https://netzpolitik.org/2025/neues-digitalministerium-so-will-schwarz-rot-das-land-digitalisieren/

Anmerkungen

1 *https://bmds.bund.de/*
2 *https://www.bundesregierung.de/resource/blob/2196306/2345476/cdff731d8650c3ea9281853dedf46d2c/2025-05-06-organisationserlass-data.pdf?download=1*
3 *https://netzpolitik.org/2025/designiertes-bundeskabinett-vom-lobbyisten-zum-digitalminister/*
4 *https://www.linkedin.com/posts/markus-richter-134315204_bmds-digitalstaat-staatsmodernisierung-activity-7325644781894713345-zqZW*
5 *https://bmds.bund.de/ministerium/das-bmds-stellt-sich-vor*
6 *https://netzpolitik.org/2024/onlinezugangsgesetz-2-0-verwaltungsdigitalisierung-mit-ausstiegsklausel/*
7 *https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-des-bundes/it-des-bundes-node.html*
8 *https://www.itzbund.de/DE/dasitzbund/ueber-uns/ueber-uns.html?nn=178014#bodyText1786221*
9 *https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-des-bundes/netze-des-bundes/netze-des-bundes-node.html*
10 *https://netzpolitik.org/2023/ein-jahr-digitalstrategie-reihenweise-fehlzuendungen/*
11 *https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-des-bundes/it-konsolidierung/it-konsolidierung-node.html*
12 *https://www.fitko.de/*
13 *https://www.it-planungsrat.de/*
14 *https://netzpolitik.org/2022/nach-sieben-monaten-im-amt-ampel-einigt-sich-auf-digitalzustaendigkeiten/*
15 *https://netzpolitik.org/2024/beirat-digitalstrategie-fundamentale-kritik-an-der-digitalpolitik-der-ampel/*
16 *https://netzpolitik.org/2023/pseudo-kompromiss-ratspraesidentschaft-haelt-an-chatkontrolle-fest/*
17 *https://netzpolitik.org/2025/koalitionsvertrag-das-planen-union-und-spd-in-der-netzpolitik/#infrastruktur*
18 *https://netzpolitik.org/2018/nun-offiziell-bundesrechnungshof-zerpflueckt-ex-minister-alexander-dobrindt/*
19 *https://netzpolitik.org/2025/neuer-innenminister-dobrindts-zweiter-versuch/*
20 *https://netzpolitik.org/2024/gemaechliches-beschleunigungsgesetz/*
21 *mailto:tomas@netzpolitik.org*
22 *https://keys.openpgp.org/search?q=tomas%40netzpolitik.org*
23 *https://bsky.app/profile/tomasrudl.bsky.social*

Ingo Dachwitz, Chris Köver, Daniel Leisegang,Tomas Rudl

Tomas Rudl ist in Wien aufgewachsen, hat dort für diverse Provider gearbeitet und daneben Politikwissenschaft studiert. Seine journalistische Ausbildung erhielt er im *Heise-Verlag*, wo er für die Mac & i, c't und Heise Online schrieb.
Kontakt: E-Mail[21] (OpenPGP[22]), Bluesky[23]

Autoreninformationen zu **Ingo Dachwitz**, **Chris Köver** und **Daniel Leisegang** siehe Seite 54

Alexandra Keiner

Petra Molnar: The Walls Have Eyes.

Surviving Migration in the Age of Artificial Intelligence – Eine globale Geschichte von Macht, Gewalt und Technologie

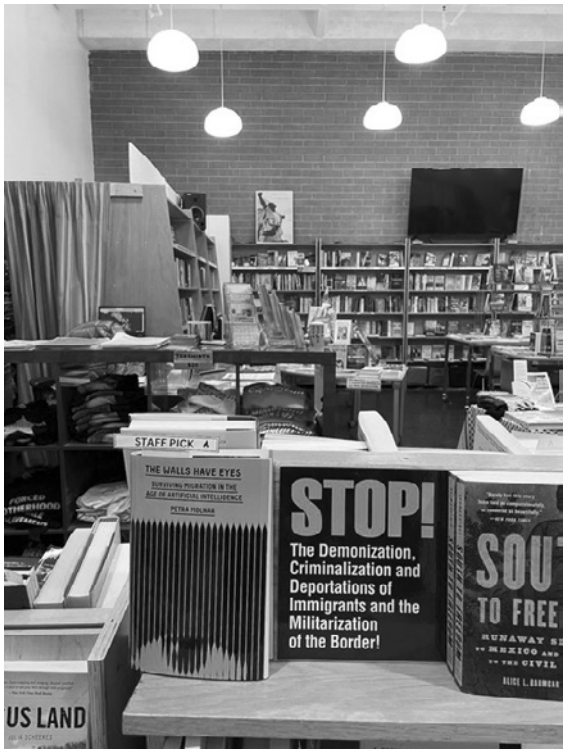
Kaum ein Thema hat in den vergangenen zwei Jahren so viel Aufmerksamkeit erfahren wie Künstliche Intelligenz. Bisher war der Diskurs häufig von visionären Zukunftsszenarien und wirtschaftlichen Potenzialen geprägt, mittlerweile geraten auch die konkreten Anwendungsfelder der Technologien in den Blick. In ihrem Buch *The Walls Have Eyes. Surviving Migration in the Age of Artificial Intelligence* widmet sich Petra Molnar einem solchen Anwendungsfeld: dem Einsatz von KI und anderen modernen Technologien zur Grenzüberwachung und Migrationskontrolle. Die kanadische Anthropologin und Juristin zeigt, wie Technologien an Grenzen und Checkpoints sowie in Geflüchtetencamps und Asylverfahren eingesetzt werden, welche verheerenden Auswirkungen dies für die betroffenen Menschen hat und wie technologische Grenzsicherung zu einem lukrativen Geschäft für westliche Staaten und große Unternehmen avancierte.

Smarte Grenzen, tödliche Realität

Im ersten Kapitel begleitet Molnar Aktivist:innen, die in der Sonora-Wüste an der Grenze zwischen Mexiko und den USA Wasserflaschen verteilen, Menschen auf der Flucht mit Essen und Medikamenten versorgen oder die Leichen derer bergen, die auf ihrer Flucht gestorben sind. Den Grenzübergang, der als einer der gefährlichsten Orte der Welt gilt, markiere längst nicht mehr nur eine hohe, rostige Mauer, sondern auch Technologie-gestützte Überwachung: etwa Türme mit KI-basierten Bewegungssensoren, Drohnen, die das Gelände aus der Luft kontrollieren, und *Robodogs* – vierbeinige Militärroboter, die mit hochauflösenden Kameras in der Wüste patrouillieren, Personen identifizieren und Videobilder in Echtzeit übertragen.

Das zweite Kapitel beleuchtet die europäischen Außengrenzen. Molnar widmet sich hier vor allem der Europäischen Agentur für die Grenz- und Küstenwache Frontex, die in den letzten Jahren mit erheblichen finanziellen Mitteln ausgestattet wurde, um sich technologisch aufzurüsten. Die Autorin beschreibt ein immer umfangreicheres Überwachungsarsenal, das Roboter, Drohnen, Luftschiffe, 360-Grad-Kameras, Schiffsradare, Sensoren und biometrische Datenbanken umfasst. Die COVID-19-Pandemie habe den *„appetite for technological solutions at the border"* (S. 61) verstärkt und Frontex als Legitimation für den weiteren Ausbau dieser Infrastruktur gedient.

Regierungen und Behörden stellen, Molnar zufolge, sogenannte *smart borders* – also den Einsatz vermeintlich intelligenter Technologien an Grenzen wie denen zwischen den USA und Mexiko oder zwischen Griechenland und der Türkei – als humanere und zugleich effizientere Alternative zu alten Methoden des Grenzschutzes dar. Die Realität an den Grenzen sehe aber anders aus: Die technologische Aufrüstung habe nicht zu weniger Migration geführt, vielmehr seien Menschen auf der Flucht dazu gezwungen, immer gefährlichere und weniger berechenbare Routen zu wählen, um den umfassenden Überwachungssystemen zu entgehen. Zugleich kämen die eingesetzten Technologien nur selten den Schutzsuchenden zugute. Statt Hilfe zu leisten oder Schutzbedürftige zu lokalisieren, würden die Überwachungsdaten beispielsweise dazu genutzt, gewaltsame *Pushbacks* zu koordinieren. Das Ergebnis sei eine humanitäre Katastrophe: Noch nie seien so viele Menschen bei dem Versuch gestorben, die europäischen Außengrenzen oder die Grenze zwischen den USA und Mexiko zu überqueren, so Molnar.



Techno-Solutionismus

Die Kapitel 3 und 4 zeigen, wie Grenztechnologien über den unmittelbaren Grenzraum hinaus wirksam sind – in griechischen Geflüchtetencamps oder in Visavergabe- und Asylverfahren. Molnar bezeichnet die Geflüchtetencamps, die sie in Griechenland besucht hat, als *„digital prisons"* (S. 71): Kameras und Sensoren der Hochsicherheitszäune erfassen jede Bewegung, mit

den Daten werden *„Riskscores"* für die Bewohner:innen erstellt. Wie wichtig – und zugleich absurd – die technologische Infrastruktur ist, zeigt sich besonders am Beispiel eines Camps auf der Insel Samos, in dem biometrische Überwachungssysteme einsatzbereit waren, noch bevor es fließendes Wasser gab.

Im vierten Kapitel beschreibt Molnar ausführlicher, welche Rolle die Technologien bei der Visavergabe und bei Asylanträgen spielen. Dazu zählen etwa *„[v]isa-triaging algorithms"* (S. 100) von Microsoft, die in Kanada automatisiert über Visaanträge entscheiden, oder elektronische Fußfesseln, die den Aufenthaltsort von Asylsuchenden in Echtzeit übermitteln. Auch Spracherkennungs-Software zur Identifizierung von Personen und Lügendetektoren, die anhand von Gefühlsanalysen überprüfen sollen, ob Menschen über ihre Einreisegründe oder bezüglich persönlicher Daten die Wahrheit sagen, gehören in dieses Repertoire.

Auch geht Molnar in diesem Zusammenhang auf die Digitalisierungs-Agenda des Bundesamtes für Migration und Flüchtlinge (BAMF) in Deutschland ein, die unter anderem die Auswertung von Handydaten, die automatische Transliteration arabischer Namen sowie Dialekterkennungs-Software umfasst. Diese Technologien, kritisiert Molnar, seien nicht nur teuer und griffen massiv in die Privatsphäre der überwachten Menschen ein, sie wiesen zudem oft hohe Fehlerquoten auf oder funktionierten gar nicht. Dennoch würden sie weiter eingesetzt – ein blindes Vertrauen in technische Lösungen, das Molnar als *„techno-solutionism"* (S. 59) bezeichnet. Die Hybris der Big-Tech-Unternehmen und der Reiz der schnellen Lösungen suggeriere, man könne so komplexe soziale und politische Probleme wie Migration, Fluchtursachen oder Schmuggel mit Technologien lösen.

„A global multibillion-dollar border industrial complex"

Ein zentrales Argument des Buches lautet, dass mit eben dieser Wahrnehmung von Migration als technologisch lösbares Problem ein lukratives Geschäftsfeld entstanden ist. Molnar spricht von einem wachsenden *„global multibillion-dollar border industrial complex"* (S. 160), zu dem große Technologieunternehmen wie Palantir, Clearview AI, Google, Microsoft und Amazon gehören. Der Begriff des *industrial complex* verweist – analog zum Militär- und Gefängnissystem – auch bei der Grenzüberwachung auf enge *„public-private partnerships"* (S. 33): Sowohl staatliche Behörden als auch private Unternehmen hätten ein Interesse daran, die Nachfrage nach neuen Grenztechnologien hochzuhalten – unabhängig davon, ob sie tatsächlich notwendig oder effektiv sind.

Molnar verdeutlicht die Mechanismen am Beispiel der systematischen *Datafizierung* von Geflüchteten in Kenia (Kap. 5), wo Hunderttausende Geflüchtete aus Somalia und dem Südsudan leben. Dort erfassen humanitäre Organisationen wie das UNHCR zunehmend biometrische und persönliche Daten, über die der Zugang der Geflüchteten zu grundlegenden Leistungen wie Arbeitserlaubnis, medizinischer Versorgung oder Unterkunft geregelt sei.

Wie Unternehmen die Grenz- und Migrationskontrolle als Testgelände für ihre neuen Technologien nutzen, zeigt Molnar in Kapitel 6 am Beispiel israelischer Sicherheitsfirmen, die ihre Überwachungstechnologien an der Grenze zum Gazastreifen und in den besetzten palästinensischen Gebieten einsetzen, um sie dann als *„battle tested"* (S. 153) auf dem internationalen Markt zu bewerben. So wurden die Überwachungstürme in der Sonora-Wüste zuvor an der Grenze zum Gazastreifen getestet. Auch der besetzte Teil der palästinensischen Stadt Hebron sei laut einem ehemaligen israelischen Soldaten zu einem *„laboratory for technology but also the laboratory for violence"* (S. 139) geworden, in dem Firmen wie Pegasus oder Cellebrite Überwachungs- und Verhörtechnologien testen, die später von Frontex oder deutschen Migrationsbehörden eingesetzt werden.

Im siebten Kapitel analysiert Molnar das politische Narrativ, das den Einsatz von *„military-grade technology against the most vulnerable"* (S. 21) legitimiert. Dabei verweist sie auf verschiedene Theorien, die sich mit der Entstehung einer Politik der *„exclusion and fear"* und mit der Unterscheidung zwischen erwünschter und unerwünschter Migration befassen. Während manche Menschen die Grenzen trotz – oder wegen – deren technologischer Aufrüstung relativ ungehindert passieren könnten, würden andere bereits aufgrund der Tatsache, dass sie migrieren oder flüchten, kriminalisiert.

„Storytelling as a form of resistance"

Im letzten Kapitel widmet sich Molnar der Frage, welche Strategien des Widerstands es angesichts der zunehmenden Kriminalisierung von Migrant:innen und der fortschreitenden Technologisierung der Grenzen geben kann. Dabei zeigt sie verschiedene Ansätze auf: Zum einen könnte bestehendes Recht genutzt oder verändert werden, um die *„legal black holes"* (S. 65) rund um Grenztechnologien zu schließen. Ein Beispiel hierfür wäre eine Reform des *Act to Regulate Artificial Intelligence* (AI Act) der EU, der KI-Technologien explizit verbieten sollte, die existenzielle Folgen für Menschen auf der Flucht haben können. Zum anderen sieht Molnar die Möglichkeit, digitale Technologien im Sinne der Migrant:innen einzusetzen – etwa durch *„technologies of assistance"* (S. 201), die bei Asylanträgen unterstützen oder psychosoziale Hilfe zugänglich machen.

Molnar betont auch die Bedeutung individueller Widerstandsformen und berichtet von Menschen, die auf unterschiedliche Weise Widerstand gegen Grenztechnologien und -politiken leisten, darunter Journalist:innen, Rechtsanwält:innen oder Aktivist:innen wie Jaime, der in der Sonora-Wüste täglich Wasser an Migrant:innen verteilt, oder Igor, der an der polnisch-belarussischen Grenze sein Haus den von Pushbacks bedrohten Geflüchteten als Zufluchtsort anbietet.

Petra Molnar: The Walls Have Eyes. Surviving Migration in the Age of Artificial Intelligence. Mit einem Vorwort von E. Tendayi Achiume. USA, New York 2024: The New Press, 304 S., 28,99 USD, ISBN 978-1-620-97836-8

Hinweis: Bei diesem Text handelt es sich um eine leicht bearbeitete und gekürzte Fassung einer Rezension, die ebenfalls unter dem Titel „Eine globale Geschichte von Macht, Gewalt und Technologie" am 8. April 2025 bei Soziopolis erschienen ist.

Sylvia Johnigk

Christian Reuter (ed): Information Technology for Peace and Security

Der Herausgeber ist Professor am Lehrstuhl Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) an der Technischen Universität Darmstadt. Er hat gemeinsam mit 31 Autor:innen aus seinem eigenen Lehrstuhl und weiteren Universitäten und Institutionen ein umfassendes Lehrbuch verfasst, das in der Hochschullehre eingesetzt werden kann und einen Überblick über den aktuellen Stand der Forschung bietet.

Das Lehrbuch ist nach fünf Jahren in seiner 2. Auflage erschienen. Es führt in das weite Gebiet der Friedens-, Konflikt- und Sicherheitsforschung aus naturwissenschaftlicher, technischer und informationstechnischer Perspektive ein. Es bildet so die Basis für das neue, interdisziplinäre Fachgebiet *Peace Informatics*. Aktuelle politische Veränderungen wie die Kriege in Russland/Ukraine oder Israel/Gaza-Hamas sind eingeflossen.

Das Buch ist in Englisch verfasst. Es hat insgesamt acht Abschnitte/Themengebiete mit 22 Kapiteln, deren Struktur einheitlich ist. Die einzelnen Kapitel beginnen mit einer Zusammenfassung und den Zielen, im Mittelteil werden die Lehrinhalte präsentiert. Die Kapitel enden mit einer Schlussfolgerung, Übungsaufgaben, einer Liste empfohlener Literatur und dem Quellenverzeichnis.

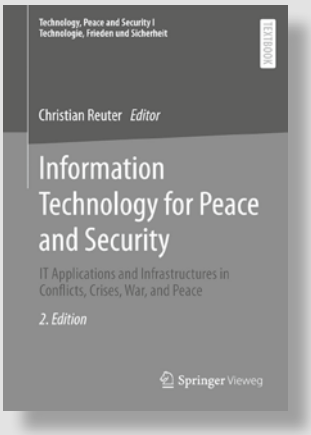
Der erste Abschnitt ist als Einführung konzipiert. Nach einem kurzen Überblick über die folgenden Kapitel, werden die Grundlagen des Lehrbuchs dargelegt. Es wird erklärt, welche Rolle die IT in Krieg und Frieden spielt und die Bedeutung resilienter Infrastrukturen betont, die Konflikte und Krisen verhindern können. Es wird u. a. das Thema Sicherheitsdilemma angerissen. Weiter wird gezeigt, wie Rüstungswettläufe die Sicherheit gefährden, wobei die Bedeutung naturwissenschaftlicher Forschung und Rüstungskontrollen hervorgehoben wird.

Der zweite Abschnitt widmet sich Cyber-Konflikten und Krieg. Er beschreibt die Bedeutung moderner Informationstechnologie für Militär und Geheimdienste, inklusive Cyberkriegsführung. Im Folgenden wird Cyberspionage erklärt, wobei ihre Vorteile und Risiken für Bürger und Unternehmen aufgezeigt werden. Außerdem wird ein Überblick über Darknets gegeben, auf ihre Nutzung für legale und illegale Aktivitäten sowie die Sicherheitsarchitektur dieser Plattformen eingegangen.

Im dritten Abschnitt geht es um Cyber-Frieden. Kapitel 7 analysiert, wie die IT des Militärs beeinflusst und verändert wird und beschreibt politische Entwicklungen im Cyberspace. Weiterhin werden verschiedene Technologien mit Dual-Use Charakter beleuchtet, es werden ethische Aspekte aufgezeigt und die Umsetzung von Bewertungsrichtlinien beschrieben. Schließlich werden vertrauensbildende Maßnahmen im Cyberspace behandelt, die durch Abkommen unterstützt werden.

Der vierte Abschnitt beschäftigt sich mit Rüstungskontrolle im Cyberbereich. Es werden die Architektur von Rüstungskontrollregimen und Herausforderungen im Cyberspace erläutert. Im Folgenden werden Verifikationsmethoden für Cyberwaffen mit denen für chemische, biologische und atomare Waffen verglichen. Schließlich wird die Attribution von Cyberangriffen erklärt und die Fortschritte bei der Täterzuordnung hervorgehoben.

Im fünften Abschnitt werden kritischen Infrastrukturen behandelt. Zunächst wird in das Forschungsgebiet eingeführt, beschrieben werden die wichtigsten Sektoren/Branchen, in denen kritische Infrastrukturen zum Einsatz kommt und die zunehmende Bedeutung der IT insgesamt. Risiken und Beispiele für Angriffe aus der Vergangenheit werden aufgezeigt und allgemeine Verteidigungsmaßnahmen. Zum Schluss werden Merkmale kritischer Infrastrukturen, ihre Bedrohungen und Strategien zu deren Schutz thematisiert.



Christian Reuter ed (2024)
Information Technology for Peace and Security (IT Applications and Infrastructures in Conflicts, War, and Peace),
2. Edition 2024,
ISSN 3004-9318,
ISBN 978-3-658-44809-7,
Springer Fachmedien Wiesbaden GmbH,
532 Seiten, 57,99 Euro

Der sechste Abschnitt widmet sich Künstlicher Intelligenz. Er beschreibt den Einsatz von KI in Cyberwaffen und deren zunehmende Autonomie. Es werden neue Ansätze im Rüstungskontrollwesen gefordert, da die neuen, technologischen Entwicklungen die bisherige Stabilität internationaler Beziehungen gefährden können.

Im siebten Abschnitt wird die Rolle der IKT in Frieden und Konflikt beleuchtet. Untersucht wird der Einfluss sozialer Medien auf Konflikte, inklusive Fake News und Hassrede. Es wird aufgezeigt, wie soziale Medien in Konflikten genutzt werden, und es wird beschrieben, wie Frieden mittels IKT gefördert werden kann, dabei werden ihre Potenziale und Herausforderungen betont.

Der letzte Abschnitt gibt einen Ausblick. Es wird die Bedeutung interdisziplinärer Ausbildung hervorgehoben, insbesondere an der TU Darmstadt und der Goethe-Universität Frankfurt. Er gibt einen Ausblick auf die nächsten 5-15 Jahre im Bereich der IT für Frieden und Sicherheit und zeigt die zukünftigen Herausforderungen auf.

Fazit

Das Buch kann von Anfang bis Ende linear durchgearbeitet werden. Es können aber auch nur einzelne Kapitel gelesen werden. Da die Kapitel für sich einzeln lesbar sind, fehlt eine (buchweite)

einheitliche Definition von Begriffen, dafür existieren kleinere Wiederholungen oder verschiedene Sichten. Dies ist der Vielzahl der Autor:innen aus 14 verschiedenen Einrichtungen geschuldet.

Das Buch erfüllt den Anspruch, interdisziplinär zu sein, vollumfänglich. Die Themen Friedens-, Konflikt- und Sicherheitsforschung werden aus verschieden Perspektiven (naturwissenschaftlich/technisch und informationstechnisch) betrachtet. Die neue politische Weltlage wurde wie eingangs erwähnt berücksichtigt, analysiert und bewertet.

Das Thema Künstliche Intelligenz und Maschinelles Lernen wurde zwar ausgeweitet – ist meines Erachtens aber nicht ausreichend berücksichtigt. Die Aktualität und Relevanz der Beiträge werden mit umfassender und aktueller Quellenangabe belegt. Mit den Übungsaufgaben, der weiterführenden Literatur und den Quellen, bietet es eine sehr gute Basis, um im Unterricht Studierende zu ermuntern, ihr Wissen zu vertiefen und so selbständig vertiefende Seminararbeiten zu den einzelnen Themen anzufertigen.

Für eine weitere Auflage würde ich mir wünschen, dass das Thema Künstliche Intelligenz stark ausgeweitet wird. Insbesondere sollten ethische Aspekte und Verantwortung beim Einsatz von KI in Angriffswaffen diskutiert werden. Das Thema Künstliche Intelligenz sollte in folgenden Punkten ausgebaut werden:

- Aspekte der defensiven Verteidigung insbesondere in kritischen Infrastrukturen
- bei der Angriffserkennung in IT-Netzwerken und
- bei der Malware-Erkennung auf Servern und Endgeräten.

Es könnte untersucht werden, inwiefern eine gute Angriffserkennung und Unschädlichmachen den Aufwand eines Angriffs so kostenintensiv macht, dass es sich nicht mehr lohnt, offensive Digitalwaffen zu entwickeln.

Ebenso sehe ich das KI/ML-Thema im Bereich Social Media, beim Erkennen von Fake News und Hate Speech, aber auch im frühzeitigen Erkennen von Konflikten und Verwerfungen in der physischen Welt.

Weitere Themen wären der Transhumanismus, insbesondere die wachsende Verquickung von Mensch/Maschine/KI zu einem „Superhybrid“ im militärischen Bereich sollte aus technischer, aber auch ethischer Sicht stärker diskutiert werden.

Trotz der angesprochenen Kritikpunkte bleibt es ein solides (Lehr-)Buch, das für angehende Sicherheits-, Friedens- und Informationstechnik gleichermaßen wie für Studierende, für Forschende und weitere an dem Thema Interessierte einen umfassenden Einblick in den Stand der Forschung bietet.

Grundrechte-Report

Grundrechte-Report 2025 der Öffentlichkeit vorgestellt

Am 21. Mai 2025 wurde der Grundrechte-Report 2025. Zur Lage der Bürger- und Menschenrechte in Deutschland *im Haus der Demokratie in Berlin der Öffentlichkeit vorgestellt.*

Der 29. Grundrechte-Report behandelt die Gefährdung von Grund- und Menschenrechten im Jahr 2024. In bislang nicht gekanntem Ausmaß stehen die Kommunikationsgrundrechte und damit die Grundlagen der pluralistischen Demokratie unter Druck. Bestimmte Arten von Versammlungen werden pauschal verboten und Protestcamps mit Gewalt geräumt, die Äußerung von Meinungen wegen ihres Inhalts kriminalisiert, Kulturschaffende und Wissenschaftler:innen unter Generalverdacht gestellt. Der Report behandelt außerdem unter anderem die anhaltende Einschränkung von Rechten Geflüchteter, den Umgang mit Menschen in Haft und Strafvollzug sowie die Militarisierung von Politik und Gesellschaft.

Der Report versteht sich als „alternativer Verfassungsschutzbericht“ und bespricht Entscheidungen von Parlamenten, Behörden und Gerichten, aber auch von Privatunternehmen. Er wird von zehn Bürgerrechtsorganisationen herausgegeben.

Maximilian Steinbeis, freier Publizist und Geschäftsführer des Verfassungsblogs, präsentierte den Grundrechte-Report heute in Berlin. Er unterstrich, wie wichtig der Einsatz für die Grundrechte aktuell ist: „Wir leben in dunklen Zeiten. Die täglichen Nachrichten aus den USA dürfen nicht überdecken, wie sehr auch im Geltungsbereich des Grundgesetzes die autoritäre Wende voranschreitet. Das legt der Grundrechte-Report offen. Genau zur richtigen Zeit.“

Grundrechte-Report 2025 – Zur Lage der Bürger- und Menschenrechte in Deutschland. Herausgegeben von: Peter von Auer, Charlotte Ellinghaus, Rolf Gössner, Martin Heiming, Max Putzer, Britta Rabe, Rainer Rehak, John Philipp Thurn, Marie Volkmann, Rosemarie Will, Fischer Taschenbuch Verlag, Frankfurt/M 2025,
ISBN: 978-3-596-71238-0,
240 Seiten, 14,00 Euro.

Sevda Can Arslan, die in der Initiative 2. Mai aktiv ist, trug vor: „Die vielen Fälle von tödlicher Polizeigewalt haben ein Muster: Die Getöteten sind marginalisiert und befinden sich häufig in psychischen Krisen. Immer ist im Polizeinarrativ von Notwehr die Rede, nie von institutionellem Rassismus. Die Hinterbliebe-

nen werden allein gelassen und müssen selbst für Aufklärung und Gerechtigkeit sorgen. Doch die Deutungshoheit der Polizei beginnt immer mehr zu bröckeln, zu viele Menschen sagen inzwischen, dass dies keine Einzelfälle sind."

Jessica Grimm, Strafverteidigerin in Berlin, berichtete über Strafverfahren gegen Studierende, die aus Protest u. a. gegen den Krieg in Gaza Teile der Humboldt-Universität zu Berlin sowie der Freien Universität besetzt haben: „Meinungsfreiheit versus Staatsräson: Die in Deutschland wiederauflebenden Studierendenproteste werden von staatlichen Institutionen mit drastischen Grundrechtseinschränkungen beantwortet. Das Recht auf Protest ist fundamental und muss verteidigt werden. Dem geht der Grundrechte-Report nach."

Charlotte Ellinghaus, die Rechtswissenschaft an der Universität Hamburg studiert und Mitglied im Bundesvorstand der Vereinigung Demokratischer Jurist:innen (VDJ) ist, erläuterte die Ziele der Redaktion des Grundrechte-Reports: „Die im Report erläuterten Fälle zeigen deutlich, wie unsere per Grundgesetz geschützten Bürgerrechte zunehmend durch den deutschen Staat eingeschränkt werden. Der Report dokumentiert, an welchen Stellen und mit welchen Mitteln diese Entwicklung vorangetrieben wird, und möchte damit zum politischen Engagement gegen diese Tendenz motivieren."

Das Buch ist ab dem 28. Mai 2025 über den Buchhandel oder die Webseite der Herausgeber zu beziehen (http://www.grundrechte-report.de/quermenue/bestellen/).

*Der Grundrechte-Report 2025 ist ein gemeinsames Projekt von: Humanistische Union, vereinigt mit der Gustav Heinemann-Initiative • Bundesarbeitskreis Kritischer Juragruppen • Internationale Liga für Menschenrechte • Komitee für Grundrechte und Demokratie • Neue Richter*innenvereinigung • PRO ASYL • Republikanischer Anwältinnen- und Anwälteverein • Vereinigung Demokratischer Jurist:innen • Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung • Gesellschaft für Freiheitsrechte*

Wissenschaft und Frieden 2/2025

Nicht verzagen!
Weitermachen in Zeiten multipler Krisen

Kriege, Polarisierung und Katastrophen: Die 20er Jahre dieses Jahrhunderts sind eine Zeit multipler Krisen. Lässt auch Sie die globale Situation derzeit an die Grenzen Ihrer Zuversicht stoßen? In dieser neuen Ausgabe wendet sich W&F der Frage zu, warum und wie in Zeiten wie diesen weitergekämpft werden kann und muss.

Auf der Suche nach konkreten Handlungsmöglichkeiten wider das Resignieren diskutieren die Beiträge der Ausgabe 2/25 Konzepte wie *Resilienz* und *Widerstand*, *Hoffnung* und *strategischen Optimismus* und schaffen so eine Basis „zum Weitermachen". Sie stellen aber auch Beispiele aus der Praxis vor, die der Feindlichkeitsspirale mit Solidarität trotzen und argumentieren, warum gerade jetzt Errungenschaften wie Völkerrecht und Abrüstung gemeinsam gestärkt werden müssen.

Mit Beiträgen von *Kerstin Schlögl-Flierl* und *Tim Zeelen, Werner Wintersteiner, Emma Brahm et al, Juliane Hauschulz* und weiteren

Weitere Schwerpunkte: Salakhova und Danylov: Interview zur Situation in der Ukraine im 3. Kriegsjahr I Klippert: Neue Perspektiven auf Friedenspädagogik

W&F 2/25 | Mai | 52 Seiten | 12 € (druck) / 9 € (ePUB+PDF)

Beilage: Dossier 100 – Johann Ivanov und Paul Schäfer (Hrsg.): Krise der Weltpolitik: Multilateralismus gefragt | 28 Seiten | 2 € Schutzpreis (print+digital)

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung

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

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

FIfF online

Das ganze FIfF
www.fiff.de
Twitter FIfF e.V. – *@FIfF_de*

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

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

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

FIfF-Mailinglisten

FIfF-Mailingliste
An- und Abmeldungen an:
https://lists.fiff.de
Beiträge an: *fiff-L@lists.fiff.de*

FIfF-Mitgliederliste
An- und Abmeldungen an:
https://lists.fiff.de

FIfF-Beirat

Ute Bernhardt (Berlin); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Christina B. Class** (Jena); 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); Prof. Dr. **Eberhard Zehendner** (Jena)

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Rainer Rehak (stellv. Vorsitzender) – Berlin
Michael Ahlmann – Kiel / Blumenthal
Gilbert Assaf – Berlin
Alexander Heim – Berlin
Sylvia Johnigk – München
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Dr. **Friedrich Strauß** – München
Prof. Dr. **Werner Winzerling** – Magdeburg
Margita Zallmann – Bremen

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen
Benjamin Kees – Berlin

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 200 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck
Schwerpunktredaktion	Stefan Hügel
V.i.S.d.P.	Stefan Hügel
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder, München
Cover	Impression von der FIfF-Konferenz 2022 FIfFKon22 CC BY XPulse
Druck	Girzig+Gottschalk GmbH, Bremen Heftinhalt auf 100 % Altpapier gedruckt.

Druckprodukt mit finanziellem Klimabeitrag
ClimatePartner.com/12164-2404-1001

Aktuelle Ankündigungen

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

FIfF-Konferenz 2025: 21.-23. November 2025, Wien
Digitaler Humanismus für eine techno-öko-soziale Transformation der Weltgesellschaft

FIfF-Kommunikation

3/2025 Schwerpunkt noch nicht entschieden; Vorschläge erwünscht

Zuletzt erschienen:

2/2024 40 Jahre FIfF – denkwürdige Zeiten
3/2024 Datenschutz überall – außer in der Praxis?
4/2024 Künstliche Intelligenz zwischen euphorischen Erwartungen und dystopischen Szenarien
1/2025 FIfF-Konferenz 2024: Nachhaltigkeit in der IT green coding – open source – green by IT

W&F – Wissenschaft & Frieden

2/24 Fokus Mittelmeer
3/24 Widerstehen – Widersetzen
4/24 Eskalationen im Nahen Osten
1/25 Wider das Vergessen
2/25 Nicht verzagen! Weitermachen in Zeiten multipler Krisen

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

#245/246 Klima(un)gerechtigkeit
#247 Kontrolle der Polizei
#248 Zukunft der Bildung
#249 Zum Stand der deutschen Einheit
#250 Demokratisierung

DANA – Datenschutz-Nachrichten

1/24 DSGVO und BDSG und Datenschutzaufsicht
2/24 Gesundheitsdaten
3/24 Nach der Europawahl
4/24 Betroffene und ihre Rechte
1/25 Digitalzwang
2/25 Social Media

Das FIfF-Büro

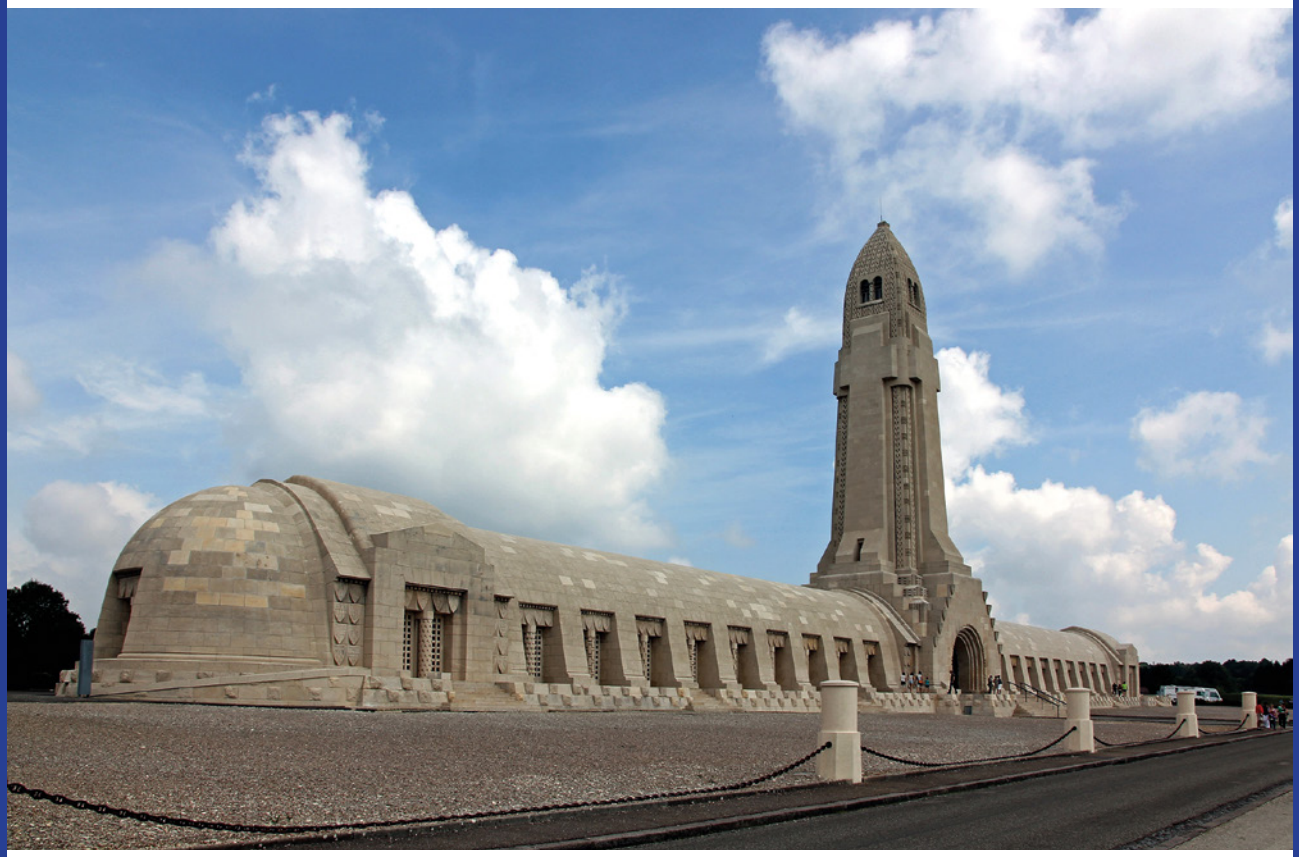
Geschäftsstelle FIfF e. V.
Ingrid Schlagheck (Geschäftsführung)
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
E-Mail: fiff@fiff.de
Die Bürozeiten finden Sie unter *www.fiff.de*

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

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

Schluss FIfF

Über 130.000



Das Beinhaus von Douaumont (französisch Ossuaire de Douaumont) ist eine französische nationale Grabstätte für die Gebeine der Gefallenen, die nach der Schlacht um Verdun nicht identifiziert werden konnten.

Das Beinhaus (Ossarium) befindet sich auf dem Gebiet der ehemaligen Ortschaft Douaumont. In ihm werden die Gebeine von über 130.000 nicht identifizierten französischen und deutschen Soldaten aufbewahrt.

2019 waren 556.424 Besucher vor Ort.

Quelle: https://de.wikipedia.org/wiki/Beinhaus_von_Douaumont

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