Chris Piallat (Hg.)

DER WERT DER DIGITALISIERUNG

Gemeinwohl in der digitalen Welt

[transcript] Digitale Gesellschaft

Chris Piallat (Hg.)
Der Wert der Digitalisierung

Digitale Gesellschaft | Band 36

Die freie Verfügbarkeit der E-Book-Ausgabe dieser Publikation wurde ermöglicht durch den Fachinformationsdienst Politikwissenschaft POLLUX

und ein Netzwerk wissenschaftlicher Bibliotheken zur Förderung von Open Access in den Sozial- und Geisteswissenschaften (transcript, Politikwissenschaft 2021)

Die Publikation beachtet die Qualitätsstandards für die Open-Access-Publikation von Büchern (Nationaler Open-Access-Kontaktpunkt et al. 2018), Phase 1
https://oa2020-de.org/blog/2018/07/31/empfehlungen_qualitätsstandards_oabücher/

Hauptsponsor: Staats- und Universitätsbibliothek Bremen (POLLUX – Informationsdienst Politikwissenschaft)
Vollsponsoren: Universitätsbibliothek Bayreuth | Universitätsbibliothek der Humboldt-Universität zu Berlin | Freie Universität Berlin - Universitätsbibliothek | Staatsbibliothek zu Berlin | Universitätsbibliothek Bielefeld | Universitätsbibliothek der Ruhr-Universität Bochum (RUB) | Universitäts- und Landesbibliothek Bonn | Vorarlberger Landesbibliothek | Universitätsbibliothek der Technischen Universität Chemnitz | Universitäts- und Landesbibliothek Darmstadt | Sächsische Landesbibliothek Staats- und Universitätsbibliothek Dresden (SLUB) | Universitätsbibliothek Duisburg-Essen | Universitäts- und Landesbibliothek Düsseldorf | Universitätsbibliothek Erlangen-Nürnberg | Universitätsbibliothek Frankfurt/M. | Niedersächsische Staats- und Universitätsbibliothek Göttingen | Universitätsbibliothek Greifswald | Universitätsbibliothek der FernUniversität in Hagen | Staats- und Universitätsbibliothek Carl von Ossietzky, Hamburg | TIB – Leibniz-Informationszentrum Technik und Naturwissenschaften und Universitätsbibliothek | Gottfried Wilhelm Leibniz Bibliothek - Niedersächsische Landesbibliothek | Universitätsbibliothek Heidelberg | Universitätsbibliothek Kassel | Universitätsbibliothek Kiel (CAU) | Universitätsbibliothek Koblenz · Landau | Universitäts- und Stadtbibliothek Köln | Universitätsbibliothek Leipzig | Zentral- und Hochschulbibliothek Luzern | Universitätsbibliothek Otto-von-Guericke-Universität Magdeburg | Universitätsbibliothek Marburg | Max Planck Digital Library (MPDL) | Universitäts- und Landesbibliothek Münster | Universitätsbibliothek der Carl von Ossietzky-Universität, Oldenburg | Universitätsbibliothek Osnabrück | Universitätsbibliothek Passau | Universitätsbibliothek St. Gallen | Universitätsbibliothek Vechta | Universitätsbibliothek Wien | Universitätsbibliothek Wuppertal | Zentralbibliothek Zürich
Sponsoring Light: Bundesministerium der Verteidigung | Landesbibliothek Oldenburg
Mikrosponsoring: Stiftung Wissenschaft und Politik (SWP) - Deutsches Institut für Internationale Politik und Sicherheit | Leibniz-Institut für Europäische Geschichte, Mainz

Chris Piallat, geb. 1984, arbeitet zu gesellschaftspolitischen Fragen der Digitalisierung. Er ist Referent für Digital- und Netzpolitik für die Bundestagsfraktion Bündnis 90/Die Grünen. Neben seiner politischen Beratung arbeitet er als Autor, Redakteur und Sprecher, u.a. für die Kulturstiftung des Bundes, die Berliner Gazette und die Heinrich-Böll-Stiftung. Er hat Politikwissenschaften an der Freien Universität Berlin, der Rutgers University New Jersey und der Universität Kassel studiert.

Chris Piallat (Hg.)

Der Wert der Digitalisierung

Gemeinwohl in der digitalen Welt

[transcript]

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Erschienen 2021 im transcript Verlag, Bielefeld

Umschlaggestaltung: Maria Arndt, Bielefeld
Korrektorat: Leandra Thiele
Druck: Majuskel Medienproduktion GmbH, Wetzlar
Print-ISBN 978-3-8376-5659-6
PDF-ISBN 978-3-8394-5659-0
EPUB-ISBN 978-3-7328-5659-6
https://doi.org/10.14361/9783839456590
Buchreihen-ISSN: 2702-8852
Buchreihen-eISSN: 2702-8860

Gedruckt auf alterungsbeständigem Papier mit chlorfrei gebleichtem Zellstoff.
Besuchen Sie uns im Internet: *https://www.transcript-verlag.de*
Unsere aktuelle Vorschau finden Sie unter *www.transcript-verlag.de/vorschau-download*

Inhalt

Vorwort

Wir erleben einen Zeitenbruch. Wie wir arbeiten, kommunizieren und lernen, wandelt sich in kaum zu fassender Geschwindigkeit. Internet und Digitalisierung haben sich schnell und allumfassend verbreitet und sind zentraler Bestandteil unseres Alltags geworden. Diese Beschleunigung erleben wir aktuell auch mit der Verbreitung und Normalisierung von Homeoffice, Lernplattformen, Online-Handel oder Apps für Kontaktnachverfolgungen und Check-Ins.

Gesellschaftliche und politische Debatten über Wandel werden allerdings nicht nur von schieren Fakten geleitet. Gedankliche Deutungsrahmen, mit denen wir die uns umgebende Welt zu erfassen versuchen, haben einen mindestens so großen Einfluss auf unser Handeln. Angesichts der Herausforderungen der Zeit werden wir uns zunehmend bewusst, dass individuelle Lebensweisen und gesellschaftlicher Konsens nicht selbstverständlich sind. Die ganze Dimension des Wandels zu erfassen, birgt die Chance, unser Verhältnis zu vorher als selbstverständlich erachteten Werten neu auszutarieren: Welche Freiheit wollen wir? Was ist gerecht? Wie wahren wir das Gemeinwohl?

Das gilt insbesondere für die große Herausforderung des 21. Jahrhunderts, die *Gestaltung der digitalen Transformation*. Wir haben die Segnungen des technologischen Fortschritts bisher wohlwollend in unseren Alltag aufgenommen. Nun sind wir an einem Punkt angekommen, an dem wir die Digitalisierung nicht mehr als etwas Selbstverständliches, als etwas, das einfach passiert oder einfach ist, hinnehmen können. Denn wir schaffen sie mit unserem Handeln oder eben auch unserer Untätigkeit. Wir müssen uns ihrer also bewusst werden und die immer drängendere Frage stellen: Wie wollen wir die digitale Transformation gestalten?

Denn Digitalisierung ist weder gut noch schlecht; schon gar nicht ist sie neutral. Sie ist das, was wir aus ihr machen. Digitalisierung kann uns als Werkzeug beispielsweise bei der Bekämpfung einer Pandemie helfen. Apps, Plattformen, autonome Systeme oder digitalisierte Prozesse können uns zu-

sammenführen, uns erkennen lassen, was wir bisher nicht zu sehen vermochten oder neue Kulturtechniken und gesellschaftliche Teilhabe ermöglichen. Die Zukunft der Digitalisierung ist ungewiss. Klar ist aber, dass wir uns mit den Faktoren der Gestaltung der digitalen Transformation befassen müssen.

Ohne Übertreibung stehen wir vor weitreichenden Entscheidungen. Konkret geht es beispielsweise um den Einsatz von künstlicher Intelligenz sowie algorithmischer und automatisierter Systeme, die über Preise und Kredite, Ausbildungsplätze oder individuelle medizinische Behandlungen entscheiden. Wie viel menschliche Entscheidungskompetenz wollen wir im Gericht, in der Schule oder im Krankenhaus abgeben? Wie integrieren wir technologische Innovationen wie gemischte Realitäten und Mensch-Maschine-Entgrenzungen in unseren Alltag und für eine bessere Gesellschaft? Wollen wir humanoide Roboter, teilautonome (Fahr)assistenten und autonome tödliche Waffen einsetzen, und wenn ja, wie? Diese Herausforderungen diskursiv zu begleiten und politisch zu gestalten, ist eine der dringlichsten und meist diskutierten Aufgaben unserer Zeit und entscheidet maßgebend, wie wir leben werden. Daher gibt es mindestens drei Gründe, warum dieses Buch notwendig ist.

Der erste liegt in der gesellschaftspolitischen Dringlichkeit. Wir können die digitale Zukunft als Gesellschaft nicht weiter aussitzen, wir müssen sie gestalten. Nur wie? Damit kommen wir zum zweiten Grund für dieses Buch: Mit ihm wird der Versuch unternommen, das normative Konstrukt des *Gemeinwohls* für die Digitalisierungsdebatte fruchtbar zu machen. Und drittens wird mit diesem Buch eine diskursive Lücke geschlossen. In der deutschsprachigen Digitaldebatte gibt es bisher kaum einen in einem Buch versammelten breiten Querschnitt von Beiträgen von Politiker*innen, Wissenschaftler*innen und Praktiker*innen, der aufzeigt, wie technologische Phänomene mit unseren Werten in Einklang gebracht werden können und wie die Idee des Gemeinwohls einer progressiven Gestaltung der Digitalisierung und einer besseren Gesellschaft dienen kann. In diesem Sinne soll das vorliegende Buch zu einer breiteren gesellschaftlichen Debatte über die Herausforderungen der digitalen Transformation beitragen und Angebote für eine wertegeleitete Gestaltung der Digitalisierung unterbreiten.

Für diese diskursive Suche sind folgende Fragen leitend: Welche Werte wollen wir für die Gestaltung der digitalen Welt heranziehen? Wie können wir das einende Band der gemeinsamen Werte und Grundrechte in das digitale Zeitalter transformieren? Wie können wir, statt mit *Reparatur-Ethik* und korrigierendem Recht zu reagieren, vor die Lage kommen und konstruktive

und progressive Ideen für eine (rechtliche) Ordnung der digitalen Zukunft entwickeln? Welche Formen der gesellschaftlichen und politischen Steuerung sind für digitale Technologien und Werte denkbar, erfolgversprechend und durchsetzbar? Diesen Themen und Herausforderungen widmen sich die Autor*innen dieses Buches.

Die Beiträge in diesem Buch bieten eine breite und tiefe Diskussion über normative Impulse und Ideen für das Gemeinwohl in der digitalen Welt. Sie beleuchten theoretische, kritische und praxisorientierte Perspektiven. Sie sind dabei stilistisch und konzeptionell höchst vielfältig. Mal argumentieren sie konkret rechtlich oder sind visionär, mal kreisen sie um Phänomene oder bieten klare handlungsleitende Antworten. Dabei folgen sie keinem dezidiert theoretischen oder politischen Programm. Alle stellen auf unterschiedliche Art gemeinwohlorientierte Ansätze für die digitale Welt vor.

In diesem Buch wird die analytisch-prognostische Sicht auf die digitale Zukunft durch eine bewusst normative Sicht des Wollens und Sollens ergänzt. So soll der Versuch unternommen werden, der Naturalisierung (Digitalisierung ist und passiert einfach) ein handlungs- und gestaltungsleitendes Verständnis von Werten gegenüberzustellen. Kurz: Der existierenden normativen Kraft des Faktischen der Digitalisierung aller Lebensbereiche wird eine faktische Kraft des Normativen zur Gestaltung der Digitalisierung entgegen gestellt.

Die ausgewählten Themen für den Theorie-Empirie-Dialog zeigen, wie sich Digitalisierungsphänomene auf die Gesellschaft sowie ihre Werte auswirken und umgekehrt. Selbstverständlich können nicht alle Phänomene und Themen umfassend erörtert werden. Es fehlen beispielsweise Diskussionen über Bildungsgerechtigkeit als Voraussetzung für Teilhabe in der digitalen Welt oder eine globale Perspektive auf den *digital gap* zwischen hoch technologisierten und weniger durchdigitalisierten Staaten. Ohnehin spiegelt dieses Buch größtenteils die deutsche Digitaldebatte, unter anderem, da sich die Gemeinwohlbindung einer Digitalpolitik und das geforderte Primat der Werte und des Rechts besser auf nationalstaatlich umschriebene und verfasste Gesellschaften anwenden lassen. Die allgegenwärtige Digitalisierung macht es freilich nötig, Ideen und Vorschläge auch über nationale Grenzen hinweg zu entwickeln. Das soll und muss Gegenstand weiterer Debatten sein. Ebenso deuten sich am Horizont bereits neue disruptive Technologien an, beispielsweise erweiterte Realitäten, Internet-of-Things und die zunehmende Entgrenzungen von Mensch-Maschine-Verhältnissen, breite Anwendungsfelder künstlicher Intelligenz und der große Sprung in der Rechenleistung durch

Quantencomputing. Dementsprechend stehen wir erst am Anfang, die richtigen Fragen zu stellen und die Wirkung der Digitalisierung auf unser Leben zu begreifen. Die angebotenen Perspektiven in diesem Buch sollen helfen, unseren Blick auf die notwendige Gestaltung der digitalen Zukunft zu schärfen. Denn alles wird vernetzt, alles wird smart und alles wird digital. Nur wie?

Aufbau des Buches

Das Buch folgt einer Dreiteilung. Nach einer Einführung in das Thema des Buches, einer gemeinwohlorientierten Antwort auf die Verantwortungsdiffusion in der digitalen Welt, werden unterschiedliche Wertekonzepte diskutiert.

Im zweiten Teil werden die zahlreichen digitalen Phänomene und die vielen Wertedimensionen ansatz- und auszugsweise besprochen. Dabei wird der Wandel prägender Konzepte und Werte wie Freiheit, Demokratie oder Nachhaltigkeit mit verschiedenen Digitalisierungsphänomenen konfrontiert und zusammengeführt. Das macht die Auseinandersetzung zugänglicher und öffnet ein breites Themenspektrum. In den Beiträgen nähern sich die Autor*innen dem stets zu verhandelnden Gemeinwohl aus unterschiedlicher Perspektive an. Sie legen dafür so divergierende Werte wie Freiheit und Autonomie (1.), Gerechtigkeit und Gleichheit (2.) oder Demokratie, Zugang und Souveränität (3.) zugrunde.

Im dritten Teil geben die Autor*innen übergeordnete Antworten auf die Frage, was aus den bisherigen Transformationen gelernt werden konnte, welche Handlungsspielräume es auf welcher Ebene gibt und wie gesellschaftspolitische Steuerung aussehen kann. Wir kommen also vom Warum und der Beschreibung verschiedener Werte schließlich zur Frage, wie eine gemeinwohlorientierte Gestaltung realisiert werden kann.

Überblick über die Beiträge

Im einführenden Beitrag werden die Wechselwirkungen zwischen den digitalen Realitäten und den Entwicklungen der Werte skizziert und zur Orientierung der Kompass des Gemeinwohls angeboten. **Chris Piallat** legt damit ein konzeptionelles Fundament für die folgenden Kapitel. Zunächst wird kurz die rasante Reise des Digitalisierungsdiskurses von den libertären Anfängen des

Internets hin zu einer gesamtgesellschaftlichen Debatte über die Gestaltung der Digitalisierung rekapituliert, um danach die diskursiven Pole der Debatte und den ethischen sowie faktischen Gestaltungs- und Handlungsdruck aufzuzeigen. Über den Dreischritt Freiheit, Verantwortung und Nachhaltigkeit gelangen wir zum Konzept des Gemeinwohls. Schließlich wird erörtert, wie Gemeinwohl zur Gestaltung der digitalen Zukunft beitragen kann.

Wenn wir die Parameter festlegen, entlang derer wir unsere digitale Zukunft gestalten wollen, müssen wir uns zunächst darüber verständigen, wie sich unser gemeinsamer ethischer Kompass zusammensetzt. **Petra Grimm** erläutert hierfür im zweiten Teil die Grundlagen und diskutiert, wie unterschiedliche Konzepte von Werten (teleologisch, deontologisch und tugendhaft) für die Gestaltung der Digitalisierung gedacht und genutzt werden können. Entlang von Beispielen werden potenzielle Wertekonflikte beim Einsatz neuer Technologien aufgezeigt. Anschließend wird der Unterschied zwischen moralischen und universalen Werten erläutert und herausgearbeitet, welche für die Gestaltung der Digitalisierung relevant sind. Dafür wird eine kursorische Werte-Topografie mit Stärken und Schwächen der Ansätze angeboten.

Ein Überblick über die Werte, die in einer digitalen Gesellschaft verhandelt werden, kann nicht allumfassend sein. Im zweiten Teil des Buches werden deshalb unter dem Gesichtspunkt des Gemeinwohls digitale Phänomene hinsichtlich dreier ausgewählter Wertebereiche abgesucht: 1. Freiheit und Autonomie, 2. Gerechtigkeit und Gleichheit und 3. Demokratie, Zugang und Souveränität.

Im ersten Abschnitt »Freiheit und Autonomie« betrachten wir verschiedene Freiheitsformen und wie diese in der digitalen Welt realisiert werden können.

Den Anfang macht **Ellen Ueberschär**, die vor der historischen Folie von Totalitarismuserfahrungen fragt, wie wir ein stärkeres Bewusstsein für Grund- und Freiheitsrechte in der digitalen Welt erreichen können. Sie argumentiert, dass digitale Freiheit nur als Teilhabeprojekt zu verwirklichen ist.

Christiane Woopen und **Sebastian Müller** diskutieren, ob Menschen mit zunehmender Digitalisierung ihre Selbstbestimmung und ihre Freiheit verlieren und wenn ja, wie dem entgegengewirkt werden kann. Dies erläutern sie entlang von Alltagsbeispielen aus dem digitalisierten Gesundheitssektor.

Anschließend untersuchen **Thomas Rademacher** und **Erik Schilling**, wie sich die zunehmende digitale Berechenbarkeit menschlichen Handelns auf unsere Autonomie auswirkt und welche Bedeutung dem Zufall bei der Wah-

rung von Freiheiten zukommt. Dazu betrachten sie zunächst das Verhältnis von Berechenbarkeit und Zufall in der fiktionalen Literatur, um dann zu fragen, ob dem Zufall von Rechts wegen ein Platz in unserem Leben eingeräumt werden sollte.

Eng verknüpft mit der Wahrung der Autonomie in der digitalen Welt ist die konkrete rechtliche Um- und Durchsetzung von Persönlichkeitsrechten. **Nils Leopold** beschreibt, warum der viel diskutierte Datenschutz auch weiter ein umkämpftes Feld bleiben wird, wie er konstruktiv weiterentwickelt und wie die Privatheit in einer durchdigitalisierten Welt gewahrt werden könnte.

Die Grundlage aller Wertedebatten bildet die grundrechtlich geschützte Würde. **Philipp Staab** und **Dominik Piétron** führen uns ins Zentrum der uns bekannten digitalen Realität, die Plattformmärkte. Sie erläutern, wie Modelle digitaler Plattformen funktionieren und wie diese mit der Theorie gesellschaftlicher Freiheit zusammengedacht werden können. Schließlich bieten sie mehrere Prinzipien für gemeinwohlorientierte Plattformen an.

Im zweiten Abschnitt »Gerechtigkeit und Gleichheit« soll es um die großen Fragen der Gerechtigkeit gehen. Wie können Ungleichheiten und Ungerechtigkeiten wertegeleitet überwunden werden? Gibt es den dafür notwendigen langen Atem in der Digitalisierung überhaupt?

Lorena Jaume-Palasí nimmt uns mit auf eine archäologische Reise. Dabei lernen wir, dass Diskriminierung durch algorithmische Systeme (Künstliche Intelligenz) im Wesentlichen auf einem tief verankerten mechanischen Denken basiert. Sie argumentiert, dass für die vielfach geforderte Diskriminierungsfreiheit das kategoriale und mechanische Denken überwunden werden müssen.

Künstliche Intelligenz steht aktuell im Mittelpunkt des Digitalisierungsdiskurses. In diesem Kontext gibt **Eric Hilgendorf** einen Einblick in die Entstehung und Logik konkreter Handlungsempfehlungen, die einerseits zur Wahrung der Menschenwürde beitragen sollen und andererseits Menschenwürde als Fundament für die Gestaltung künstlicher Intelligenz nutzen.

Francesca Schmidt und **Nicole Shephard** positionieren Geschlechtergerechtigkeit als notwendigen Bestandteil der digitalen Transformation. Dabei führen sie in die intersektionale feministische Perspektive ein. Aufbauend auf feministischen Theorien wird beleuchtet, wie Geschlechterfragen die digitalisierte Gegenwart prägen, insbesondere in Bezug auf digitale Gewalt, algorithmische Mehrfachdiskriminierung sowie Vielfalt in der Digitalisierung.

Kann Nachhaltigkeit für die Gestaltung der Digitalisierung fruchtbar gemacht werden? **Tilman Santarius** verortet das Konzept der Nachhaltigkeit normativ und arbeitet heraus, wie eine breit gedachte Klimagerechtigkeit eine gemeinwohlorientierte Gestaltung der Digitalisierung leiten könnte.

Im dritten Abschnitt »Demokratie, Zugang und Souveränität« geht es um die Erosion gesellschaftlich geteilter Werte und um Macht. Wie können wir zum demokratischen Konsens und zur Souveränität zurückfinden?

Die plattformbasierte mediale Öffentlichkeit ist geprägt durch einen tiefen Wandel. **Christian Stöcker** stellt anhand zahlreicher Beispiele die Frage, wie liberale Demokratien die digitale Öffentlichkeit als konstruktiven und produktiven Ort der Willensbildung bewahren können.

Angesichts der rasanten Karriere des Frames der digitalen Souveränität analysieren **Julia Pohle** und **Thorsten Thiel** die unterschiedlichen Deutungen des Begriffs und welche Erwartungen und politische Maßnahmen sich daraus ableiten. Sie diskutieren dabei, ob und wie Werte wie Gemeinwohl oder Offenheit mit Souveränität zusammengedacht werden können.

Im dritten Teil des Buches suchen die Autor*innen nach Antworten, wie wir von der Verantwortungsdiffusion zur Governance des Digitalen gelangen können. Sie zeigen, wie breit das Feld der Governance ist, und bieten Ausblicke an, wie diese in Zukunft aussehen könnte. Die Richtung deutet sich an, wird die Digitalisierung doch zunehmend genormt, rechtlich geordnet und so Verantwortung hergestellt.

Um Antworten geben zu können, müssen wir zunächst Digitalpolitik lokalisieren. Einführend gibt **Matthias C. Kettemann** einen Überblick über die unterschiedlichen Ebenen und Formen der nationalen und internationalen Governance der digitalen Welt. Anhand von Beispielen, wie Regelsetzungen durch technische Standards, durch *soft law*, durch nationale und internationale Gesetze und völkerrechtliche Kodifizierung, diskutiert er, ob es international geteilte Werte für die Digitalisierung gibt und wie sie in einem Mehrebenensystem für die Digitalisierung verankert werden können.

Wie kann eine wertegeleitete Digitalpolitik konkret umgesetzt werden? **Stefan Heumann** fokussiert sich bei der Antwortsuche auf den Staat, die Ministerien und Behörden, die einen großen Teil der Digitalpolitik umsetzen. Er plädiert für einen Kulturwandel auf der Mikroebene und schlägt Reformen in der Governancestruktur vor.

Nicht nur der Gesetzgeber, sondern auch die Rechtsprechung muss mit der Zeit gehen. **Ulf Buermeyer** und **Malte Spitz** zeigen auf, wie Gerichte und insbesondere das Bundesverfassungsgericht mit wegweisenden Urteilen den

technologischen Fortschritt immer wieder wertebasiert einhegen und so die (Verfassungs)rechtsordnung fit für das digitale Zeitalter machen.

Julia Kloiber und **Elisa Lindinger** verweisen in ihrem Beitrag auf die oft unterschätzte Bedeutung der Vielfalt und die kreative Kraft der Zivilgesellschaft. Sie stellen heraus, wie zivilgesellschaftliche Organisationen mit eigenen Visionen die Digitalisierung im Sinne des Gemeinwohls mitgestalten können.

Abschließend hebt **Tyson Barker** die Debatte auf die internationale Ebene. Er skizziert, wie wertebasierte Standards im geopolitischen Systemwettbewerb gewahrt werden können und bietet drei Wege in die europäische digitale Zukunft an.

Dank

Die Entstehung dieses Buchs habe ich mehreren Menschen zu verdanken. Zunächst danke ich den hier versammelten Autor*innen. Sie haben allesamt unter pandemiebedingt erschwerten Bedingungen ihre Texte geschrieben und in intensiver wie anregender Zusammenarbeit weiterentwickelt. Von Seiten des transcript Verlags möchte ich Jakob Horstmann für Impulse und Beantwortung aller Fragen danken. Jana Schrewe danke ich für das minutiöse Lektorat. Für konzeptionelles, inhaltliches und formales Feedback bedanke ich mich bei Krystian Woznicki, Julian Wenz, Sabine Muscat und Klaus Jähnert-Piallat. Mein größter Dank gilt Lili und Lino. Für alles.

Chris Piallat, Juni 2021

I. Welche Digitalisierung – Welche Werte? Warum wir (wieder) über Werte reden müssen

1.1 Von der Verantwortungsdiffusion zum Gemeinwohl in der digitalen Welt

Chris Piallat

1 Digitaler Gestaltungsdruck

Alles wird vernetzt, alles wird smart und alles wird digital. Der Digitalisierungsschub der letzten Jahrzehnte hat so große Erwartungen und gesellschaftliche Umbrüche ausgelöst, dass er zu einer oder gar der dominierenden transformativen Kraft des 21. Jahrhunderts geworden ist. Immer eindringlicher wird uns vor Augen geführt, dass wir die digitale Zukunft als Gesellschaft nicht aussitzen können, sondern sie gestalten müssen. Jede Epoche bringt neue ethische Herausforderungen, aber diesmal sind wir gleich mit der digitalen Transformation aller Gesellschaften und aller gesellschaftlichen Bereiche konfrontiert. Noch nie war der Bedarf nach Ansätzen für eine wertegeleitete Gestaltung der digitalen Welt so groß. Dabei müssen wir uns umfassenden Fragen stellen: Wie ist unser gesellschaftliches Verhältnis zur digitalen Welt, die wir geschaffen haben und die uns umgibt? Müssen wir uns im Angesicht eines globalen digitalen Systemwettbewerbs von einigen Werten verabschieden, um schneller und vermeintlich innovativer zu werden? In welcher digitalen Zukunft wollen wir als Gesellschaft leben?

Haben sich bei anderen gesellschaftlichen Umbrüchen kollektive Konventionen und rechtliche Normen über Jahrhunderte etabliert, vollzieht sich die digitale Transformation in extrem schneller Taktung. Wir sind in wenigen Jahrzehnten von ultra-libertären Anfängen des Internets und gesellschaftlichen Versprechen (Stichwort: »Unabhängigkeitserklärung für den Cyber-Raum«) über eine kurze Phase der individuellen Freiheitsversprechen (Stichwort: Interaktives Web 2.0 und Arabischer Frühling), deren Bruch und der Dominanz von Themen wie Überwachung, IT-Sicherheit und Datenschutz (Stichwort: Snowden-Enthüllungen und Überwachungskapitalismus) zu einer rechtlichen Einhegung der ökonomisierten Digitalisierung (Stich-

wort: Regulierung von Plattformmärkten, autonomen und automatischen Systemen) gereist. Innerhalb einer Generation hat sich die Debatte von individueller Tugendhaftigkeit (Stichwort: Netiquette) hin zur Etablierung einer Weltordnung des Digitalen weiterentwickelt (Stichwort: Digitales Ordnungs- und Völkerrecht).

Der Handlungs- und Gestaltungsdruck ist entsprechend riesig und überall spürbar. Die Bewältigung der *Corona-Krise* hat dies eindrucksvoll und teils leidvoll aufgezeigt. Denken wir nur an die mit Schnappatmung geführten Debatten über die effektive und doch grundrechtswahrende Ausgestaltung und Weiterentwicklung der Corona-Warn-App oder des Freiheiten ermöglichenden digitalen Impfpasses. Oder an die vielen Eltern, die angesichts nicht funktionierender digitaler Dienste für das Homeschooling schier verzweifelten. Oder an die lange verschleppte und dann innerhalb weniger Tage beschleunigte Debatte über den rechtlichen Anspruch auf Homeoffice.

Vor lauter technologischer Überwältigung und Faszination erkennen wir nicht, dass wir als Gesellschaft genau jetzt eine Phase durchleben, die kommende Generationen womöglich als die historische und verpasste Chance der Gestaltung beschreiben werden. Auch nach Jahren der wissenschaftlichen, gesellschaftlichen und politischen Debatten über den *Megatrend des 21. Jahrhunderts* fehlt uns eine klare Richtung, wie die Digitalisierung gestaltet werden soll. Unser Kompass schlägt angesichts der großen Herausforderung erratisch in alle Richtungen aus. Schaffen wir es nicht, die digitale Transformation jetzt zu gestalten, verlieren wir in einem relativ kurzen Moment der Geschichte lang erkämpfte Grund- und Freiheitsrechte,[1] nicht nur national, sondern global, nicht nur einzeln, sondern als Gesellschaft, nicht nur digital, sondern allumfassend.

Geboten ist eine nach vorn orientierte Rückbesinnung auf eine Handlungs- und Gestaltungsfreiheit, um die digitale Transformation nach gesellschaftlichen Werten weiterentwickeln zu können. Wir müssen jetzt neue Technologien so entwickeln, dass sie soziale Ungleichheiten und Diskriminierung abbauen, die Menschenwürde fördern, Rechte wahren, sozial-ökologische Innovationen ermöglichen und die Umwelt schützen, also dem Gemeinwohl dienen. Es ist allerhöchste Zeit, den »Realitätsschock«[2] der digitalen Welt zu

1 Siehe auch den Beitrag von Ellen Ueberschär in diesem Band.

2 Lobo, Sascha: Realitätsschock. Zehn Lehren aus der Gegenwart, Köln: Kiepenheuer & Witsch 2019.

überwinden und Ideen für eine ganzheitlich wertegeleitete Digitalisierung zu entwickeln.

In diesem einführenden Beitrag machen wir gemeinsam einen kurzen Zwischenstopp auf der atemberaubenden Reise der Digitalisierung und nutzen ihn für Fragen. Was ist überhaupt diese Digitalisierung (1.1)? Wie sind wir von den libertären Anfängen des Netzes zu einer gesamtgesellschaftlichen Debatte über die Gestaltung der Digitalisierung gelangt (1.2)? Welche diskursiven Pole gibt es in der mit großem Handlungsdruck aufgeladenen Debatte (1.3)? Wie kommen wir vom laissez faire zum Primat der Werte und des Rechts (2)? Welche Regulierungsansätze gibt es (2.1)? Welche Angebote für eine Ethik der Digitalisierung bestehen bereits (3)? Wie kann eine Ethik der Digitalisierung als moralische Orientierungshilfe für die Gestaltung und Bewahrung der freiheitlich-demokratischen Gesellschaftsordnung in der digitalen Welt dienen? Wie kommen wir im Dreischritt von Freiheit über Verantwortung und Nachhaltigkeit zum Gemeinwohl (3.1-3.3)? Könnte das Konzept des Gemeinwohls uns Orientierung auf unserer Reise in die digitale Zukunft bieten (4)?

1.1 Digi-dies – Digi-das – Digi-was?

Mit unzähligen Definitionen wurde versucht, das Phänomen Digitalisierung greifbar zu machen. Die vielleicht schönste Annäherung lautet frei nach dem ersten Kranzberg'schen Technologiegesetz[3]: Digitalisierung ist weder gut noch schlecht; schon gar nicht ist sie neutral.

Nüchternere Ansätze betonen den technischen Kern, das Umwandeln von analogen Werten in digitale Formate, die digitale Repräsentation oder den Prozess »der darauf abzielt, eine Entität zu verbessern, indem er durch Kombination von Informations-, Computer-, Kommunikations- und Konnektivitätstechnologien signifikante Änderungen an ihren Eigenschaften auslöst«[4]. Diese Ansätze entsprechen damit dem englischen Begriff *digitization*.

Andere beschreiben den interaktiven Charakter der Digitalisierung als »die verbesserte Konnektivität und Vernetzung digitaler Technologien zur

3 Kranzberg, Melvin: »Technology and History, Kranzberg's Laws«, in: Technology and Culture, 27 (3), 1986, S. 544-560.

4 Vial, Gregory: »Understanding digital transformation: A review and a research agenda« 2019, S. 121., zitiert nach: Spraul, Katharina: Nachhaltigkeit und Digitalisierung. Wie digitale Innovationen zu den Sutainable Development Goals beitragen, Baden-Baden: Nomos 2019, S. 22.

Verbesserung der Kommunikation, von Dienstleistungen und des Handels zwischen Menschen, Organisationen und Dingen«[5]. Vermehrt beziehen sich Definitionen auf die Eigenschaft der Quantifizierbarkeit und die Fähigkeit der Datenverarbeitung, um beispielsweise ein »Gesamtbild des Wertes einer Person zu erstellen«.[6] Das kommt dem englischen *digitalization* nahe, die auf die Veränderung von Prozessen durch Digitalisierung abzielt.

Uns interessiert hier allerdings weniger der technische Kern als vielmehr die sozio-kulturelle Dimension des Phänomens. Die Digitalisierung wird nicht als ein gegebenes technisches Phänomen verstanden. Entsprechend geht es uns nicht um eine *Naturalisierung* des Wandels, sondern um die Zwecke, die mit neuen Technologien erreicht werden sollen, und damit auch immer um die Werte, die solchen Zielen zugrunde liegen. Das dieses Verständnis noch nicht etabliert ist, lässt sich auch leicht defätistisch zusammenfassen: »The real problem of humanity is the following: we have paleolitic emotions; medieval institutions; and god-like technology.«[7]

In der öffentlichen Debatte wird dazu passend von *digitalen Revolutionen, Disruptionen, Wandel-* oder *Transformationsprozessen* gesprochen, die weit über den bloßen technischen Fortschritt hinausweisen. Hier wird der Begriff der *Transformation* bevorzugt, da er einen gewollten und gerichteten Prozess meint, der auch die gesamtgesellschaftlichen Implikationen einschließt und beispielsweise nicht die Spontanität einer ungeplanten Revolution annimmt. Kurz: Die digitale Transformation passiert nicht einfach, wir schaffen und gestalten sie.

Die gesellschaftliche Wucht dieser Transformation hat der Kultur- und Medienwissenschaftler Felix Stalder auf die Formel der *Kultur der Digitalität*[8] gebracht. Sie »taucht als relationales Muster überall auf und verändert den Raum der Möglichkeiten« der »Konstitution und der Verknüpfung der unterschiedlichsten menschlichen und nichtmenschlichen Akteure«[9]. Im Mit-

5 Linkov et al.: »Governance Strategies for a Sustainable Digital World«, 2018, S. 1, zitiert nach: Spraul, Katharina: Nachhaltigkeit und Digitalisierung. Wie digitale Innovationen zu den Sutainable Development Goals beitragen, Baden-Baden: Nomos 2019, S. 22

6 Mau, Steffen: Das metrische Wir – Über die Quantifizierung des Sozialen, Berlin: Suhrkamp 2017, S. 9.

7 Wilson, Edward O. bei einer Debatte am 9. September 2009, zitiert nach: https://harvardmagazine.com/breaking-news/james-watson-edward-o-wilson-intellectual-entente

8 Stalder, Felix: Kultur der Digitalität, Berlin: Suhrkamp, 2016.

9 Ebd. S. 18

telpunkt steht also die Frage, wie umfassend unsere Gesellschaft durch diese Transformation geprägt wird, und weniger das Faszinosum Digitalisierung an sich. Entscheidend ist also gar nicht mehr die binäre Unterscheidung von analog versus digital, eins versus null, offline versus online oder alt versus neu. Der Soziologe Armin Nassehi geht einen Schritt weiter und beschreibt die Digitalisierung als »die dritte, vielleicht sogar endgültige Entdeckung der Gesellschaft«. »Wenn sie [die Digitalisierung] nicht zu dieser Gesellschaft passen würde, wäre sie nie entstanden oder längst wieder verschwunden«.[10] Die aktuelle Ausprägung der Digitalisierung verweist demzufolge auf gesellschaftliche Strukturen, die zu ihrer Entwicklung beigetragen haben. Es werden gleichermaßen die Thesen vertreten, dass »die gesellschaftliche Moderne immer schon digital war«[11], das Ende der Digitalisierung (wie wir sie kennen)[12] naht oder aber das »Zeitalter der Frühdigitalisierung«[13] begonnen hätte.

Es gibt unzählige Zugänge, mit denen wir die *Kultur der Digitalität*, die *Muster* und *Folgen* zu verstehen versuchen: Mal ist die Digitalisierung der direkte Auslöser für eine gesellschaftliche Veränderung, mal werden gesellschaftliche Konstitutionen vorausgesetzt und mal bedingen sie sich gegenseitig. Zunehmend setzt sich eine relationale Perspektive durch, wonach sich digitale Phänomene und gesellschaftliche Konstitutionen gegenseitig beeinflussen.[14] In der kurzen aber rasanten Geschichte des Netzes und der digitalen Welt gab es allerdings auch andere Zugänge.

10 Nassehi, Armin: Muster. Theorie der digitalen Gesellschaft, München: C.H. BECK 2019, S. 8.

11 Nassehi, Armin: Muster. Theorie der digitalen Gesellschaft, München: C.H. BECK 2019, S. 11.

12 Vgl. Dyson, George: Childhood's End, https://www.edge.org/conversation/george_dyson-childhoods-end

13 Oswald, Michael und Borucki, Isabelle: Demokratietheorie im Zeitalter der Frühdigitalisierung, Wiesbaden: Springer VS 2020.

14 Berg et al. schlagen mit der »digitalen Konstellation« eine politikwissenschaftliche Perspektive auf das Verhältnis technischer und gesellschaftlicher Entwicklungen vor. Berg, Sebastian; Rakowski, Niklas und Thiel, Thorsten: »Die digitale Konstellation. Eine Positionsbestimmung«, in: Zeitschrift für Politikwissenschaft.

1.2 Von den ultra-libertären Anfängen des Netzes zur horizontalen Regulierung des Digitalen

Wenn wir die heutigen Debatten zur Digitalisierung verstehen wollen, müssen wir zunächst nach dem Weg ins Jetzt fragen. Welche Positionssteine haben diese äußerst rasante Reise markiert? Die Digitalisierung beflügelt seit Langem[15] wissenschaftliche, politische und gesamtgesellschaftliche Debatten und füllt aktuell ganze Regalwände mit dramatischen Beschreibungen und visionären Erzählungen.

Dabei hat in den letzten Jahrzehnten eine diskursive Verschiebung stattgefunden. Das Internet, wie wir es heute kennen, war primär eine Geburt der (öffentlich finanzierten) Wissenschaft und privater Akteure, die sich selbst vorrangig technische Regeln gaben. Nach welchen Werten diese neue, faszinierende Welt auszurichten sei, wurde nur von einer sehr kleinen Gruppe technischer Pioniere in der *wilden Phase des frühen Internets* implizit mitgedacht.[16] Das Netz war noch weit von staatlicher oder gar suprastaatlicher Regulierung entfernt. Die Euphorie über das Tor zu einer neuen Welt dominierte. Der Tenor war: Die Logik der staatlichen Regulierung ist nicht kompatibel mit der emanzipatorischen, dezentralen, selbstverwalteten und dynamischen Kraft des Netzes.[17] Die frühen Pamphlete, Chartas und Unabhängigkeitserklärungen der 1990er Jahre waren von dem Anspruch geprägt, »Sozialutopien als Alternativkonstruktion gesellschaftlicher Ordnung«[18] zu schaffen. Ihre Autor*innen beanspruchten nichts weniger als die universelle Gültigkeit selbstgegebener Normen und Regeln in der virtuellen Welt.

Diese Haltung war essenziell für die emanzipatorische Kraft und die offene Entwicklung des Netzes. Was die Pioniere dabei übersahen, war die Fra-

15 Ein eindeutiger Geburtstermin ist kaum festzumachen. Es konkurrieren mehrere Geburtsmythen. Am prominentesten ist wohl der von der erste Netzwerkverbindung vor über 50 Jahren, gefolgt von der öffentlichen Zugänglichmachung des World Wide Webs vor über 30 Jahren. Siehe auch https://de.wikipedia.org/wiki/Geschichte_des_Internets

16 Ebd.

17 Exemplarisch sei hier auf die viel zitierte »A Declaration of the Independence of Cyberspace« von John Perry Barlow von 1996 zu verweisen: https://www.eff.org/de/cyberspace-independence

18 Dickel, Sascha: »Der neue Mensch – Ein (technik)utopisches Upgrade«, in: Aus Politik und Zeitgeschichte, 66. Jahrgang, 37-38/2016, 12. September 2016, Der neue Mensch: S. 85.

ge der *Verantwortung*.[19] Wer ist im Netz für was wann verantwortlich? Diese Frage löste ab den 2000er Jahren regelrechte Kulturkämpfe aus. Die Autonomiebewahrer auf der einen Seite sehen sich als technische und kulturelle Avantgarde. Auf der anderen Seite stehen staatliche Regulierungsinstanzen, die ihre Souveränität (zurück)gewinnen wollen, aber auch Wirtschaftszweige und Bürger*innen, die sich von den Umbrüchen überrumpelt fühlen. So wurden und werden beispielsweise harsche Auseinandersetzungen um ein modernisiertes Urheberrecht geführt. Als zentrales Gestaltungsrecht der digitalen Wissensgesellschaft soll es die Interessen zwischen Grundrechten wie Eigentumsfreiheit sowie Meinungs- und Informationsfreiheit ausgleichen. Dieser Konflikt entfachte immer wieder rund um Softwarepatente (2005) sowie internationale Handelsabkommen (ACTA 2012) und trieb 2018 europaweit Hunderttausende Menschen auf die Straßen, was für einen technisch-rechtlich komplexen Gegenstand beispiellos war.[20] Letztlich ebnete auch diese Debatte um den Interessensausgleich in der Wissensgesellschaft den Weg für das neue Feld der Netz- und Digitalpolitik. Nachdem das »*Neuland Internet*«[21] lange Zeit vernachlässigt worden war, wurde die Digitalpolitik (neben der Umwelt- und Klimapolitik) in den 2010er und 2020er Jahren zum Brennpunkt der Verhandlung unserer Zukunft. Sie ist in der politischen Mitte des Bundestags, der Bundesregierung und der europäischen Institutionen voll angekommen.[22]

Die Digitalpolitik ist dabei nur vordergründig eine technische Gegenstandspolitik. Sie setzt sich aus vielen Bereichen wie Medien-, Infrastruktur-,

19 Gemeinhin wird die Freistellung von der Verantwortung für durchgeleitete Inhalte Dritter durch Provider, also das sogenannte »Haftungsprivileg« in der E-Commerce-Richtlinie, als Erfolgsgarant für die freie Entwicklung des Internets betrachtet. Diese »heilige Kuh« muss sich angesichts des digitalen Wandels der Öffentlichkeit auch bewegen. Sie ist beispielsweise ein zentrales Element des horizontalen Regulierungsansatzes des Digital Services Act und vieler weiterer Gesetze.

20 Vgl. https ://www.sueddeutsche.de/digital/upload-filter-urheberrecht-demo-berlin-1.4380487

21 »Das Internet ist für uns alle Neuland.« Angela Merkel auf einer Pressekonferenz mit US-Präsident Barack Obama am 19. Juni 2013, https://de.wikiquote.org/wiki/Angela_Merkel

22 Eine eindeutige Geburtsstunde ist nicht auszumachen. Retrospektiv kommt die Einsetzung der Enquete-Kommission »Internet und digitale Gesellschaft« im deutschen Bundestag im Jahr 2010 einem Gründungsmythos in Deutschland am nächsten. Die Mitglieder der Kommission entwickelte ein Grundverständnis für das neue Politikfeld, das bis heute tief in Regierungskreise hineinwirkt.

Wirtschafts- oder Kulturpolitik zusammen. Sie bedient sich und ändert zahlreiche Rechtsgebiete und behandelt quasi jeden politischen Bereich: von Menschenrechten über Wirtschaft und Arbeit bis hin zur Transformation der Bildung und des Staats. Mit ihrer Hilfe werden neue technologische Phänomene entlang bestehender Werte gesellschaftspolitisch und ethisch bewertet und neu verhandelt. Die Politikwissenschaftlerin Jeanette Hofmann und ihre Kolleg*innen[23] fragen dementsprechend, was die konstitutiven Schutzgegenstände der Netz- beziehungsweise Digitalpolitik sind und kommen zu dem Schluss, dass diese noch diffus, nicht klar zuortbar und vor allem wenig institutionalisiert sind.[24]

Seit einigen Jahren wird vermehrt nach einer stärkeren Regulierung neuer Technologien gerufen, seien es Regeln für den Einsatz digitaler Technologien wie künstliche Intelligenz (KI) in allen Lebensbereichen, die Bändigung von Plattformmärkten oder die Einhegung einer überdrehten digitalen Medienöffentlichkeit, deren zersetzende Kräfte die deliberativen Demokratien gefährden.[25] Scheinbar kontraintuitiv rufen selbst global tätige Digitalunternehmen nach staatlicher Regulierung für existierende oder sich am Horizont abzeichnende Technologien.[26] Gefordert wird ein handlungsfähiger Staat, der

23 Zur Frage, ob es ein oder mehrere Schutzgüter der Netz- und Digitalpolitik gibt und welche das sein könnten, siehe Hösl, M.; Kniep, R: »Auf den Spuren eines Politikfeldes: Die Institutionalisierung von Internetpolitik in der Ministerialverwaltung«, Berlin Journal für Soziologie,29, 2019, S. 207-235, https://doi.org/10.1007/s11609-020-00397-4; Vortrag Jeanette Hofmann und Ronja Kniep: https://media.ccc.de/v/15np-2-wen_oder_was_schuetzt_die_netzpolitik_eine_retrospektive

24 Wenn nach Ansätzen der Digitalpolitik gesucht wird, muss auch die Frage gestellt werden: Wer entscheidet und wer regiert und wer kontrolliert den digitalen Raum? Diese Frage nach der Macht(um)verteilung im Netz und der Gestaltungsmacht in der digitalen Welt wurde vielfach bearbeitet und soll und kann hier nicht in der nötigen Tiefe verfolgt werden.

25 Siehe zu Letzterem auch den Beitrag von Christian Stöcker in diesem Band.

26 Exemplarisch: Musk, Elon: «Künstliche Intelligenz ist einer der wenigen Fälle, wo wir proaktiv statt reaktiv regulieren sollten. Denn wenn wir bei der Künstlichen Intelligenz erst reaktiv handeln, dann ist es zu spät.«, https://www.handelsblatt.com/unternehmen/it-medien/tesla-gruender-fordert-regulierung-risiko-fuer-die-menschheit-musk-warnt-vor-kuenstlicher-intelligenz/20069146.html?ticket=ST-6731104-NrChsKHMcK5d4bUccEjo-ap6; Brad Smith als Präsident von Microsoft: Facial recognition technology: The need for public regulation and corporate responsibility, https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/. Angesichts extrem komplexer

die Sicherheit der Bürger*innen und der Unternehmen auch in der digitalen Sphäre gewährleisten soll.

Angstvoll wird vor kognitiv überlegenen Maschinen (Singularität)[27] und damit verbundenen Souveränitätsverlusten gewarnt. Handlungsleitende Ethiken, aber auch eine eigenständige Ordnungspolitik für die digitale Sphäre, die sich an klassischen europäischen[28] und universellen Normen und Werten orientiert, sollen hier einen schützenden Rahmen bilden. Zu beobachten ist, dass der technikdeterministische Fortschrittsglaube des »Solutionism«[29] zunehmend daran scheitert, dass »die Moderne an sich selbst unsicher geworden«[30] ist. Unsere modernitätstypische Hoffnung, dass der Weg des Menschen durch Bereitstellung immer weiterer technischer Instrumente »zu immer glücklicheren Ufern führe«, ist »krisenhaft geworden«[31]. Aus dem innovationsgläubigen Heilsversprechen (»Das technisch Mögliche tun«) wird vermehrt das technikeinhegende Dogma (»Es kann nicht sein, was nicht sein darf«). Die Erzählung der Digitalisierung kleidet sich also in die unterschiedlichsten Gewänder.

1.3 Extreme Pole der zeitdiagnostischen Digitalnarrative

Die digitale Transformation weckt Fortschrittshoffnungen, aber auch Verlustängste. Mal erscheint sie als Förderer und Katalysator von individuellen Verwirklichungen und gesellschaftlichen Freiheiten, ein anderes Mal als Gefähr-

---

Digitalmärkte rufen insbesondere etablierte Marktakteure nach klaren Regeln, die Rechtssicherheit und damit zukunftsfeste Investitionssicherheit ermöglichen.

27 Mit dem Begriff wird ein möglicher Zeitpunkt beschrieben, ab dem künstliche Intelligenz die menschliche Intelligenz überflügelt und unabänderlich die Zukunft der Menschheit mitbestimmt. Der prominenteste Vertreter: Kurzweil, Ray: Menschheit 2.0. Die Singularität naht, Berlin: Lola Books 2013.

28 Siehe hierzu auch den Beitrag von Eric Hilgendorf zu den sieben Kernforderungen der Ethik-Leitlinien der Hochrangigen Expertengruppe Künstliche Intelligenz in diesem Band.

29 Morozov, Evgeny: To Save Everything, Click Here: The Folly of Technological Solutionism, New York City: PublicAffairs 2013

30 Küenzlen, Gottfried: »Der alte Traum vom neuen Menschen«, in: Aus Politik und Zeitgeschichte, 66. Jahrgang, 37-38/2016, 12. September 2016: Der neue Mensch, S.8.

31 Ebd.

der und Verletzer unserer Werte, Rechte und des gesellschaftlichen Zusammenhalts.[32]

Das Ergebnis ist eine eigentümliche Mischung aus enttäuschten Emanzipationserwartungen der frühen Netzkultur und -bewegung[33] und latenten Überwältigungsängsten vor kommenden digitalen Entwicklungen. Diese Ansichten pendeln sich bestenfalls zwischen diffuser Hoffnung und wabernder Skepsis ein, verharren aber oft an den entgegengesetzten Polen.[34] In Zeiten des Wandels demokratischer Öffentlichkeiten, in dem uns der *common ground* des Sag- und Diskutierbaren wegdriftet, treten diese Pole umso deutlicher hervor und wir treffen verstärkt auf separierte Lager.

All dies sind schwierige Vorzeichen für eine Debatte über moralische Grundprinzipien in der digitalen Welt. Westliche Gesellschaften stecken in *Wertekrisen*, da beachtliche Teile der Bevölkerungen bereit zu sein scheinen, als selbstverständlich erachtete Werte wie Freiheit und Gleichheit und deren rechtsstaatliche Garantie infrage zu stellen. An allen Ecken sind klagende Stimmen über eine grundsätzliche Erosion unserer Wertefundamente und Erschütterungen des Hauses der liberalen Demokratie zu vernehmen. Ein großer Teil hat mindestens eine digitale Komponente. Beispielsweise bestimmen private Plattformanbieter weitestgehend die Regeln der medialen Öffentlichkeit in Demokratien. Diese Polarisierung wird auch durch die Aufmerksamkeitsökonomie sozialer Netzwerke befördert, die die konstitutive Bedingung liberaler Demokratien unterläuft, nämlich den offenen öffentlichen Diskurs. Digitale Dienstanbieter verschieben lang erkämpfte Sozialstandards in der Arbeitswelt und fordern damit sozialstaatliche Ausgleichsmechanismen heraus. Datenbasierte und individualisierte Preise oder Versicherungen rütteln am kollektiven Solidarprinzip. Womöglich erleben wir gerade eine »Wiederauferstehung der Geschichte«[35], in der verschie-

32 Der Autor musste das größenwahnsinnige Vorhaben aufgeben, sämtliche deutschsprachige Diskussionsveranstaltungen der letzten Jahre zu zählen, die »Chancen und Risiken der Digitalisierung« im Titel tragen. Sie bleiben wohl auf immer unzählbar.

33 Exemplarisch: Lessig, Lawrence: Freie Kultur, Wesen und Zukunft der Kreativität, München: Open Source Press 2006; Shirky, Clay: Here Comes Everybody – The Power of Organizing Without Organizations, London: Penguin Group 2009.

34 Für einen kurzen und ähnlichen Überblick siehe auch: Bendiek, Annegret und Neyer, Jürgen: Smarte Resilienz. Wie Europas Werte in der Digitalisierung gestärkt werden können, Gütersloh: Bertelsmann Stiftung 2020, S. 15.

35 Gabriel, Markus: Moralischer Fortschritt in dunklen Zeiten – Universale Werte für das 21. Jahrhundert, München: Ullstein 2020, S. 9

dene Ideologien und Systeme konkurrieren. Im Systemwettbewerb stehen abwägendes und wertegebundenes Handeln unter Rechtfertigungsdruck, insbesondere, wenn es um schnelllebige digitale Technologien geht. In dieser angespannten Konstellation haben sich zwei extreme Pole im Digitaldiskurs etabliert.

Auf der leuchtend-utopischen Seite sehen wir eine Form von technikdeterministischem Fortschrittsglauben, der bereit ist, technologische Segnungen zu empfangen. Der leitende Gedanke hinter dieser *essenziellen Freiheit*[36] ist, dass das freiheitliche Wesen der Technik auch auf uns Menschen als Nutzer*innen übergeht, wenn wir es nur zulassen. In der Frühzeit der Netzkultur-Bewegung war die technikdeterministische Hoffnung, dass sich Demokratien wieder legitimieren und revitalisieren würden und zwar durch die algorithmische Festschreibung von Recht (»Code is law«[37]), die Aktivierung der »read-write-society«[38] und der souveränen »prosumer«[39] oder durch »mehr Transparenz wagen«[40]. In der »Transparenzgesellschaft«[41]. Der Glaube an das *Internet als Instrument der Freiheit* beflügelt nicht nur die Hoffnungen auf mehr Transparenz, sondern auch auf mehr und gerechter verteiltes Wissen, an dem im »infotopischen Idealfall alle partizipieren können«.[42]

Zeitgenössische Autor*innen folgen oft dem Topos, dass die Innovationspotenziale der »vierten industriellen Revolution«[43] für mehr Wohlstand freigesetzt werden müssten. Ansonsten drohe, der Anschluss wahlweise an Chi-

36 Für eine sehr gewinnbringende Systematik verschiedener Freiheitskonzepte in Relation zu Technologie siehe auch die Kategorisierung von Freiheit als Essenz, als Instrument, als Verfahren, als Entscheidungsfreiheit, als Aufklärung, als Autonomie und als Verantwortung in: Wagner, Benjamin: »Was Bedeutet ›Freiheit‹ in einem sozio-Technischen Kontext?«, in: Oswald, M. und Borucki, I., Demokratietheorie und Demokratie im Lichte des digitalen Wandels, Wiesbaden: Springer, S. 201-219.

37 Lessig, Lawrence: Code and Other Laws of Cyberspace, New York City: Basic Books 1999.

38 Lessig, Lawrence: Remix: Making Art and Commerce Thrive in the Hybrid Economy, https://archive.org/details/LawrenceLessigRemix2009

39 Toffler, Alvin: Die dritte Welle, Zukunftschance. Perspektiven für die Gesellschaft des 21. Jahrhunderts, München: Goldmann Verlag 1983.

40 Jarvis, Jeff: Mehr Transparenz wagen! Wie Facebook, Twitter & Co. die Welt erneuern, Berlin: Quadriga 2012.

41 Han, Byung-Chul: Transparenzgesellschaft, Berlin: Matthes und Seitz Berlin 2012.

42 Sunstein, Cass: Infotopia. Wie viele Köpfe Wissen produzieren, Frankfurt a.M.: Suhrkamp 2009.

43 Schwab, Klaus: Die Vierte Industrielle Revolution, München: Pantheon Verlag 2016.

na,[44] die USA[45] oder auch an Best Practices aus dem Baltikum oder an die skandinavischen Länder[46] verpasst zu werden. Um dies zu verhindern, müssten nun endlich, auch in ganz Europa die infrastrukturellen Bedingungen (von Breitbandinternet bis Whiteboards in Schulen) für digitale Innovationen geschaffen werden. Vor allem seien Barrieren für den freien Datenfluss[47] zu entfernen – wahlweise, um neue Sprünge in der medizinischen Forschung zu ermöglichen oder durch KI-basierte Effizienzgewinne endliche Ressourcen zu schonen. »Die Singularität naht«[48], in der uns überlegene KI zu besseren Menschen macht und neue Technologien ihre Befreiungspotenziale ausspielen können. Zumindest sollen scheinbar objektiv lernende und entscheidende Maschinen die Fehlbarkeit des Menschen und damit Ungerechtigkeiten überwinden. So zum Beispiel in der Justiz, bei der Auswahl von Bewerber*innen oder in der Bewertung von Schüler*innen oder Sportler*innen. Die Sozialutopie, dass uns Maschinen repetitive Tätigkeiten abnehmen würden, erlebt eine Renaissance.[49] Mit der Digitalisierung könnten beispielsweise Pflegekräfte den »Mensch[en] in den Mittelpunkt stellen«[50], da Pflegeroboter ihnen die körperlich anstrengenden abnehmen würden. Mit einer Dividendenabgabe auf die Produktivitätsgewinne durch Maschinen (»Robotersteuer«) könnte ein bedingungsloses Grundeinkommen finanziert werden.[51] Wir Menschen könnten uns dann höheren Formen der Selbstverwirklichung – individuellen Bestimmungen oder gleichermaßen sozialen Aufgaben – widmen.

---

44 Exemplarisch: Hobbs, Carla: Europe's digital sovereignty: from rulemaker to superpower in the age of US-China rivalry, https://ecfr.eu/archive/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf

45 Exemplarisch: Keese, Christoph: Silicon Valley: Was aus dem mächtigsten Tal der Welt auf uns zukommt, München: Albrecht Knaus Verlag 2014.

46 Exemplarisch: Digitalstrategien in Europa – Systematik, Erfolgsfaktoren und Gestaltungsräume digitaler Agenden, Gütersloh: Bertelsmann Stiftung 2020.

47 EU-Kommission: https://digital-strategy.ec.europa.eu/en/policies/non-personal-data

48 Kurzweil, Raymond: »The Singularity Is Near: When Humans Transcend Biology« (deutscher Titel: »Menschheit 2.0: Die Singularität naht«).

49 Vollautomatischer Kommunismus, https://www.zeit.de/kultur/2016-12/automatisierung-arbeitsgesellschaft-roboter-utopie-kommunismus/komplettansicht

50 Rede von Kardinal Reinhard Marx, Vorsitzender der Deutschen Bischofskonferenz am 7. Mai 2015: https://www.dbk.de/fileadmin/redaktion/diverse_downloads/presse_2015/2015-074a-40-Jahre-MDG-Rede-Kardinal-Marx.pdf; Volkens, Bettina und Anderson, Kai: Digital human: Der Mensch im Mittelpunkt der Digitalisierung, Frankfurt a.M.: Campus Verlag 2017.

51 Für ein Pro und Contra siehe: https://www.bpb.de/dialog/netzdebatte/253494/pro-und-contra-zur-robotersteuer

Auf der düster-dystopischen Seite wird vor der Zentralisierung von Datenmacht,[52] vor der Auflösung der Privatsphäre durch (Überwachungs-)Technologien,[53] sowie vor der totalitären Kraft der Ausbeutung im digitalen Überwachungskapitalismus[54] gewarnt. In einer nicht allzu fernen Zukunft drohe der Mensch von überlegener KI in die Unselbstständigkeit gedrängt zu werden, sodass die Formung der Evolution nicht mehr in Menschenhand liegen (Singularität)[55] wird. Angesichts einer »Übermacht im Netz«[56], einem die Gesellschaft komplett durchdringenden und formenden »Plattformkapitalismus«[57] drohe der Gesellschaft der demokratische Kollaps[58] und den Menschen »Digitale Demenz«[59]. Schlimmer noch, wir sind digitalen »Leviathanen«[60] ausgesetzt, die sich als »Monarchen von technologischen Gnaden«[61] sehen und alleine die Spielregeln bestimmen wollen.[62] Da wir die »dunkle Seite des Internets«[63] erblickt haben, stehen nichts weniger als die »digitale Technik und die Freiheit des Menschen«[64] auf dem Spiel. Der ehemals zivile

52 Vgl. Mayer-Schönberger, Viktor und Ramge, Thomas: Das Digital: Markt, Wertschöpfung und Gerechtigkeit im Datenkapitalismus, Düsseldorf: Econ Verlag 2017.

53 Exemplarisch: Rosenbach, Marcel und Stark, Holger: Der NSA-Komplex – Edward Snowden und der Weg in die totale Überwachung, München: DVA 2014.

54 Vgl. Zuboff, Shoshana: The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power, New York: PublicAffairs 2019.

55 Exemplarisch: Bostrom, Nick: Superintelligenz. Szenarien einer kommenden Revolution, Berlin: Suhrkamp 2014.

56 Brodnig, Ingrid: Übermacht im Netz – Warum wir für ein gerechtes Internet kämpfen müssen, Wien: Brandstätter Verlag 2019.

57 Lobo, Sascha: Auf dem Weg in die Dumpinghölle, https://www.spiegel.de/netzwelt/netzpolitik/sascha-lobo-sharing-economy-wie-bei-uber-ist-plattform-kapitalismus-a-989584.html

58 Hofstetter, Yvonne: Das Ende der Demokratie – Wie die künstliche Intelligenz die Politik übernimmt und uns entmündigt, München: Bertelsmann 2016.

59 Spitzer, Manfred: Digitale Demenz -Wie wir uns und unsere Kinder um den Verstand bringen, München: Droemer Knaur 2012.

60 Gegenhuber, Thomas: Eine Vision für das digitale Europa – Von der widerspenstigen Zähmung der Plattformen zu einem digitalen Humanismus, http://library.fes.de/pdf-files/fes/16146.pdf, S. 9ff.

61 Ebd.

62 Vgl. Nachtwey, Oliver: Der Geist des digitalen Kapitalismus: Solution und Techno-Religion, https://19.re-publica.com/de/session/geist-des-digitalen-kapitalismus-solution-techno-religion, 2019.

63 Morozov, Evgeny: The Net Delusion: The Dark Side of Internet Freedom, Philadelphia, PA: Perseus Book Group 2011.

64 Morozov, Evgeny: Smarte neue Welt. Digitale Technik und die Freiheit des Menschen, Blessing: München 2013.

Raum Internet hat sich in sein kriegerisches Gegenteil gewandelt, der »Gefahr aus dem Netz«[65]. Auch populärwissenschaftliche Autor*innen greifen den Topos auf und fordern »Internet abschalten – Das Digitale frisst uns auf«[66] oder »Das Internet muss weg – Eine Abrechnung«[67]. Denn die Heilsversprechen der frühen Netzbefürworter*innen hätten sich nicht bewahrheitet und auch hinsichtlich der individuellen Tugendethik hätten die Angebote der digitalen Dienste nur das Schlechteste des Menschen nach außen gekehrt.

Beide Extrempositionen können kaum handlungsleitend sein, denn sie erschweren einen gesellschaftlichen Konsens über die Gestaltung der digitalen Transformation. Nötig ist eine Fundierung der Diskussion entlang von Wertfragen: Welche individuellen und gesellschaftlichen Herausforderungen stellen sich und deuten sich am Horizont an? Wie schaffen wir es, die technologischen Neuerungen als gesellschaftliche Aufgabe zu begreifen, in der die Rechte und die Würde aller Menschen gewahrt bleiben? Welche Werte müssen wie mit der digitalen Transformation in Einklang gebracht werden, um das Gemeinwohl zu stärken? Wie richten wir unseren moralischen Kompass auf dieser Reise aus? Die Reflektion über einen Orientierung bietenden Wertekompass scheint dringlicher denn je. Das liegt auch an der vorherrschenden *normativen Kraft des Faktischen*, wie wir im Folgenden sehen werden.

2 Die faktische Kraft des Normativen und das Primat des Rechts

»Das Recht hinkt hinterher« zitierte *Der Spiegel* den als »Datenminister« titulierten Bundesinnenminister Gerhart Rudolf Baum, und das bereits im Jahr 1979. Baum forderte, dass »technische Entwicklungen im Bereich der Informationstechnologie […] in den Dienst der inneren Sicherheit gestellt werden«[68] müssten, sah aber das Recht noch nicht auf der Höhe der Zeit. Diese Ungleichzeitigkeit von voranschreitender Technologie und lahmendem Recht wurde und wird oft beklagt. Mittlerweile bewirkt die

65 Kurz, Constanz und Rieger, Frank: Cyberwar: Die Gefahr aus dem Netz. Wer uns bedroht und wie wir uns wehren können, München: Bertelsmann 2018.

66 Heidtmann, Jan: Internet abschalten – Das Digitale frisst uns auf, München: Süddeutsche 2019.

67 Silberstein, Schlecky: Das Internet muss weg – Eine Abrechnung, München: Knaus Taschenbuch 2018.

68 Der Spiegel, 26/1979, S. 39 https://magazin.spiegel.de/EpubDelivery/spiegel/pdf/40349447

technologische Beschleunigung gar eine »Veränderung der Zeitstrukturen in der Moderne«[69], sodass »unsere demokratischen Entscheidungsprozesse und Rechtsstaatlichkeitspraxis kaum mehr Schritt halten können mit der Geschwindigkeit und der Dimension«[70] des technologischen Fortschritts. Dementsprechend konnte durch die bisherigen Regulierungsversuche »keine funktionierende Ordnungsstruktur, geschweige denn Regierungsstruktur«[71] für die digitale Welt geschaffen werden.

Dieser defensiv ausgerichtete Kampf der Bastion der liberalen Demokratie gegen voranpreschende technologische Innovationen ist nicht nur beschwerlich und zermürbend. Er rüttelt auch am modernen Verständnis von gelingendem technologischem Fortschritt. Denn dieser Gedanke lebt von der Voraussetzung, wonach moralischer Fortschritt und das kodifizierende Recht mindestens Schritt halten müsse, wenn sie nicht sogar die primäre Bedingung für technologische Transformation ist. Bisher hat sich jedoch keine gesellschaftliche (Rechts-)Ordnung herausgebildet, mit der wir die digitale Transformation ganzheitlich gestalten können, anstatt mit »Reparatur-Ethiken«[72] den digitalen Fakten hinterherzulaufen. Im Gegenteil, wir erleben eine *Verantwortungsdiffusion*, in der sich nationale und supranationale Regulatoren erst an neue technologische Entwicklungen heranrobben, Unternehmensverantwortung in Wolken verschwindet, Hersteller Haftungen für Produkte untereinander herumreichen und Nutzer*innen in Unkenntnis in alle möglichen Datenverarbeitungen einwilligen (müssen). Wie in keinem anderem gesellschaftlichem Bereich erlauben wir, dass die gemeinwohlorientierte und rechtsstaatliche Steuerung so oft hinterher- und leerläuft. Das Primat des Rechts ist aktuell keins.

Wie können wir also (Grund-)Rechte in der digitalen Welt um- und durchsetzen und gleichzeitig Innovationspotenziale wahren? Angesichts der Geschwindigkeit, der Tiefe und der Reichweite der digitalen Transformation wird gefordert, dass das »Recht technologische Gestaltungsanforderungen

69 Rosa, Hartmut: Beschleunigung. Die Veränderung der Zeitstrukturen in der Moderne. Frankfurt a.M.: Suhrkamp 2005.

70 Mihr, Anja und Görisch, Sabrina: »Der Schutz der Grundrechte im Digitalen Zeitalter«, in: Hofmann et al., Politik in der digitalen Gesellschaft. Zentrale Problemfelder und Forschungsperspektiven, Bielefeld: transcript 2019, S. 206.

71 Ebd.

72 Vgl. Mittelstraß, Jürgen: Auf dem Wege zu einer Reparaturethik?, Tübingen: Attemto 1991.

formulieren und verfahrensmäßige Lösungen bereitstellen« müsse.[73] Wissenschaftliche und politische Debatten drehen sich darum, wie die »Relativierung des Rechts« und ein »unscharfes Recht«[74] in der digitalen Welt verhindert werden könnten und auf welcher Ebene dies erfolgen müsste. Braucht es einzelne, neue Rechtsvorschriften und Vertragsformen für digitale Phänomene oder gleich ein neues Ordnungsmodell für das Recht der digitalen Gesellschaft? Susanne Bär, Richterin am Bundesverfassungsgericht, fragte bereits vor über zehn Jahren, ob angesichts zunehmender Digitalisierung das »Grundgesetz ein Update benötigt«.[75] Die EU-Kommission wiederum verfolgt mit dem Digital Services Act[76] einen horizontalen Ansatz, mit dem unterschiedliche Gesetze miteinander verknüpft und harmonisiert werden sollen. Nicht zu unterschätzen ist die korrigierende Wirkung von europäischen Grundsatzurteilen,[77] die »inzwischen eine Normativität entfaltet [haben], die über den ursprünglichen Regelungszweck und Wirkungsraum an vielen Stellen hinaustreibt«[78].

Die Debatte hat sich also gründlich verschoben, von den anfangs beschriebenen Appellen in der frühen und wilden Phase des Internets hin zu konkreten und oft sehr komplexen Kodifizierungen von rechtlichen Regeln auf nationaler, supranationaler und völkerrechtlicher Ebene.[79] Kurz: Die Digita-

---

73 Schaar, Peter: Leitplanken für die digitale Gesellschaft in: Bär, Christian et al.: Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht, Wiesbaden: Springer Gabler 2018, S. 387

74 Boehme-Neßler, Volker: Unscharfes Recht. Überlegungen zur Relativierung des Rechts in der digitalisierten Gesellschaft, Berlin: Duncker & Humblot 2008.

75 Bär, Susanne: »Braucht das Grundgesetz ein Update? Demokratie im Internetzeitalter«, Blätter für deutsche und internationale Politik, 1/2011, S. 90-100.

76 Der DSA ist ein Legislativvorschlag der Europäischen Kommission, der dem Europäischen Parlament und dem Europäischen Rat am 15. Dezember 2020 vorgelegt wurde. Mit dem DSA sollen den Plattformbetreibern zahlreiche Sorgfaltspflichten auferlegt werden. Mehr: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_de

77 Beispielsweise: Urteil zu allgemeinen Überwachungs- und Filterverpflichtungen für Plattformbetreiber (unter anderem 2012 und 2018), Urteil zum Recht auf Vergessen im Internet (2014), Vorratsdatenspeicherung (u.a. 2010 und 2020), Urteil zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (2008).

78 Becker, Carlos und Seubert, Sandra: »Die Stärkung europäischer Grundrechte im digitalen Zeitalter«, , in: Hofmann et al.: Politik in der digitalen Gesellschaft. Zentrale Problemfelder und Forschungsperspektiven, Bielefeld: transcript 2019, S. 226.

79 Siehe auch den Beitrag von Matthias C. Kettemann in diesem Band

lisierung wird zunehmend (rechtlich) genormt. Wie kann denn nun die normative Kraft von Werten faktisch durchgesetzt werden? Es scheint ein Methodenmix[80] angezeigt, um Werte und individuelle Rechte in den unterschiedlichen Sphären der digitalen Welt durchzusetzen.

Regelungsansätze in der digitalen Sphäre

Bei den Voraussetzungen für die Durchsetzung von Recht ist zunächst an den Schutz der Grundrechte zu denken. Da diese Freiheits- und Abwehrrechte des Einzelnen in der digitalen Welt leicht durch Dritte bedroht werden können, greift zusätzlich eine zweite staatliche Schutzpflicht. Diese wird besonders intensiv entlang zweier wegweisender Urteile des Bundesverfassungsgerichts diskutiert.[81] Zum einen leitete das oberste Gericht 1983 das *informationelle Recht auf Selbstbestimmung* direkt von den Menschenrechten ab und formulierte damit den Persönlichkeitsschutz als weiterentwickeltes Grundrecht im digitalen Zeitalter. Zum anderen wurde 2008 das *Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* etabliert. Nicht erst die rechtskonforme Verarbeitung von (personenbezogenen) Daten, schon die Sicherheit der genutzten digitalen Geräte muss (staatlich) garantiert werden. Es gibt also eine Schutzpflicht des Staates gegenüber den Bürger*innen. Diese Grund- und Freiheitsrechte werden zunehmend in zahlreichen Formen kodifiziert, etwa im Grundgesetz, in der europäischen Grundrechtecharta, in Dutzenden internationalen Verträgen und im Völkerrecht.[82]

Vermehrt wird auch eine stärkere Grundrechtsbindung für die Akteur*innen gefordert, die uns die digitale Welt durch ihre Dienste und Plattformen vermitteln.[83] Dabei geht es nicht mehr nur um die staatlichen Einschränkungen oder Gewährleistungen von Grundrechten. Oftmals missachten interna-

80 Zur Frage der Governance auf der Mikroebene siehe den Beitrag von Stefan Heumann in diesem Band.

81 Siehe auch den Beitrag von Ulf Buermeyer und Malte Spitz in diesem Band.

82 Vgl. Kettemann, Matthias C.: Die Weltordnung des Digitalen, https://zeitschrift-vereinte-nationen.de/fileadmin/publications/PDFs/Zeitschrift_VN/VN_2019/Heft_5_2019/02_Ketteman_Heft_VN_5-2019_1-10-2019_web.pdf

83 Ausgangspunkt ist das Urteil des Bundesverfassungsgerichts zu »Fraport« von 2011 in dem die Grundrechtsbindung privater Unternehmen ausdrücklich betont wurde: https://www.rechtsprechung-im-internet.de/jportal/portal/t/18fq/page/bsjrsprod.psml?doc.hl=1&doc.id=KVRE392231101&documentnumber=2&numberofresults=2&doctyp=juris-r&showdoccase=1&doc.part=L&paramfromHL=true#focuspoint

tional tätige Digitalunternehmen geltendes Recht, indem sie beispielsweise den Schutz der Privatsphäre umgehen. Besonders komplex wird es, wenn mit der Nutzung digitaler Werkzeuge die Hoffnung einhergeht, automatisiert (Grund-)Rechte durchzusetzen. Denn dabei können gleichzeitig andere Rechte eingeschränkt werden. Besonders schwierig wird es, wenn diese sensible und komplexe Rechtsgüterabwägung auch noch an private Akteur*innen delegiert wird. Das Paradebeispiel sind hier automatisierte Entscheidungssysteme in Form von Inhaltsfiltern. Erhoffen sich die einen die effektive Durchsetzung der grundrechtlich geschützten Eigentumsrechte (GG Artikel 14), befürchten andere die Einschränkung der ebenfalls grundrechtlich geschützten Informations- und Meinungsfreiheit (GG Artikel 5).[84] Im Kern zeigt sich hier der klassische Konflikt zwischen einem liberal-individualistischen absoluten Freiheitsschutz und einer kommunitären Abwägung von Individual- und Gemeinschaftsinteressen. So wird beispielsweise bei der Frage der Autonomie Privatheit nicht mehr als individualistisches »right to be alone« verstanden. Es dominiert ein »soziales Privatheitsverständnis«[85], das eine Rechtsgüterabwägung und die technische Realität dezentraler Netzwerke berücksichtigt und Privatheit als zwingende Vorbedingung für soziale und damit gesellschaftliche Freiheit einfordert. Hier wird bereits deutlich, wie komplex es geworden ist, Freiheitsrechte zu wahren und in Einklang mit anderen Rechten zu bringen, und wie dringend diese gesetzlich abgesichert werden müssen.

Die bisher skizzierten Ansätze zielen primär auf den ethischen Umgang mit den Effekten der Digitalisierung. Beispielsweise werden Regeln formuliert, wie mit Ergebnissen von automatisierten Entscheidungen umgegangen oder durch (Nicht-)Einsatzgebiete verhindert werden sollen.[86] Ein *nicht-judikativer,* dafür *normativ-präskriptiver Ansatz* entfaltet seine Wirkung bereits bei der Entwicklung von digitalen Produkten und Dienstleistungen. Mit den po-

84 Ob sogenannte Uploadfilter diese Rechtsgüterabwägung ausreichend abbilden können war und ist auch der Hauptstreitpunkt bei der europäischen Urheberrechtsreform beziehungsweise dem Artikel 13 (heute Artikel 17).

85 Becker, Carlos und Seubert, Sandra: Die Stärkung europäischer Grundrechte im digitalen Zeitalter, 2019, S. 233

86 Exemplarisch: Gundlach, Julia und Müller-Eiselt, Ralh: »Mit künstlicher Intelligenz zum Kitaplatz«, in: Die Zeit, https://www.zeit.de/2021/06/kuenstliche-intelligenz-kita-anwendung-regulierung-gesellschaft-technologie?utm_referrer=https%3A%2F%2Fwww.google.com%2F

pulärer werdenden Methoden *Values in Design* oder *Ethics by Design*[87] sollen potenzielle ethische Konflikte frühzeitig erkannt, Wertentscheidungen direkt in technische Artefakte eingeschrieben und so Diskriminierung verhindert werden. Verstöße gegen Recht oder gesellschaftliche Normen werden technisch unterbunden, um damit das große Ziel aufgeklärter Gesellschaften, die Autonomie ihrer Mitglieder, zu erreichen.[88] Diese Ingenieurs- und Design-Perspektive beeinflusst etwa ethische Überlegungen darüber, wie die Kontrolle automatisierter Entscheidungssysteme ausgestaltet werden sollte. Ziel ist eine frühzeitige Implementierung ethischer Überlegungen in digitale Systeme, also bereits bei der Entwicklung, und ein partizipatives Vorgehen, das unterschiedliche Perspektiven und Bedürfnisse (Stakeholder) einbindet. Besonders intensiv und öffentlichkeitswirksam wird das am Beispiel von (teil)autonomen Fahrassistenten diskutiert. Ihnen müssen ethische Entscheidungsparameter einprogrammiert werden, die festlegen wer in einer Notsituation verletzt oder gar getötet wird. Automatische Entscheidungssysteme sollen also die *Freiheit als Autonomie*[89] sichern. Der Glaube an diese selbststeuernde positive Freiheit durch moralische Einsicht ist allerdings schwer ramponiert. Angesichts der markt- und handlungsbeherrschenden privater Anbieter und die dominierenden Allgemeinen Geschäftsbedingungen ist die Hoffnung, diese schwierigen Fragen an privat organisierte Systeme abzugeben, bei einigen zerstört: »Ethische Prinzipien können und sollen die Technologieentwicklung positiv beeinflussen, Ethik lässt sich aber nicht an Technik delegieren.«[90]

Neben gesetzlicher Regulierung und technischer Implementierung finden sich freilich auch andere Regelungsansätze. Forscher*innen der Universität Zürich kamen Anfang 2019 auf nicht weniger als 84 ethische Richtlinien, die einen gestalterischen Anspruch hegen.[91] Zu Recht wird daher mittlerweile

87 Einführend: Manders-Huits, Noëmi: »What values in design? The challenge of incorporating moral values into design« Science and Engineering Ethics, 17(2), 2011, S. 271-87.

88 Siehe auch den Beitrag von Timo Rademacher und Erik Schilling in diesem Band.

89 Vgl. Wagner, Ben: »Was bedeutet ›Freiheit‹ in einem sozio-technischem Kontext?«, 2020, S. 208ff.

90 Datenethikkommission der Bundesregierung: Gutachten der Datenethikkommission, S. 74. https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf?__blob=publicationFile&v=2

91 Jobin, Anna; Ienca, Marcelo und Vayena, Effy: »The global landscape of AI ethics guidelines«, Nature Machine Intelligence 1, 2019, S. 389-399 ,https://doi.org/10.1038/s42256-019-0088-2

vor einem *Ethics-Washing* gewarnt.[92] Diese Vorbehalte beziehen sich in erster Linie auf die Ethikinitiativen, Ethikbeiräte und Codes of Conduct privater Akteur*innen, in denen Ethik funktional mit Selbstregulierung gleichgesetzt wird, die harte staatliche Regulierung überflüssig machen möchte. Doch es genügt nicht mehr, solch komplexe Vorgänge mit individueller Verantwortungsethik, kollektiv mahnenden Chartas oder Regulierung vorbauenden unternehmerischen Selbstverpflichtungen rahmen zu wollen. So können kaum noch entscheidende Impulse für die hochdynamische Entwicklung der Digitalisierung gegeben werden. Einen anderen und durchaus vielversprechenden Weg gehen Initiativen, die ethische Prinzipien konkret operationalisieren, in dem diese Leitlinien in Form von Auditierungen, Zertifizierungen und für Siegel genormt werden und so Positivanreize zur wertegeleiteten Gestaltung neuer Technologien setzen wollen.[93]

Die Rufe von Unternehmen nach Rechtsicherheit gebender Regulierung, die Umtriebigkeit der Gesetzgeber auf europäischer, nationaler, sowie auf Länderebene und die aktiver werdenden Aufsichts- und Regulierungsbehörden zeigen deutlich, dass die Zeichen der Zeit auf eine eigenständige *Ordnungspolitik für die digitale Sphäre* und das *Primats des Rechts* stehen. Auf politischer Ebene hat sich diese Dringlichkeit vor allem in Form des Konzepts der *digitalen Souveränität* manifestiert, die in der Logik eines Systemwettbewerbs[94] gedacht wird.[95] Dieses Dekaden überspannende Maßnahmenpaket eines ganzen Kontinents umfasst gesetzliche Regelungen, das Setzen technischer Standards, die Förderung strategisch wichtiger Technologien und vieles

92 Vgl. Bietti, Elettra: »From ethics washing to ethics bashing: a view on tech ethics from within moral philosophy«, in: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, FAT* ›20 (New York, NY: Association for Computing Machinery, 2020) S.210-219; Metzinger, Thomas: »Ethics washing made in Europe«, in: Der Tagesspiegel (8.04.2019), https://www.tagesspiegel.de/politik/eu-guidelines-ethics-washing-made-in-europe/24195496.html

93 So zum Beispiel der interessante Ansatz von Bertelsmann Stiftung (Hg.): From Principles to Practice – An interdisciplinary framework to operationalise AI ethics, Gütersloh: Bertelsmann Stiftung 2020.

94 Siehe hierzu auch den Beitrag von Tyson Barker in diesem Band.

95 Zum Begriff der digitalen Souveränität siehe den Beitrag von Julia Pohle und Thorsten Thiel in diesem Band. Zur Priorität der EU-Kommission 2019-2024 siehe »Ein Europa für das digitale Zeitalter«, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_deund »Europas digitale Dekade: ein digital gestärktes Europa bis 2030«, 09.03.2021, https://ec.europa.eu/commission/presscorner/detail/de/ip_21_983

mehr. Es zielt neben einer staatlichen Souveränität bei der Gestaltung technologischer Neuerungen auch auf eine individuelle Souveränität zur Wahrung der Selbstbestimmung.[96]

Diese Bemühungen zeigen, dass es für das Selbstverständnis eines demokratischen Rechtsstaats und des Gesetzgebers zunehmend nicht mehr hinnehmbar ist, dass *Fakten schaffen* vor *Recht schaffen* gilt. Die Kernfrage lautet daher:

Wie können wir die normative Kraft des Faktischen der Digitalisierung aller Lebensbereiche in eine faktische Kraft des Normativen zur Gestaltung der Digitalisierung umkehren?

3 Digitale Ethiken

Wenn wir die digitale Transformation als gesellschaftlichen Fortschritt gestalten, erkämpfte Werte in der digitalen Gesellschaft verteidigen, weiterentwickeln, durchsetzen und als produktive Kraft nutzen wollen, müssen wir zunächst über unsere Werte und die zu verfolgenden normativen Ziele reflektieren. Für einen konzeptionellen Fortschritt bedarf es also eines kleinen Zwischenschritts, der die Reflexion über die eigenen Wertziele ermöglicht. Dieses Intermezzo erlaubt uns Fragen zu stellen wie: Welche Werte machen uns als freiheitliche Gesellschaft aus und wie lassen sich dieses auf technologische Innovationen in der digitalen Welt übertragen? Welche systemischen Herausforderungen gibt es für die hoheitlichen Sphären von Recht, Demokratie und Menschenrechte? Welche erkämpften und verinnerlichten Werte stel-

96 Bendiek und Neyer wählen hierfür den erfolgsversprechenden Ansatz der Smarten Resilienz der eine europäische Digitalsouveränität fordert, die sich an der strukturellen Dynamik und Lernfähigkeit offener Gesellschaften und der regulativen Einhegung neuer Technologien entlang europäischer Werte orientiert. Smarte Resilienz. Wie Europas Werte in der Digitalisierung gestärkt werden können. Vgl. Neyer, Bendiek: Smarte Resilienz. Wie Europas Werte in der Digitalisierung gestärkt werden können,2020, S. 37.

len wir angesichts der digitalen Verlockungen zur Disposition (Technologie-Paradox)?[97]

Die gute Nachricht ist: Noch können wir neue Technologien so ausrichten, dass sie unseren gesellschaftlichen Werten entsprechen. Die Fähigkeit, sich stets eine neue Zukunft auszudenken, ist bereits Ausdruck von Freiheit. Die Digitalisierung birgt genau dieses schöpferische Potenzial, Fortschritt im gesellschaftlichen Zusammenleben zu projizieren und als leitend für unser Handeln zu bestimmen, denn Technologie ist schließlich auch eine Art zu denken und zu handeln.[98] Einen legitimierenden Anker können normative Philosophie und Ethik bilden, die zu allen Zeiten den Menschen halfen, sich bei großen Zukunftsfragen zu orientieren.[99] Dafür müssen wir beantworten, welche Werte konstituierend sein sollen und wie wir die Digitalisierung gestalten können und wollen. Wir müssen uns darüber verständigen, wie wir über Werte wie *Freiheit, Verantwortung, Nachhaltigkeit* und *Gemeinwohl* im digitalen Zeitalter denken. Das Wertverständnis dient also keinem Selbstzweck, sondern als moralische Orientierungshilfe für eine regulative Gestaltung freiheitlich-demokratisch-rechtsstaatlicher Gesellschaftsordnungen in der digitalen Welt.

Die Frage nach dem Verhältnis von Mensch und Technik bewegt zahlreiche neue wissenschaftliche Einrichtungen.[100] In den letzten Jahren hat sich in Deutschland ein ganzer Zweig der *Digital Humanities* (digitale Geisteswissenschaften) und der digitalen Ethik etabliert.[101] Auch populärwissenschaft-

97 Das Technologie-Paradox besagt, dass die Gewinnung neuer Freiheiten und Möglichkeiten durch Technik untrennbar mit Anpassungsleistungen an Technik erkauft wird. Vgl.: Grunwald, Armin: Der unterlegene Mensch. Die Zukunft der Menschheit im Angesicht von Algorithmen, Robotern und Künstlicher Intelligenz, München: RIVA-Verlag 2019.

98 In einem sehr bescheidenen Maßstab soll hier also der habermaschen Idee des Selbst- und Weltverständnisses gefolgt werden. »die Philosophie nach wie vor ihrer Aufgabe nachgehen [sollte], im Licht der verfügbaren wissenschaftlichen Erkenntnisse ein begründetes Selbst- und Weltverständnis zu artikulieren« Habermas, Jürgen: Nachmetaphysisches Denken II, Berlin: Suhrkamp 2012.

99 Als einer der Begründer einer Informations- oder Digitalethik kann Rafael Capuro gelten. Für einen Überblick siehe: Capuro, Rafael: Homo Digitalis: Beiträge zur Ontologie, Anthropologie und Ethik der digitalen Technik, Wiesbaden: Springer VS 2017.

100 Vgl. Jakobi, Tobias; Breindl, Yana und Busch, Andreas: Einleitung S. 6ff, in: Jakobi, Tobias; Breindl, Yana und Busch, Andreas: Netzpolitik. Ein einführender Überblick, Wiesbaden: Springer VS 2019, S. 17-51.

101 Für einen breiten Überblick über die Entwicklung und den Stand der sozialwissenschaftlichen Forschung zu Internet und Digitalisierung siehe: Hofmann, Jeanette et

liche Bestseller zeigen, dass das Thema in der gesellschaftlichen Mitte angekommen ist.[102] Da die Effekte der Digitalisierung nicht nur auf Individuen, sondern systemisch auf die gesamte Gesellschaft wirken, ist es nur konsequent, dass die »Digitalethik den Kreis ihrer Adressaten sehr weit«[103] zieht. Angesprochen werden nämlich sämtliche Nutzer*innen, also wir alle.

Im Zentrum steht die Frage, wie wir die zunehmende Digitalisierung sämtlicher Lebensbereiche zum (Gemein-)Wohle aller gestalten können und welche Parameter wir hierfür anlegen sollten. Die Digitalethik kann sich an etablierten ethischen Konzepten orientieren. Breiter Konsens ist die uneingeschränkte Menschenwürde als Fixpunkt einer anthropozentrischen Rechts- und Gesellschaftsordnung, die auch das Fundament des deutschen Grundgesetzes bildet. Welche Werte darüber hinaus handlungsleitend sein sollten, ist freilich umstritten. Hinzu kommt die Komplexität steigernde Schwierigkeit, dass von dem Regelungsgegenstand selbst eine Dynamik ausgeht, auf die Gestaltende und Regulierende fortwährend eingehen müssen. Werte in der digitalen Welt müssen sich gleichermaßen an universell gültigen Prinzipien orientieren und an durch Digitalisierung ausgelösten neuen Phänomenen. Wir müssen uns beispielsweise fragen, wie sich unser Verständnis von Diskriminierungsfreiheit verändert,[104] wenn klassische Regulierungsinstrumente auf algorithmische und automatisierte Entscheidungssysteme treffen, die sich fortwährend selber weiterentwickeln und deren Entscheidungsfindung und Ergebnisse für Menschen kaum transparent, nachvollziehbar und geschweige denn erklärbar sind. Die Macht des Faktischen von neuen Technologien schafft also selbst Zustände und Normen, an denen sich Wertkonzeptionen und Recht abarbeiten müssen. Sonst besteht die Gefahr, dass sich latente Gegebenheiten verstetigen und starre Wertkonzeptionen und verstaubtes Recht leerlaufen.

---

al.: Politik in der digitalen Gesellschaft. Zentrale Problemfelder und Forschungsperspektiven, Bielefeld: transcript 2019.

102 Exemplarisch: Harari, Yuval Noah: Homo Deus – Eine Geschichte von Morgen, München: C.H. Beck 2017; Precht, Richard David: Jäger, Hirten, Kritiker. Eine Utopie für die digitale Gesellschaft, München: Goldmann 2018.

103 Wischmeyer, Thomas und Herzog, Eva: Digitale Ethik in der Demokratie – Zur Rolle von Ethik-Kommissionen in der Digitalpolitik, in: Juristen Zeitung (JZ) 74(14), 2019, S. 696-701 (6).

104 Siehe hierzu auch den Beitrag von Lorena Jaume-Palasí und der Frage der Geschlechtergerechtigkeit den Beitrag von Francesca Schmidt und Nicole Shephard in diesem Band.

Angesichts der verschwimmenden Grenze zwischen Mensch und Maschine (Stichwort: Quantified Self und Cyborgs) wackelt auch immer mehr der rechtliche Dualismus aus Rechtssubjekt, also Menschen, die Rechte und Pflichten genießen, und Objekten, die dies nicht tun. Unser Verständnis von Verantwortlichkeit wird damit vor große Herausforderungen gestellt. Das zeigt sich auch am Herumreichen von ökonomisch relevanter Haftungsverantwortung zwischen Zulieferern, Herstellern, Vertreibenden und Nutzer*innen, (Stichwort Verantwortungsdiffusion) an der beispielsweise bis heute Rechtsrahmen für autonomes Fahren im Straßenverkehr scheitern.

Wollen wir abstrakte, offene und normative Konzepte wie *Freiheit, Verantwortung* oder *Nachhaltigkeit* als Legitimation für eine ganzheitliche Gestaltung der Digitalisierung heranziehen, müssen wir diese Konzepte ausleuchten. Dabei ist zu beachten, dass der digital-ethische Diskurs jung und fluide ist und noch zahlreiche blinde Flecken hat. Monolithische Ideologien und Großtheorien wie Deontologie, Utilitarismus oder Tugend- und Verantwortungsethiken haben sich noch nicht fest etabliert.

3.1 Vom Libertarismus zur Freiheit als Autonomie[105]

Wenn normative Konzepte als Gestaltungsmaximen in Stellung gebracht werden sollen, müssen wir damit beginnen, uns über den Wert der Freiheit zu verständigen. Überwunden scheint in großen Teilen der libertäre Ansatz der kalifornischen Ideologie.[106] Frühe Gründer*innen, Entwickler*innen und Nutzer*innen setzten ihre Individualrechte absolut. Das heißt, die eigene Freiheit wurde nicht durch die Wahrung der Freiheit anderer begrenzt. Dieser unbeschränkte Anspruch galt auch gegenüber dem Staat, der höchstens als Dienstleister verstanden wurde. Dieses Freiheitsverständnis schwingt in einigen heutigen Debatten nach, ist aber deutlich abgemildert.

Digitale *Freiheit* wird meist als die Möglichkeit freier individueller und kollektiver Selbstverwirklichung im Netz und in der digitalen Welt verstanden. Sie hat sowohl eine positive als auch eine negative Dimension. Positiv werden die größeren selbstverwirklichenden Entwicklungsmöglichkeiten

105 Einen Überblick über alle Werte und Wertverständnisse kann an dieser Stelle nicht geleistet werden. Hier sollen lediglich einzelne Aspekte hervorgehoben werden. Für einen Überblick über unterschiedliche Wertkonzeptionen siehe den Beitrag von Petra Grimm in diesem Band.

106 Vgl. Daub, Adrian: Was das Valley Denken nennt – Über die Ideologie der Tech-Branche, Berlin: Suhrkamp 2020.

durch digitale Technologien gesehen. Negativ dagegen die potenzielle Einschränkung von Freiheit durch private oder staatliche Kontrolle und die Überwachung durch digitale Technologien. Dabei erleben wir in der gesellschaftlichen Verhandlung von Freiheit in der digitalen Welt ein *Technologie-Paradox*. Viele Nutzer*innen digitaler Dienste sind bereit, mehr staatliche und private Kontrollen und Überwachungen (negative Freiheit) gegen größere Entfaltungsmöglichkeiten oder zumindest komfortablere Dienste (positive Freiheit) einzutauschen. Freiheit wird also zunehmend zu einer individuell und nicht gesellschaftlich interpretierten Größe.

Inwieweit unter diesen Umständen und bei dieser Form von individueller Freiheit von einer tatsächlichen *Autonomie* gesprochen werden kann, ist zumindest diskussionswürdig. Insbesondere an der Idee der *Autonomie* wird deutlich, wie die Digitalisierung wesensverändernd auf den selbstbestimmten Menschen einwirkt[107] und damit Werte infrage stellt, die in Deutschland und Europa in Grundrechte mit Verfassungsrang gegossen sind. Vor allem der Schutz der *Privatsphäre* in Form von Datenschutz wurde und wird viel und hitzig diskutiert.[108] Es wurde bereits das »Post-Privacy«-Zeitalter[109] ausgerufen, in dem überkommene Schutzinstrumente aufzugeben seien. Der Mensch wird nicht mehr als freies, individuelles und selbstbestimmtes Wesen betrachtet, sondern primär als ein Datenträger, der sich geradezu sozialkonstruktivistisch algorithmisch optimieren lassen sollte. In dieser Logik müssen Grundrechte nicht vor der autoritären oder totalitären Kraft neuer Technologien geschützt oder zumindest das Wechselverhältnis austariert werden. Im Gegenteil, Selbstbestimmung müsse nicht rechtlich geschützt werden, sondern könne erst technisch assistiert hergestellt werden. Ob damit in der Menschenwürde wurzelnde Freiheitsrechte eingeschränkt werden, ist in dieser Logik gar nicht mehr die richtige Frage.

---

107 Siehe hierzu auch den Beitrag von Christiane Woopen und Sebastian Müller in diesem Band.

108 Besonders verdichtet zeigte sich das einerseits bei der Einführung der europäischen Datenschutzgrundverordnung im Mai 2018 und an der 2020 öffentlich geführten Debatte um die deutsche Corona-Warn-App. Sollte sie zentral, geschlossen und möglichst viele Funktionen nutzend gestaltet werden oder sollten die Daten dezentral gespeichert, der verwendete Code durch Offenlegung nachvollziehbar und eine Abwägung der epidemiologischen Ziele mit der informationellen Selbstbestimmung erfolgen?

109 Exemplarisch: Heller, Christian: Post-Privacy – Prima leben ohne Privatsphäre, München: C.H. Beck 2011.

Der scheinbar natürliche Gegenspieler zu Freiheit, Autonomie und Privatheit ist Sicherheit. Ob Freiheit eine Vorbedingung für Sicherheit ist, oder umgekehrt, ist auch in der digitalen Welt eine Standardsituation der Wertekollision und Zielkonflikte, und kann auch hier nicht abschließend beantwortet werden. Unabhängig davon, ob es gewinnbringend ist, die beiden Werte als Antagonismen gegeneinander laufen zu lassen, lässt sich aber festhalten, dass das Konzept der Sicherheit in der digitalen Welt eine neue Bedeutung erlangt. Die technologischen Möglichkeiten von Überwachung und Kontrolle sowie die gestiegene globale Verflechtung haben zu einem spiegelbildlich wachsenden Bedürfnis nach Sicherheit geführt. Einerseits hat sich die Wahrung der inneren Sicherheit in der digitalen Welt ausdifferenziert. Quasi jede digitale Neuerung wird auf neue Straftatbestände oder Überwachungsmöglichkeiten abgeklopft. Andererseits ist zur Schutzverantwortung auch die Wahrung der Sicherheit digitaler Infrastrukturen hinzugekommen (Stichwort »informationelle Selbstbestimmung« und »Integrität informationstechnischer Systeme«). Der Wert der staatlich garantierten Sicherheit erhält mit der Etablierung des Frames der *digitalen Souveränität* derzeit ein digitales Upgrade.

3.2 Von der Freiheit zur Verantwortung

Wie oben beschrieben, wurde oft diagnostiziert, dass Ethik als bloße *Reparaturethik* der technischen Entwicklung ohnmächtig hinterherlaufe. Die Lösung kann allerdings nicht darin liegen, eine individualisierte Verantwortungsethik (Freiheit als Autonomie) zu proklamieren, die das Heil im ethisch richtigen Handeln sucht. Das überantwortet die Bewältigung disruptiver Strukturveränderungen jedem Einzelnen und wäre in letzter Konsequenz das Gegenteil von liberaler Freiheit. Vielmehr müssen wir ethische Konzepte entwickeln, mit denen auf die Bedingungen der Digitalisierung gewirkt werden kann, ohne die Verantwortung auf die Tugendhaftigkeit Einzelner abzuwälzen.

Kritisch ist die Frage, wo die verantwortungsvolle Grenze der Freiheit verläuft, sowohl für individuelle Nutzer*innen, als auch für private Diensteanbieter oder staatliche Akteure. *Freiheit als Verantwortung* kann nicht darauf reduziert werden, dass »für sich selbst verantwortlich zu sein, eine befreiende Komponente haben kann, wodurch der Einzelne aufgrund der von ihm selbst

auferlegten Einschränkungen erst frei sein kann«[110]. Oder lebenspraktischer formuliert: Nicht nur die Selbstbeschränkung durch einzelne Nutzer*innen, sondern die Einsicht aller staatlichen, unternehmerischen und sonstigen Akteur*innen, dass nicht alles technisch Mögliche auch technisch umgesetzt werden sollte, beschreibt eine ethisch fundierte Freiheit, die verantwortungsbewusst ist und damit nachhaltig sein kann.

Zur Wahrung der gesellschaftlichen Freiheiten wird also eine *prozedurale Freiheit* benötigt, die zuverlässige Mechanismen zur Entscheidungsfindung und Weiterentwicklung des Schutzes von Rechten beiträgt. Erst wenn die prozedurale Freiheit abgesichert ist, lässt sich die *faktische Kraft des Normativen* in Form von Recht durchsetzen. Im Sinne von John Rawls[111] liegt die Herausforderung von Verantwortung und Rechenschaftslegung maßgeblich in der Verteilung zwischen und der fairen Partizipation von Akteur*innen. Demokratische Strukturen müssen so geschaffen sein, dass sie die staatlichen und zivilgesellschaftlichen Akteur*innen einbinden,[112] um dialogisch einen digitalen Gesellschaftsvertrag mit Sanktionsmöglichkeiten zu etablieren. So kann ein Konzept von *Freiheit als Verfahren* und *Freiheit als Verantwortung* begründet werden.[113] Beispielsweise ermöglicht erst die Komplexität und Verfahrenstiefe der europäischen Datenschutz-Grundverordnung, *Freiheit als Autonomie* in Form von Privatsphäre durchzusetzen. Ob dies immer und reibungslos gelingt und das Instrumentarium ausgereizt ist, steht auf einem anderen Blatt.[114]

Angesichts der oben skizzierten Eingriffstiefe und Diffusionsgeschwindigkeit moderner Technikentwicklungen ist es unverantwortlich zu warten, bis solch negative Entwicklungen eingetreten sind, dass sie unübersehbar Schaden anrichten und Gegenmaßnahmen notwendig werden. Stattdessen besteht eine Verpflichtung, mit einer vorausschauenden und problemorientierten Ethik konstruktiv zur Gestaltung beizutragen.

Mit der Suche nach normativ-präskriptiven Rechtfertigungslogiken für die Gestaltung der Digitalisierung, die auf abstrakten europäischen oder universellen Werten beruhen, erleben wir aktuell eine Renaissance des Vorsor-

110 Wagner, Ben: »Was bedeutet ›Freiheit‹ in einem sozio-technischen Kontext?«, 2020, S. 21.

111 Vgl. Rawls, John: Eine Theorie der Gerechtigkeit, Frankfurt a.M.: Suhrkamp 1979.

112 Siehe hierzu auch den Beitrag von Julia Kloiber und Elisa Lindinger in diesem Band.

113 Siehe Wagner, Ben: »Was bedeutet ›Freiheit‹ in einem sozio-technischem Kontext?«, 2020.

114 Siehe hierzu auch den Beitrag von Nils Leopold in diesem Band.

geprinzips nach Hans Jonas. Im bereits 1979 erschienenen Werk *Das Prinzip Verantwortung*[115] entwickelte Jonas eine »Ethik für die technologische Zivilisation«, die im Kern das operationalisierbare Vorsorge- und Nachhaltigkeitsprinzip etablierte. Potenziell negative Wirkungen von zukünftigen disruptiven Technologien müssten bereits im Hier und Jetzt regulativ eingehegt werden. Aus dem Portfolio der verantwortlichen Gestaltung von Technik und Innovation hat sich in Deutschland die Technikfolgenabschätzung am stärksten durchgesetzt. Sie wurde beispielsweise in Form eines parlamentarischen Technikfolgenabschätzungsbüros organisatorisch fest in der Politikberatung verankert.[116] Zahlreiche weitere Ansätze werden aktuell diskutiert und ausprobiert, wie zum Beispiel die partizipative Technikfolgenabschätzung, die Bürger*innen in die Gestaltung einbezieht, das Value Sensitive Design oder Ethics by Design[117] oder der Ansatz der Responsible Research and Innovation[118] in der europäischen Forschungs- und Technologiepolitik. Viele dieser Ansätze folgen dem Prinzip Verantwortung von Hans Jonas. Auch hier folgen wir der Idee einer *Freiheit als Verantwortung*.

3.3 Von der Verantwortung zur Nachhaltigkeit

Die Frage nach der Zuschreibung von Verantwortung öffnet die Perspektive für das Konzept der *Nachhaltigkeit* und dessen Integration in die digitale Welt. Unsere ethischen Debatten sind allgemein so fortgeschritten, dass wir zur Beantwortung moralischer Fragen auch die Dimensionen mitdenken können, die über das räumliche und zeitliche Nahfeld hinausreichen. Universelle Werte müssen genau diesem Anspruch allgemeiner Gültigkeit auch für folgende Generationen gerecht werden.

Bislang wurde Nachhaltigkeit im Digitalisierungsdiskurs überwiegend mit Blick auf die ökologische Analyse einzelner digitaler Phänomene disku-

115 Jonas, Hans: Das Prinzip Verantwortung – Versuch einer Ethik für die technologische Zivilisation, Frankfurt a.M.: Insel-Verlag 1979.

116 Grunwald, Armin: Technikfolgenabschätzung – Eine Einführung. Zweite, grundlegend überarbeitete erweiterte Auflage, Berlin: edition sigma 2010.

117 van den Hoven, Jereon et al.: Handbook of Ethics, Values, and Technological Design, Wiesbaden: Springer 2015.

118 Lindner, Ralf: Responsible Research and Innovation als Ansatz für die Forschungs-, Technologie- und Innovationspolitik –Hintergründe und Entwicklungen, 2016, https://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Hintergrundpapier-hp022.pdf

tiert. Das Konzept muss aber zum ganzheitlichen und damit auch sozialen Leitmotiv für die Gestaltung der digitalen Welt weiterentwickelt werden. Der Informatiker Peter Reichl und der Soziologe Harald Welzer plädieren dafür, die Digitalisierung weder binär (Ablehnung oder Zustimmung) noch segmentär (eben nicht ganzheitlich) zu betrachten, sondern immer im Zusammenhang mit Nachhaltigkeit.[119]

Womöglich müssen wir als digitale Gesellschaft erst all die Erkenntnisschritte nachholen, die die moderne Umweltbewegung bereits vor über 50 Jahren vollzogen hat. Wir stehen womöglich am Beginn einer Epoche, in der verstanden wird, dass wir die digitale Umwelt selbst schaffen und beeinflussen. Nachhaltigkeitsfragen können dann zu einer gesamtgesellschaftlich akzeptierten Notwendigkeit und politischen Größe aufsteigen. Wir müssen den Nachhaltigkeitsbegriff breiter, sozialer und nicht nur ökologisch denken. Denn Nachhaltigkeit meint nicht nur die ressourceneffiziente Gestaltung digitaler Anwendungen, sie bedeutet eine breite, wertebasierte Gestaltung, mit der Bedingungen für die Entfaltungsmöglichkeiten künftiger Generationen geschaffen werden.[120] Konzeptionell muss mit ihr beispielsweise auch gefragt werden, ob heutige Designentscheidungen oder die Nutzung geschlossener (proprietärer Standards Innovationen und damit künftige (Weiter-)Entwicklung erschweren. Oder ob eine auf fortwährende Eskalation ausgelegte digitale Aufmerksamkeitsökonomie in dem Sinne nicht nachhaltig, als sie selbst die Axt an die Wurzel offener und demokratischer Öffentlichkeit legt. Digitale Nachhaltigkeit ist also nicht lediglich konservativ (bewahrend) und ökologisch (ressourcenschonend), sondern progressiv (ermöglichend) ausgerichtet.

Der Ausgangspunkt aller Werteüberlegungen im digitalen Zeitalter muss also sein, die im doppelten Sinne weitreichenden Folgen digitaler Phänomene zu berücksichtigen. Sie wirken einerseits in die Tiefe, beispielsweise indem automatisierte Entscheidungen konkret die soziale Teilhabe von Menschen beeinflussen. Und sie wirken in der Weite, da heute getroffene Entscheidungen mittel- und langfristige Folgen für die digitale (Um-)Welt haben. Eine so

119 Vgl. Reichl, Peter und Welzer, Harald: »Achilles und die digitale Schildkröte – Thesen zu einer Digitalen Ökologie«, in: Hengstschläger, Markus (Hg.), Digitaler Wandel und Ethik – Rat für Forschung und Technologieentwicklung, Wals bei Salzburg: Ecowin 2020.

120 Zur Frage wie ein ökologisch, sozial und ökonomisch verstandener Nachhaltigkeitsbegriff für Fragen der Gerechtigkeit in der digitalen Welt fruchtbar gemacht werden kann siehe den Beitrag von Tilman Santarius in diesem Band.

verstandene digitale Nachhaltigkeit umfasst eine reflektierte und konstruktive Gestaltung von digitaler Realität, um neue Entwicklungschancen in einer noch digitaleren Zukunft zu eröffnen. Diese weitreichenden Auswirkungen verlangen eine progressive und aktive Politik der digitalen Risikofolgenabschätzung von Veränderungen in Gesellschaft und Technologie. Allerdings ist diese Perspektive angesichts der Geschwindigkeit der digitalen Transformation schwierig und vor allem weitestgehend ungeübt. Deshalb wird hier für den Mut zu einer ganzheitlichen Perspektive plädiert, um adäquat auf die vielen glitzernden und blinkenden Digitalisierungsphänomene einzugehen. Dabei können (so antiquiert anmutende) Konzepte wie *Verantwortung*, *Nachhaltigkeit* und *Gemeinwohl* eine konstruktive Rolle für die progressive Gestaltung der Digitalisierung spielen.

Letztlich hat eine verantwortungsvolle und nachhaltige Perspektive das Gemeinwohl zum Ziel – und zwar das Wohl heutiger und künftiger Generationen. Insofern kann Gemeinwohl als Kompass für eine konstruktive und progressive Gestaltung der Digitalisierung dienen.

4 Gemeinwohl als Kompass für die Gestaltung der Digitalisierung

Gemeinwohl ist zunächst ein Aggregatsbegriff. Das Konzept kann je nach normativer Deutung viele Formen und Zustände annehmen, mit denen sich sowohl »allgemeine Probleme als auch typische Muster der Problembearbeitung moderner Gesellschaften«[121] beschreiben lassen. Erst durch die Beantwortung der Frage, was gerecht ist, kann das normative Konstrukt für Gesellschaften ausgedeutet werden (Gemeinwohl ist also nicht, es wird).

Die Idee des Gemeinwohls knüpft an die Tradition kommunitaristischer Demokratietheorien an. Demnach muss sich eine Gemeinschaft über geteilte Werte und ethische Grundüberzeugungen verständigen. Es muss *einen Geist des Vertrauens* geben, der mit akzeptierten Verfahren des Interessenausgleichs einhergeht. Grundlage dafür ist ein freier und fairer Prozess der (staatlichen) Willensbildung unter Einbeziehung aller Interessensgruppen,[122] wobei die-

121 Neidhardt, Friedhelm: »Zur Einführung: Fragen zum Gemeinwohl«, in Schuppert, Gunnar Folke und Neidhardt, Friedhelm, Gemeinwohl – Auf der Suche nach Substanz, Berlin: Edition Sigma 2002, S. 13.

122 Meier und Blum nennen dies »demokratischen Kognitivismus«: Meier, Dominik und Blum, Christian: »Macht und Gemeinwohl«, in: Gesellschaft · Wirtschaft · Politik (GWP) 68(3), 2019, S. 391-399.

ser zunächst unbestimmt und offen verläuft.[123] Gemeinwohl ist also immer nur der provisorische Ertrag eines »ergebnisoffenen gesellschaftlichen Ringens von Interessen um Einfluss«[124]. Gemeinwohl ist daher Prozess und Ergebnis zugleich, muss immer weiterentwickelt und immer wieder akzeptiert werden. Gemeinwohl ist also kein fixer Wert, dem sich alle gesellschaftlichen Realitäten zu beugen hätten. Der Wert steht immer in Bezug zum zeitlichen und gesellschaftlichen Kontext, also ob eine Verantwortung unmittelbar, mittel- oder langfristig begründet wird. Wenn politisches Handeln einem Teil der Gesellschaft größeren Nutzen bringt, als es anderen abgezogen wird, gibt es eine Annäherung an ein größeres Gemeinwohl. Die Verbesserung ist aber nur relational, der größere Nutzen kann nur abhängig von den normativen Maßstäben bewertet werden, die als wünschenswert gelten.

Angesichts des disruptiven Charakters der digitalen Transformation gilt umso mehr, dass der gesellschaftliche Konsens zum Gemeinwohl nur temporär gefunden werden kann. Daher soll hier auch keine monolithische Beschreibung des Gemeinwohls in der digitalen Welt eingemeißelt werden.

Wenn wir Gemeinwohl als Grundlage politisch-regulativen Handelns betrachten, beziehen wir uns auf Werte, die uns als Gesellschaft ausmachen. Das deutsche Recht kennt bereits ein verfassungsstaatliches Gemeinwohlverständnis, »das sich an den Gemeinwohlwerten des Grundgesetzes wie Menschenwürde, Freiheit, Rechtssicherheit, Frieden und Wohlstand und damit an den Grundrechten, dem Rechtsstaat-, Sozialstaats- und Demokratieprinzip festmachen lässt«.[125] Für eine wertegeleitete Gestaltung der Digitalisierung ist daher eine Gemeinwohlbindung interessant, da diese als Kompass für andere Werte wie Freiheit, Gerechtigkeit oder Demokratie dienen kann, die sich an diesem Maßstab orientieren. Mehr noch: Eine Gemeinwohlbindung kann als zentrales Legitimationsprinzip von Macht und Gestaltungsanspruch in der digitalen Welt dienen. Oder noch steiler: Wer nicht versucht, geteilte Werte unter einem normativen Dach wie dem Gemeinwohl in der digitalen Welt durchzusetzen, wird dem großen gesellschaftlichen Anspruch, die technologische Transformation zu gestalten, nicht gerecht. Am steilsten:

123 Meier und Blum verstehen darunter »Demokratischer Pluralismus […] Das Wohl des Gemeinwesens kann niemals unabhängig von den unterschiedlichen Präferenzen, Wertvorstellungen und Überzeugungen der Bürger gedacht werden.« Ebd.

124 Ebd.

125 Vgl. von Arnim, Hans Herbert: Gemeinwohl und Gruppeninteressen, Frankfurt a.M: Alfred Metzner 1977, S. 22ff.

Wer diesen Versuch gar unterlässt, droht auf lange Sicht durch Technologie objektiviert zu werden, also zum unsouveränen Gegenstand disruptiver Transformationen zu werden und keine Legitimation mehr zu erfahren.

Es gibt bereits zahlreiche Versuche, dies zu vermeiden. Das zeigt sich beispielsweise an der breit geführten Diskussion um die Datenmacht von Plattformbetreibern, seien es Arbeits- und Wohnungsvermittler oder soziale Netzwerke. Nationale und der europäische Gesetzgeber sehen sich immer mehr genötigt, diese Dienste gesellschaftlich einzuhegen und ihre Verantwortung für das Gemeinwohl einzufordern. Dabei greifen sie instrumentell zu (1) gesetzlicher Regulierung, (2) Förderung gemeinwohlorientierter Alternativen oder zum (3) Aufbau eigener Ökosysteme. Ein paar Beispiele aus dem Bereich der digitalen Plattformen sollen dies erläutern:

Auf europäischer Ebene wird aktuell gleich mehrfach versucht, eine (1) Rechtsstaatsbindung der Plattformanbieter herzustellen. Der Digital Services Act (DSA) soll als horizontaler Ordnungs- und Kontrollrahmen für Plattformen dienen, der harmonisierte Vorschriften, Vorabverpflichtungen, bessere Beaufsichtigung und Durchsetzung von Sanktionen umfasst. Die Sorgfaltspflichten und Haftungsrisiken nehmen entsprechend der Größe und den gesellschaftlichen Auswirkungen der Dienste zu. Es gab wohl noch nie einen nationalen oder supranationalen Ansatz, der so breit und weitgehend versucht eine gerechtere Netzwelt zu schaffen und so der Logik der Internetkonzerne per *rule of law* eine gemeinwohlorientierte Gestaltung der digitalen Welt entgegenzustellen. Das Projekt *GAIA-X*[126] geht (rechts-)technisch einen Schritt weiter, indem es einen Rechtsrahmen für die Vernetzung von digitalen (Cloud-)Diensten und schließlich ein europäisches digitales Ökosystem schafft. Daneben gibt es noch eine sehr offensichtliche Gemeinwohlbindung digitaler Plattformen, die »Digitalsteuer«. Das ist allerdings keine konzeptionelle Herausforderung für eine bessere Gesellschaft, sondern schlicht eine Frage des machtpolitischen Willens und der handwerklichen Um- und Durchsetzung der Beteiligung von digitalen Diensteanbieter am Gemeinwohl an den Orten, wo sie auch ihre Umsätze und Gewinne generieren.

Um die gigantische Menge an Daten für das Gemeinwohl nutzbar zu machen, werden vermehrt (2) Intermediäre im öffentlichen Auftrag, sogenannte

126 https://www.bmwi.de/Redaktion/DE/Dossier/gaia-x.html

Datentreuhänder,[127] diskutiert. Ein Modell sieht vor, dass Daten privater oder öffentlicher Stellen von einer neutralen Instanz anonymisiert zur Verfügung gestellt werden, um dann beispielsweise gemeinwohldienliche medizinische Forschung zu ermöglichen. Entweder per freiwilliger Datenspende oder vertraglich geregelt werden Daten von Nutzer*innen in einen Datenpool eingespeist, aus dem per algorithmischer Verfahren neue Erkenntnisse und Innovationen, beispielsweise im Gesundheitswesen, abgeleitet werden können. Einseitige Abhängigkeiten von wenigen Plattformbetreibern sollen durch verschiedene Alternativkonzepte überwunden werden, beispielsweise öffentlich finanzierte Plattformen, die nicht dem Diktat des Shareholder Value, sondern einer Gemeinwohlbindung folgen.[128] Die Idee des Teilens in der plattformbasierten *Sharing Economy* soll durch einen *Plattform-Kooperativismus*[129] wiederbelebt werden. In plattformbasierten Genossenschaften sehen die Befürworter eine (nicht alles in Wert setzende) Alternative, die zwar ähnliche Infrastrukturen und Angebotsmodelle wie die kommerzielle Plattformökonomie nutzt, jedoch andere Ziele verfolgt und beispielsweise gesellschaftliche Mitbestimmung explizit ermöglichen möchte. Andere Vorhaben planen komplett alternative Plattformökosysteme (3), die bereits in ihren technischen Ausgestaltungen europäischen Werten wie Transparenz, Offenheit und Schutz der Privatsphäre folgen.[130] Gemein ist allen drei Ebenen, dass Vertreter*innen von Gemeinwohlzielen betonen, dass nicht defensive Ablehnung von digitalen Realitäten, sondern die aktive Beteiligung von und Mitgestaltung durch unterschiedliche Akteur*innen nötig ist.

Die Debatte um Gemeinwohl in der digitalen Welt reicht allerdings schon deutlich weiter zurück. Seit Beginn der Entwicklung des Internets, insbeson-

127 Die Idee der Datentreuhänder wird beispielsweise von der EU-Kommission im Data Governance Act vorgeschlagen. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act

128 Exemplarisch: Hillje, Johannes: Plattform Europa – Warum wir schlecht über die EU reden und wie wir den Nationalismus mit einem neuen digitalen Netzwerk überwinden können., Bonn: Dietz, J.H. 2019. Siehe auch den Beitrag von Philipp Staab und Dominik Piétron in diesem Band.

129 Grundlegend: Scholz, Trebor und Schneider, Nathan: Ours to Hack and to Own – The Rise of Platform Cooperativism, A New Vision for The Future of Work and a fairer Internet, New York City: OR Books 2017.

130 Vgl. Kagermann, Henning und Wilhelm, Ulrich: European Public Sphere – Gestaltung der digitalen Souveränität Europas, München: acatech IMPULS 2020, S. 6.

dere nachdem es in den 1990er Jahren öffentlich zugänglich wurde,[131] wird diskutiert, ob die digitale Infrastruktur als ein öffentliches Kollektivgut behandelt werden und der Zugang zum Internet ein Menschenrecht sein sollte.[132] Diese Frage wird immer drängender, da die technische Seite des Netzes und der Digitalisierung nicht mehr von der funktionalen zu trennen ist. Es gibt faktisch kein Offline-Leben mehr. Hier wird die oben erwähnte (auch digitale) Gemeinwohlbindung der Grundrechte beispielhaft durch das Recht, sich aus »allgemein zugänglichen Quellen informieren zu können« (GG Artikel 5, Absatz 1), deutlich.

Als ein früher Vorläufer der digitalen Gemeinwohlbindung kann die *Openness-* und *Commons-Bewegung* gelten. Unter *Openness* lassen sich viele Formen der Zugänglich- und Transparentmachung von Ressourcen für die digitale Welt zusammenfassen.[133] Viele dieser Bewegungen sind allerdings einem *instrumentellen und individuellen Freiheitsverständnis* verhaftet, wonach alle zum Gemeinwohl beitragen können, wenn nur alle offene Tools und offene Lizenzen verwenden. Am weitesten etabliert sind *Open-Source-Software* und kulturelle Gemeingüter.[134] Die Idee, offen lizenzierte Artefakte allgemein zur Verfügung zu stellen, hält langsam, aber zunehmend Einzug in das Recht (Stichwort: Urheberrecht) und IT-Großprojekte (Stichwort: *Corona-Warn-App*).

Der gesellschaftliche Mehrwert einer offenen Software, frei benutzbarer Kulturgüter oder offen zugänglicher Daten ist schnell ersichtlich, werden dadurch doch (vor allem zivilgesellschaftliche) Innovationen erleichtert. Anbieter proprietärer digitaler Dienste oder Inhaber ausschließlicher Eigentumsrechte sehen das freilich anders, da ihnen ein Teil ihres Geschäftsmodells durch die Aufhebung der Exklusivität verloren geht. Wie oben beschrieben, kann der schiere Vorteil einer gesellschaftlichen Gruppe keine hinreichende Bedingung für das Gemeinwohl einer Gesellschaft sein. Gleichwohl können

131 Zur Entwicklung und Veröffentlichung des World Wide Webs durch Sir Tim Berners-Lee siehe: https://home.cern/science/computing/birth-web

132 Die UNO-Vollversammlung sprach sich 2016 für ein Menschenrecht auf Internet aus »The promotion, protection and enjoyment of human rights on the Internet«, https://undocs.org/A/HRC/32/L.20

133 Unter der Openness-Bewegung lassen sich unter anderem Themen fassen wie Open Source (Quelleoffene Software), Open Science (Kollaborative Wissenschaft mit offenen Daten und Werken), Open Data (freie Nutzung insbesondere öffentlich finanzierter oder generierter Daten), Open Access (freier Zugang zu wissenschaftlicher Literatur) und Open Education (freier Zugang zu Lehrmaterialeien).

134 Grundlegend: Grassmuck, Volker: Freie Software – Zwischen Privat- und Gemeineigentum, Bonn: Bundeszentrale für politische Bildung 2002.

Kollektivziele wie gemeinwohldienliche Innovationen eine relative Einhegung absoluter Rechte legitimieren.

Das Ziel des Gemeinwohls kann für verschiedene Formen von Gesellschaften gelten. Traditionell zielt eine Gemeinwohlbindung auf nationalstaatlich umschriebene Gesellschaften ab, die sogenannten »imagined communities«[135]. Mit den zunehmenden gesellschaftlichen Zersplitterungen und Individualisierungen, die durch die Digitalisierung vorangetrieben werden, werden aber auch viele »virtual communities of practices«[136] im Netz, seien es Kanäle auf sozialen Netzwerken, die globale gaming communities oder Gig-Worker-Vereinigungen, relevant. Beide Gesellschaftsformen können sich dem Gemeinwohl verschreiben. Da hier auf eine prozedurale Durchsetzung von normativen Zielen durch das Primat des Rechts abgehoben wird (*Freiheit als Verfahren* und *Freiheit als Verantwortung*), wird hier primär die erste Form der Gesellschaft herangezogen. Gleichzeitig muss berücksichtigt werden, dass der Rechtsstaat einer »imagined community« das gesellschaftliche Bekenntnis zu einer gemeinwohlorientierten Gestaltung der digitalen Welt nicht erzwingen kann. Er kann lediglich die Bedingungen für einen gütlichen Aushandlungsprozess herstellen. Die Freiwilligkeit des Bekenntnisses zum entwickelten Gemeinwohl ist eine konstitutive Bedingung.

Der demokratische Rechtsstaat muss also mit allen Akteur*innen ein institutionelles Gefüge entwickeln und anbieten, in dem Argumente ausgetauscht, Entscheidungen getroffen und tatsächlich durchgesetzt werden können. Gemeinwohlbindung in der Gestaltung der digitalen Transformation kann nur hergestellt werden, wenn die grundrechtlich verankerte Gemeinwohlbindung allen staatlichen Handelns auch auf neue digitale Phänomene übertragen und dabei ein gerechter Interessenausgleich versucht wird. Diese Herausforderung markiert die »Gelenkstelle zwischen Macht und Gemeinwohl«[137], wenn die Förderung, der Schutz und der Erhalt des Gemeinwohls als zentrale Legitimationsprinzipien von Macht gelten sollen.

Angesichts des großen Gestaltungsdrucks der digitalen Transformation brauchen wir Mut zu einer holistischen Perspektive. Dazu müssen wir gleichermaßen die Extreme der technikdeterministischen Heilsversprechen und

135 Anderson, Benedict: Imagined Communities: Reflections on the Origin and Spread of Nationalism, London: Verso 1983.

136 Lave, Jean und Wenger, Étienne: Situated Learning: Legitimate Peripheral Participation, Cambridge: Cambridge University Press, 1991. Bezogen auf Online-Communities: Stalder, Felix: Kultur der Digitalität. 2016., S. 144ff.

137 Meier, Dominik und Blum, Christian: Macht und Gemeinwohl. 2019, S. 397.

des maschinenstürmenden Skeptizismus überwinden. Um der faktischen Kraft des Normativen und dem Primat des Rechts in der digitalen Welt Kraft und Geltung zu verleihen, müssen wir uns einer wertegeleiteten Gestaltung der Digitalisierung verschreiben. Unsere Suche nach handlungsleitenden Werten führt uns von der individuellen Freiheit über die gesellschaftliche Verantwortung und der progressiven Nachhaltigkeit für kommende Generationen bis zum menschenzentrierten Gemeinwohl. Dieses Gemeinwohl ist es, was uns als Maßstab zur ganzheitlichen und zukunftsorientierten Gestaltung der digitalen Welt dient. Gemeinwohl ist unser Kompass.

1.2 Werte: Was können ethische Ansätze für eine werteorientierte Digitalisierung leisten?
Analyse, Systematisierung und Einordnung

Petra Grimm

1 Problemaufriss – in welchen Zusammenhängen stellen sich Wertefragen?

Wer Digitalisierung und einen der Antriebsmotoren – die künstliche Intelligenz (KI) – nur als *technisches* Gesamtprojekt auffasst, missversteht die Bedeutung dieses Prozesses für jede beziehungsweise jeden von uns und die Gesellschaft insgesamt. Denn mit der Digitalisierung ändern sich unsere Bedingungen für ein gutes Leben, unser Denken und unsere Gefühle in einer sehr umfassenden Weise. Das betrifft sowohl das Privatleben als auch das Arbeitsleben. Wie erleben die Bürger*innen diese Veränderungen? In einer Studie[1] zu den Werten, Ängsten und Hoffnungen in der digitalen Alltagswelt zeigt sich, dass die Digitalisierung in beruflich-professionellen Kontexten übergreifend eher positiv wahrgenommen und bewertet wird. Sie wird als Segen, wenn nicht gar als Glück, von den Befragten beschrieben, wobei damit ökonomisch geprägte Werte wie Nützlichkeit, Effizienz und Effektivität gemeint sind. Im Kontext der privaten Lebenswelt wird die Digitalisierung dagegen eher kritisch – zumindest aber differenzierter – gesehen. Es werden Wertekonflikte und teils sogar Werteverluste, wie zum Beispiel der Ehrlichkeit, Zuverlässigkeit und Privatheit, benannt, vor allem in Bezug auf die sozial-kommunikativen Praktiken bei der Nutzung sozialer Internetplattformen und Kommunikationsdienste. Eine *Ethik der Digitalisierung* muss die

1 Grimm, Petra/Müller, Michael/Trost, Kai Erik: Werte, Ängste, Hoffnungen. Das Erleben der Digitalisierung in der erzählten Alltagswelt, Baden-Baden: Nomos (i. Ersch.).

Sichtweisen der Bürger*innen wie auch aller anderen Beteiligten (in Wissenschaft, Wirtschaft, Politik etc.) berücksichtigen. Gleichwohl ist die eigentliche Aufgabe einer Ethik der Digitalisierung, ethisches Handeln und Wertefragen zu reflektieren sowie normative Standards zu begründen. Hierzu muss sie auch die Bedingungen und Strukturen der digitalen Systeme sowie die damit zusammenhängenden sozialen, politischen, ökonomischen und rechtlichen Vorgaben in den Blick nehmen.

Der vorliegende Beitrag soll den Horizont für eine werteorientierte Digitalisierung abstecken: In einem ersten Schritt werden die relevanten Spannungsfelder für Wertefragen beim Einsatz *künstlicher Systeme*[2] anhand von Fallgeschichten diagnostiziert. Sodann werden die Werte selbst betrachtet: Was sind (moralische) Werte? Gibt es universale Werte? Und welche Werte sind aus digitalethischer Sicht insbesondere von Bedeutung? In diesem Zusammenhang wird eine Werte-Topografie der Digitalen Ethik vorgestellt. Schließlich werden zentrale ethische Ansätze daraufhin untersucht, welche Stärken und Schwächen sie für die Begründung und Perspektivierung einer Digitalen Ethik haben. Vollzogen wird dies sowohl beispielhaft in Bezug auf die Konflikte in den Fallgeschichten, als auch grundsätzlich in Bezug auf ethische Leitlinien, eine Wertehaltung sowie eine wertebasierte Gestaltung der Digitalisierung (Ethics by Design).

Beginnen wir mit der Diagnose der Spannungsfelder für Wertefragen beim Einsatz künstlicher Systeme.

1.1 Das individuelle Spannungsfeld des Wertehandelns

Menschen geraten in Konflikte, wenn sie im Umgang mit digitalen Systemen ihren Wertvorstellungen entsprechend handeln wollen. Die Gestaltung digitaler Systeme kann es Nutzer*innen erschweren, werteorientiert zu handeln, beziehungsweise sie davon abhalten, ihre Wertepräferenzen im Alltag umzusetzen. Hierzu eine Fallgeschichte (1):

> Der 20-jährige Alex möchte seine Privatsphäre schützen und kontrollieren, wer was in welchem Zusammenhang über ihn weiß. Er beschließt, auf In-

2 Da der Begriff der *künstlichen Intelligenz* umstritten ist (vgl. Kap 3.2), wird im Folgenden allgemein von künstlichen Systemen gesprochen; dazu zählen auch die Begriffe autonome beziehungsweise automatisierte Systeme, maschinelles Lernen, neuronale Netze etc., soweit sie nicht hinsichtlich ihrer Funktionsfähigkeit im konkreten Bezugsrahmen unterschieden werden.

stagram, Facebook und WhatsApp zu verzichten und stattdessen die privatheitssichernde Plattform Mastodon und den Messenger Signal zu verwenden. Dort trifft er jedoch nur wenige seiner Freunde. Zudem verabreden sich seine Kommiliton*innen regelmäßig in Lerngruppen auf Facebook. Das heißt, er gerät in ein moralisches Dilemma: Entweder ist er mehr oder weniger sozial ausgeschlossen und im Studium benachteiligt oder er kann seine Privatsphäre nicht schützen. Beide Handlungen würden nicht zu einer befriedigenden Lösung führen. Er könnte natürlich noch versuchen, seine Freunde zu überreden, mit ihm die Anbieter zu wechseln. Erfahrungsgemäß würde ihn dies einiges an Überzeugungskraft mit ungewissem Ausgang kosten. Was soll er tun?

Die Geschäftsmodelle der amerikanischen Digitalmonopole wie Alphabet (Google, Youtube etc.), Facebook, Amazon, Microsoft etc. beruhen auf der wirtschaftlichen Ausbeute der personenbeziehbaren Daten. Da diese Tech-Unternehmen über eine Machtkonzentration verfügen, die ohnegleichen in der Geschichte ist, können die Menschen ihre Privatsphäre nur dann weitgehend schützen, wenn sie auf das System verzichten, es (zum Beispiel als Computerspezialist*in) unterlaufen oder wenn sich die normativen Rahmenbedingungen des Systems ändern. Es genügt also nicht, allein die Mikro-Ebene der Akteure zu betrachten, sondern es bedarf auch einer systemethischen Perspektive, die die Meso-Ebene der Unternehmen und die Makro-Ebene der Gesellschaft betrifft. Um Alex zu befähigen, seine Privatsphäre schützen zu können, müssten die digitalen Angebote entsprechend gestaltet und Recht durchgesetzt werden. Warum sollten die Unternehmen das tun? Und wenn sie es tun, wie können sie wertebasierte Produkte entwickeln? Gibt es eine Pflicht der Politik, hierauf einzuwirken? Warum ist Privatsphäre überhaupt ein Wert? Können auch Nutzer*innen durch ihre Haltung und ihr Verhalten dazu beitragen, dass werteorientierte Produkte, zum Beispiel solche, die die Privatheit schützen, entwickelt werden?

Ethische Ansätze können hilfreich sein, diesen Fragen auf den Grund zu gehen. Bevor diese vorgestellt und eingeordnet werden, sollen zwei weitere Beispiele die Komplexität der digitalen Herausforderungen veranschaulichen. Denn die Digitalisierung betrifft nicht nur die sozialen Medien und Kommunikationsdienste, sie durchdringt oftmals viele, auch existenzielle Lebensbereiche und wird dabei nicht bewusst wahrgenommen. In diesem Zusammenhang lässt sich ein zweites Spannungsfeld für Wertefragen diagnostizieren:

1.2 Das Spannungsfeld zwischen Individuum und Gemeinschaft

Konflikte zeigen sich nicht nur im individuellen Wertehandeln, sondern in der Vergemeinschaftung und Verallgemeinerung von Geltungsansprüchen. Wenn digitale Systeme für Menschen oder Gruppen von Menschen ein besseres Leben ermöglichen, kann das zu Interessenskonflikten mit anderen Gruppen führen. Fragen der Gerechtigkeit, Gleichheit und Solidarität oder allgemein des Gemeinwohls, die in der sozial- beziehungsweise organisationsethischen Dimension zu verorten sind, können mit den für Einzelne oder Gruppen relevanten Werten im Spannungsfeld liegen. Folgende Fallgeschichte (2) veranschaulicht dies:

> Ingeburg K., 80 Jahre alt, lebt seit 30 Jahren in ihrer Wohnung und fühlt sich, auch wenn sie einen Rollator braucht und einmal täglich der Pflegedienst kommt, noch ziemlich fit. Ein Pflegeheim kommt für sie nicht infrage. Als sie von einem Forschungsprojekt liest, bei dem digitale Assistenzsysteme für Senior*innen zu Hause getestet werden sollen, erklärt sie sich spontan bereit, mitzumachen. Wo die Bewegungsmelder installiert werden sollen, kann sie selbst entscheiden. Auch das Angebot, Blutdruck, Herzfrequenz und andere Parameter zu überwachen, nimmt sie an. Ihre Tochter, die dem digitalen System nicht so ganz vertraut, besucht sie nach wie vor regelmäßig; ihr Sohn aber telefoniert in letzter Zeit eher mit ihr, als dass er noch bei ihr vorbeikommt. Als sie eines Tages stürzt und sich den Oberschenkelhals bricht, erfasst das System die Abweichung und informiert den Notdienst, der alles Nötige veranlasst. Unklar ist, warum sie stürzte. Fühlte sie sich durch das Kontrollsystem vermeintlich sicherer und bewegte sich deshalb risikoreicher als zuvor oder geschah der Sturz unabhängig davon? Oder fühlte sie sich möglicherweise dazu veranlasst, sich mehr als sonst zu bewegen, um einen möglichst fitten Eindruck zu hinterlassen? Mehr Bewegung ist ja prinzipiell gut, aber mit dieser Folge?

Würde sich erweisen, dass das System den Sturz mitverursacht hat, wären – abgesehen von rechtlichen Aspekten wie zum Beispiel dem Datenschutz und der Haftungsfrage – ethische, soziale und psychologische Perspektiven zu berücksichtigen, und zwar unter Einbeziehung aller Beteiligten (sogenannte Stakeholder): die Sicht der Pflegebedürftigen, des Pflegedienstes, der Kinder, der Dienstanbieter*innen und Entwickler*innen. Dabei geht es insbesondere um Wertefragen, sowohl aus individualethischer als auch sozial- und organisationsethischer Sicht. Hierbei handelt es sich um unterschiedliche Ge-

genstandsbereiche der ethischen Praxis. So adressiert die Individualethik die Mikro-Ebene der Akteure beziehungsweise des Handlungssubjekts: das Handeln der oder des Einzelnen unter den Aspekten der moralischen Rechte, Pflichten, Handlungsmotivationen, Tugenden (Charaktermerkmale, Dispositionen) sowie deren Vorstellungen von einem guten und gelingenden Leben. Die Sozialethik richtet hingegen den Blick auf die Makro-Ebene der Gesellschaftsstruktur, die die Ermöglichungsräume, Bedingungen und Grenzen für individuelles Handeln vorgibt. Wertbegriffe wie soziale Gerechtigkeit, Gemeinwohl, Solidarität und Good Governance lassen sich dieser Ebene zuordnen, wobei eine scharfe Abgrenzung zur Individualethik nicht vorgesehen ist. Es handelt sich vielmehr um zwei sich ergänzende und gegebenenfalls überschneidende Perspektiven. Die erste Fallgeschichte von Alex zeigt, dass der Schutz der Privatsphäre im digitalen Alltag sowohl eine individual- als auch sozialethische Dimension hat.

Gleiches gilt für die Geschichte von Ingeburg K.: Aus individualethischer Sicht ist zu fragen, ob und inwieweit das digitale Kontrollsystem ein Mehr an Selbstbestimmung, Gesundheit und Sicherheit (Rechte) für Ingeburg K. bietet und wie sich ihre Angehörigen ihr gegenüber verhalten sollten (Pflichten). Wenn sich das System für die häusliche Pflege für Ingeburg K. als sinnvoll erweisen würde, stellt sich aus sozialethischer Perspektive die Frage nach dem grundlegenden Anspruch und einem gerechten Zugang zu diesem Pflege-Assistenzsystem: Sollten alle Pflegebedürftigen einen Anspruch auf ein solches System haben, weil es ihnen mehr Autonomie im Alter und womöglich auch ein längeres Leben ermöglicht (zum Beispiel weil frühzeitig Gesundheitsrisiken erkannt werden)? Ist im Sinne einer Solidargemeinschaft der Geltungsanspruch auch dann noch zu rechtfertigen, wenn die Versicherungsbeiträge für alle anderen steigen? Und deren Zahl größer ist als die der Pflegebedürftigen? Liegt das Gemeinwohl in einer höheren Anzahl von Profiteuren oder in einer zu benennenden höheren Qualität des Zusammenlebens (siehe Kap. 3)?

Die zwei bislang diskutierten Beispiele für Spannungsfelder von Wertefragen bei digitalen Systemen haben noch nicht der Tatsache Rechnung getragen, dass die digitalen Systeme zunehmend selbstständig in moralischen Entscheidungssettings agieren (künstliche Systeme). Hierzu lässt sich ein weiteres Spannungsfeld von Wertefragen diagnostizieren:

1.3 Künstliche Systeme im Spannungsfeld von ethischem und nicht-ethischem Design

Künstliche Systeme sind wie alle technischen Systeme weder gut noch schlecht, aber auch nicht wertneutral, wie der Technikhistoriker Melvin Kranzberg allgemein schon feststellte.[3] Das heißt, dass technische Entwicklungen häufig ökologische, soziale und individuelle Konsequenzen haben, die weit über die unmittelbaren Zwecke der technischen Geräte und Praktiken selbst hinausgehen. Zudem fließt in die Entwicklung der digitalen Produkte und Systeme immer auch (implizit oder explizit) das Wertesystem der Entwickler*innen, Programmierer*innen und Manager*innen mit ein. Künstliche Systeme agieren nicht im luftleeren Raum, sondern in wertebezogenen Anwendungskontexten. Ob bei der Kreditvergabe, bei der Jobbewerbung, bei der Notenvergabe an Schüler*innen oder beim (teil-)autonomen beziehungsweise (hoch-)automatisierten Fahren stellen sie Prognosen auf, sind in Entscheidungsprozesse eingebunden oder agieren sogar selbstständig; sie sind gleichsam *Aktanten* mit moralischen Implikationen. Ihre Fähigkeit, Muster und Korrelationen in Big Data zu erkennen sowie Prognosen zu berechnen, kann für uns in Hinblick auf die großen Herausforderungen unserer Zeit von Vorteil sein, sei es in der medizinischen Diagnostik, bei der Energieversorgung, bei der Ressourcenschonung und der Mobilität. Zugleich können ihre Berechnungen und Prognosen nicht nur in die Selbstbestimmung und Autonomie des Menschen eingreifen, sie können auch zu Diskriminierung, Ausgrenzung und Geschlechterungerechtigkeit führen. Auch die zugrunde liegende ökonomische und politische Programmatik wirken auf die jeweilige Technikanwendung. Für Felix Stalder ist nicht die Technik, sondern eine neoliberale Ideologie das Problem: »Das zentrale Hindernis für Algorithmen, wie wir sie wollen, liegt in der nach wie vor alle Felder der Gesellschaft dominierenden neoliberalen Programmatik.«[4] Wie sich diese im Alltag auswirken kann, veranschaulicht die Fallgeschichte (3) von Louise und Ann-Kathrin:

---

3 Vgl. Kranzberg, Melvin: *Technology and history: Kranzberg's laws*, in: Technology and Culture, Vol. 27, No. 3, 1986, S. 545.

4 Stalder, Felix: *Algorithmen, die wir brauchen. Überlegungen zu neuen technopolitischen Bedingungen der Kooperation und des Kollektiven*, in: Philipp Otto/Eike Gräf (Hg.): 3Ethics. Die Ethik der digitalen Zeit, Berlin: iRights.Media 2017, S. 54.

Louise bewirbt sich bei einem großen amerikanischen Unternehmen. Sie hat sehr gute Abschlussnoten, einschlägige erforderliche Kenntnisse etc. Bei ihren Hobbys gibt sie an, dass sie auch einen Preis im Frauen-Schach gewonnen hat. Weder sie noch andere Bewerberinnen werden von dem KI-gesteuerten Auswahlinstrument für ein Vorstellungsgespräch vorgeschlagen. Denn die KI hat auf der Datenbasis vorhergehender erfolgreicher Bewerbungsprofile im Unternehmen, die vorwiegend von Männern waren, »gelernt«, dass Frauen nicht zu berücksichtigen sind. Nachdem Louise später von der diskriminierenden KI erfährt, fühlt sie sich einerseits ungerecht behandelt und gedemütigt, anderseits kann sie der KI auch keine Schuld zuweisen. In ihren Augen ist die KI nicht dafür verantwortlich zu machen, es ist ja eine Maschine.[5] Ihre deutsche Freundin Ann-Kathrin, die sie im Auslandsstudium kennengelernt hat, bewirbt sich ebenfalls gerade auf einen neuen Job. Sie wird von dem Unternehmen zu einem Telefoninterview eingeladen und ist sehr aufgeregt. Das Interview führt sie allerdings nicht mit einem Menschen, sondern mit einer Sprachanalysesoftware, die anhand von Stimmen und dem Inhalt des Gesprächs psychologische Persönlichkeitsprofile erstellt. Sie hat Glück, kurze Zeit später wird sie zu einem persönlichen Vorstellungsgespräch eingeladen. Sie freut sich darüber, hat aber auch ein unbehagliches Gefühl, denn sie fühlt sich dem System ausgeliefert: Wie kommt das Analysesystem zu dieser Entscheidung? Und welche psychologischen Informationen hat es über sie gesammelt und in welches Muster eingeordnet?

Auch wenn die Bewerbung für die beiden Frauen unterschiedlich ausgeht, relevant ist, dass die Entscheidungen der künstlichen Systeme existenzielle Konsequenzen haben. Dabei geht es nicht um die Frage der Objektivität, also ob künstliche Systeme oder Menschen objektiver entscheiden können,

5 Die Geschichte von Louise bezieht sich auf eine wahre Begebenheit. So arbeitete Amazon 2014 an der Entwicklung eines KI-gesteuerten Recruiting-Systems, das wegen des Gender Bias 2017 eingestellt wurde. Wie Reuters (1.10.2018) berichtete (https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G), wurde das System anhand von Bewerbungen trainiert, die innerhalb der letzten zehn Jahre bei Amazon eingegangen waren. Dabei handelte es sich vorwiegend um Männer. Entsprechend diesem Muster folgerte das System aus dem vorliegenden Datensatz, dass Männer die bevorzugten Kandidaten seien. Bewerbungen, in denen Begriffe wie »Frauen-Schach« als Hobby genannt wurden, wurden daher schlechter bewertet.

denn diese Frage ist müßig: weder das System noch der Mensch sind es. Vielmehr geht es darum, *dass* ein künstliches System einen Entscheidungsprozess maßgeblich steuert. Das führt uns zu der Frage, *welche Wertansprüche an die digitalen Systeme* gestellt werden sollen und, wenn überhaupt, in welchem Maße Verantwortung delegiert werden kann. Wie die Geschichte von Louise und Ann-Kathrin zeigt, sind die besagten künstlichen Systeme nicht den Werten der Fairness, Chancengleichheit, Autonomie, Privatheit, Transparenz und Nachvollziehbarkeit folgend gestaltet worden. Die Geschlechterungerechtigkeit (Gender Bias), die das künstliche System bei dem Bewerbungsverfahren von Louise verursachte, verweist noch auf eine weitere Problemlage.

1.4 Manifestationen von Diskriminierungen

Digitale Systeme können sowohl in der Gesellschaft vorhandene Diskriminierungen fixieren beziehungsweise verstärken als auch fördern.[6] Ein Beispiel für die *Fixierung* vorhandener Geschlechterrollenklischees ist der durch Microtargeting ermöglichte sogenannte Gender Commerce, der in vielfältiger Weise angeboten wird. Genderzentriertes Onlineshopping beruht auf einer stereotypen Filterung der Angebote für Werbekund*innen. Frauen werden dann eher Kosmetika als Fotoapparate angezeigt und auch die Werbeansprache wird unterschiedlich gestaltet. Dies kann möglicherweise von den Nutzer*innen sogar erwünscht sein. Ein Beispiel für die *Verstärkung* vorhandener Geschlechterrollenklischees sind Sprachassistenzsysteme wie zum Beispiel Alexa, Siri und Cortana. Standardmäßig werden sie mit weiblichen Stimmen und Namen ausgestattet. Die feminisierten Sprachassistenzsysteme erhalten Sprachbefehle und führen sie als Serviceleistung aus. Das hier gegenderte Mensch-System-Interaktionsmuster erlaubt damit Rückkoppelungen an geschlechterstereotype Interaktionsmuster, die eine *Herabwürdigung* von Frauen implizieren. Dies wird insbesondere bei feminisierten Sprachassistenten deutlich, denen devote bis allenfalls ausweichende Antworten auf sexuell belästigende Fragen einprogrammiert wurden, wie Equals und Unesco in ihrem Bericht mit Beispielen zeigen.[7]

---

6 Vgl. O'Neill, Cathy: Angriff der Algorithmen, München: Carl Hanser Verlag 2016; Criado-Perez, Caroline: Unsichtbare Frauen. Wie eine von Daten beherrschte Welt die Hälfte der Bevölkerung ignoriert, München: btb Verlag 2020.

7 EQUALS and UNESCO: I'd blush if I could. Closing gender devices in digital skills through education 2019, S. 107. https://en.unesco.org/Id-blush-if-I-could

Die symbolische Feminisierung von künstlichen Systemen kann stereotype Geschlechterrollen nicht nur online, sondern auch offline verstärken und verfestigen. Um dem entgegenzuwirken, könnte eine geschlechterneutrale, modulierte Stimme verwendet werden.[8]

Diskriminierung kann in digitale Systeme auch durch eine *Priorisierung des Männlichen* auf der sprachlichen und damit kognitiven Ebene eingeschrieben sein. Ein Beispiel hierfür ist der Übersetzungsdienst Google Translate, der in Google Chrome und damit automatisch in circa 250 Millionen Android-Smartphones europäischer Bürger*innen integriert ist. So verschwindet das weibliche Geschlecht von Berufen beziehungsweise Funktionen in der Übersetzung, wie AlgorithmWatch in einem Experiment von Nicolas Kayser-Bril zeigt:[9] »Die Präsidentin« wird im Italienischen zum »il presidente«, korrekt wäre »la presidente«. Auch ändert Google Translate das Geschlecht nach genderstereotypem Muster: »Der Krankenpfleger« wird im Französischen zur »l'infirmière«, also der »Krankenpflegerin«.[10]

Systematisiert man die Beispiele, zeigt sich folgendes Bild (vgl. Abb. 1): Gender Bias, die zu einer Diskriminierung führen können, lassen sich in einer Matrix mittels der Achse *Kommunikation/Interaktion* und *Entscheidungs-/Empfehlungssysteme* sowie der Achse *Verstärkung* der Geschlechterrollen und *Marginalisierung/Tilgung* der Frauen einordnen. Im ersten Feld der Kommunikation/Interaktion wird das Herabwürdigungsprinzip (Sprachassistenz-Beispiel) verortet, im zweiten Feld eine Priorisierung des Männlichen (Google-Translate-Beispiel), im dritten Feld der Entscheidungs- und Empfehlungssysteme besteht das Risiko der Ausgrenzung von Frauen

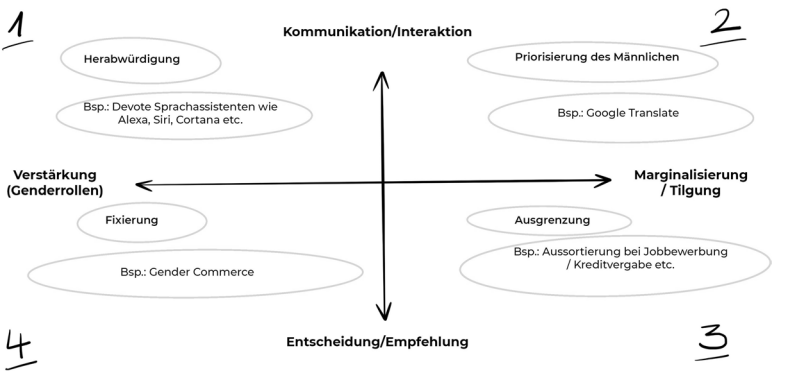
8 Hierzu s. ein praktisches Beispiel: https://www.genderlessvoice.com/

9 Kayser-Bril, Nicolas: Female historians and male nurses do not exist. Google Translate tells its European users, 17.09.2020. https://algorithmwatch.org/en/story/google-translate-gender-bias/

10 Ein Selbstversuch mit der Google Übersetzer-App zeigt ein ähnliches Ergebnis: Aus der »Medienwissenschaftlerin« wird in der italienischen Übersetzung der »lo scienziato die media«, umgekehrt wird aus der »scienziata die media« in der deutschen Übersetzung der »Medienwissenschaftler«. Hinzu kommt die von Google verursachte manipulative Nutzungslenkung, denn Android-Nutzer*innen entkommen dem Google Translate-System nicht oder nur mit Anstrengung: »Since an update in April 2019, Google Chrome prompts users to instantly translate web pages. Anyone visiting a website in a foreign language is asked to choose between the original or the google-translated version, even if the website offers an official translation in the user's preferred language.« Nicolas Kayser-Bril: Female historians and male nurses do not exist.

(Bewerbungssystem in der Louise-Geschichte) und im vierten Feld das der Fixierung von Geschlechterrollen (Gender-Commerce-Beispiel).

Abbildung 1: Geschlechterbezogenen Diskriminierung



Im philosophischen und rechtswissenschaftlichen Diskurs stellt sich zudem die Frage, ob digitale Systeme als moralische Akteure oder gar Verantwortungssubjekte zu betrachten sind und Rechtssubjekte (Träger von Rechten und Pflichten) sein können. Unzweifelhaft dürfte sein, dass sie zunehmend in Verantwortungs- und Handlungszusammenhängen agieren, die ethische Relevanz haben. Janina Loh spricht von »Verantwortungsnetzwerken«, die vorliegen, »wenn man eigentlich […] gar nicht mehr weiß, ob hier in einem gehaltvollen Sinn Verantwortung definiert werden kann, gerade weil zum Beispiel die Bestimmung eines Subjekts schwierig erscheint oder aber sich keine eindeutige Instanz ausmachen lässt oder aber die normativen Kriterien nicht benannt werden können«.[11] Ob und unter welchen Voraussetzungen Maschinen als moralische Akteure (*moral agents*) zu verstehen sind und sie verantwortlich beziehungsweise haftbar für die Folgen gemacht werden können, ist in der Roboterethik und Maschinenethik ein viel diskutiertes Thema.[12] Be-

11 Loh, Janina: *Verantwortung und Roboterethik. Ein Überblick und kritische Reflexion*, in: Matthias Rath/Matthias Karmasin/Friedrich Krotz (Hg.): Maschinenethik. Normative Grenzen autonomer Systeme, Wiesbaden: Springer VS 2019a, S. 103.

12 Vgl. hierzu u.a. Misselhorn, Catrin: Grundfragen der Maschinenethik, Dietzingen: Reclam 2018, S. 70-90; Loh, Janina: Roboterethik. Eine Einführung, Berlin: Suhrkamp 2019b, S. 48-95; Rath, Matthias: *Zur Verantwortungsfähigkeit künstlicher »moralischer Akteure«. Problemanzeige oder Ablenkungsmanöver?*, in: Matthias Rath/Matthias Karmasin/

vor auf das Für und Wider näher eingegangen wird, können hier schon die zentralen Fragen formuliert werden: Sind künstliche Systeme überhaupt als moralische Akteure zu betrachten? Falls ja, was folgt daraus?

Aus ethischer Sicht stellt sich des Weiteren die Frage, ob Roboter als »moralische Objekte« (*moral patients*) zu betrachten sind. Kurzum: Sollten wir rücksichtsvoll, anerkennend, freundlich und emphatisch mit vermenschlichten Maschinen interagieren – nicht um der Maschinen willen, sondern um unseres wertschätzenden Miteinanders willen?

Die bislang beschriebenen Spannungsfelder haben eine gemeinsame Perspektive: die des Individuums – auf sich selbst, die Gemeinschaft und das Design der digitalen Systeme. Ein bedeutsames Spannungsfeld ergibt sich aber auch auf der ideologischen Meta-Ebene hinsichtlich der Unternehmen beziehungsweise Organisationen und der Gesellschaft, die sich in konkurrierenden Meta-Narrativen widerspiegeln. Um zu verstehen, welche Wertkonzeptionen im Diskurs um die Gestaltung der Digitalisierung konkurrieren, sollen diese mithilfe einer narratologischen Analyse herausgearbeitet werden.

1.5 Digitalisierung im Spannungsfeld konkurrierender Meta-Narrative

Wie wir uns, die anderen und die Welt verstehen, hängt maßgeblich davon ab, welche Erzählungen, also Narrative, wir Phänomenen und Entwicklungen zuschreiben. Denn sie beeinflussen unsere Sicht auf die Welt und unser ethisches beziehungsweise unethisches Verhalten. Oder anders: Es gibt keine absoluten Werte, nur (geteilte) Erzählungen von diesen. Meta-Narrative sind narrative Denkmodelle, mit denen eine Kultur ihre Kommunikation zu einem Thema beziehungsweise einen Diskurs strukturiert, um so Erklärungsmuster für bestimmte vergangene Entwicklungen (*warum ist es so geworden?*) oder für mögliche zukünftige Entwicklungen (*so wird es weitergehen*) zu erhalten.[13] Meta-Narrative sind als übergeordnete Narrative zu verstehen, die sich aus einzelnen narrativen Kommunikationsakten (Kommunikaten) abstrahieren lassen. Diese Erklärungsmuster müssen nicht in einem wissenschaftlichen Sinne zutreffend oder valide sein. Oftmals ist für kulturelle

---

Friedrich Krotz (Hg.): Maschinenethik. Normative Grenzen autonomer Systeme, 2019, S. 223-242; Wallach, Wendell/Allen, Collin: Moral Machines. Teaching Robots Right from Wrong, New York: Oxford University Press 2009.

13 Vgl. Müller, Michael/Grimm, Petra: Narrative Medienforschung. Einführung in Methodik und Anwendung, Konstanz/München: UVK Verlagsgesellschaft 2016, S. 97-10.

Meta-Narrative bezeichnend, dass sie *nicht* evidenzbasiert sind: So beruhen beispielsweise die Meta-Narrative der Verschwörungserzählungen im Zuge der Corona-Pandemie, die zu einer »Infodemie«[14] geführt haben, ja geradezu darauf, dass sie alles andere als durch Fakten bestätigt sind. Der Begriff des *Meta-Narrativs* geht auf Jean-François Lyotard zurück, der vom Ende der »großen Erzählungen« sprach, was sich allerdings als falsch erwies.[15] Die Kultur einer Gesellschaft konstituiert sich durch Erzählungen, wie Wolfgang Müller-Funk meint: »Naheliegend wäre es, die konstitutive Bedeutung von Narrativen für Kulturen ins Auge zu fassen und Kulturen womöglich als mehr oder weniger (hierarchisch) geordnete Bündel von expliziten und auch impliziten, von ausgesprochenen, aber auch verschwiegenen Erzählungen zu begreifen.«[16] Mittels einer narratologischen Methode[17] lassen sich also gesellschaftliche Diskurse, sofern ihnen narrative Strukturen zugrunde liegen, beschreiben. Sie dient auch der narrativen Ethik, um ethische Werte deskriptiv zu erfassen. Die Narratologie und die narrative Ethik decken sich in ihrem Bild vom Menschen als *homo narrans*,[18] wonach der Mensch seine Identität, sein Gedächtnis, sein Werteverständnis und seine Emotionen narrativ konstruiert.

Für die Analyse der Meta-Narrative braucht es vorab eine Begriffsklärung: Was ist eigentlich ein *Narrativ*? Der Begriff hat in der Nachfolge eines *narrative turn* in den Geisteswissenschaften zu einem beinahe inflationären Gebrauch geführt und wird uneinheitlich verwendet sowie selten definiert. Hier ist unter einem Narrativ nur dann ein Narrativ zu verstehen, wenn es eine narrative Struktur aufweist. Diese besteht aus einer triadischen Struktur mit einer Ausgangssituation, einer Transformation und einer Endsituation, wobei eine

14 Grimm, Petra: *Entwirklichung – Zum Vertrauen in Zeiten der digitalen Infodemie*, in: Klaus Koziol (Hg): Entwirklichung der Wirklichkeit. Von der Suche nach neuen Sicherheiten, München: Kopaed 2020, S. 55-83.

15 Lyotard, Jean-François: Das postmoderne Wissen. Ein Bericht, Wien: Passagen 2012.

16 Müller-Funk, Wolfgang: Die Kultur und ihre Narrative. Eine Einführung, Wien/New York: Springer 2008, S. 17.

17 Müller, Michael/Grimm, Petra: Narrative Medienforschung. Einführung in Methodik und Anwendung 2016, S. 55-96; Titzmann, Michael: *Narrative Strukturen in semiotischen Äußerungen*, in: Hans Krah/Michael Titzmann (Hg.): Medien und Kommunikation. Eine interdisziplinäre Einführung. Dritte, stark erweiterte Auflage, Passau: Stutz 2013, S. 113-141.

18 Grimm, Petra: *Haltung in einer digitalisierten Kindheit. Die Perspektive der narrativen Ethik*, in: Ingrid Stapf/Marlis Prinzing/Nina Köberer (Hg.): Aufwachsen mit Medien. Zur Ethik mediatisierter Kindheit und Jugend, Baden-Baden: Nomos 2019, S. 85-99.

notwendige, aber nicht hinreichende Bedingung (es gibt noch weitere) gegeben sein muss: Die Transformation muss *ereignishaft*, also bedeutsam sein, sei es für einen Akteur, eine Gemeinschaft oder eine soziale, politische oder ökonomische Ordnung. Der Digitalisierungsprozess als solcher kann als ereignishafte Veränderung verstanden werden. Je nach Perspektive kann er allerdings unterschiedlich erzählt werden. Der Forderung, dass wir im Zuge der Digitalisierung »unsere derzeitigen Narrative einer kritischen Prüfung unterziehen müssen, und zwar auf individueller, gesellschaftlicher und politischer Ebene«, wie Luciano Floridi[19] meint, sollte nachgekommen werden. Dazu ist aber erst einmal zu klären, welche Meta-Narrative sich derzeit in Bezug auf die Digitalisierung und einen der Antriebsmotoren – die künstliche Intelligenz – in den Vordergrund drängen.

Ob in den Medien, in Unternehmen, in pädagogischen oder politischen Diskussionen, zwei gegensätzliche Meta-Narrative bestimmen die Diskurse zur künstlichen Intelligenz: das Meta-Narrativ vom *Heiligen Gral* und das von der *Büchse der Pandora*, wie es hier bezeichnet wird.

Das *Heilige-Gral-Narrativ* erzählt uns die Geschichte der künstlichen Intelligenz als eine, die unsere großen Probleme lösen wird. Demnach würde die Zukunftstechnologie der künstlichen Intelligenz eine bessere Welt ermöglichen, mehr Lebensqualität und Komfort bieten und globale Probleme (wie Klimawandel, Epidemien, Krebs etc.) überwinden helfen. Dieses Meta-Narrativ findet sich in unterschiedlichen Facetten, angefangen von moderaten Auslegungen, die bloß den wirtschaftlichen Nutzen digitaler Technologien in den Vordergrund stellen, bis zu extremen Erzählungen, nach deren Weltbild eine Optimierung des Menschen durch die digitalen Technologien unbedingt erforderlich sei. Die Erzähler*innen dieser techniktotalitären Geschichte sind die großen Tech-Unternehmen aus dem Silicon Valley, deren Welt- und Menschenbild Paul Nemitz und Matthias Pfeffer[20] als »Kalifornische Ideologie« eindrücklich beschrieben haben. Sie nehmen dabei auch auf den von Yuval Noah Harari geprägten Begriff des »Dataismus« Bezug: »Dem Dataismus zufolge besteht das Universum aus Datenströmen, und der Wert jedes Phäno-

19 Floridi, Luciano: *Die Mangroven-Gesellschaft. Die Infosphäre mit künstlichen Akteuren*, in: Otto Philipp/Eike Graf, (Hg.): 3Ethics. Die Ethik der digitalen Zeit, Berlin: IRights Media 2017, S. 28.

20 Nemitz, Paul/Pfeffer, Matthias: Prinzip Mensch. Macht, Freiheit und Demokratie im Zeitalter der Künstlichen Intelligenz, Bonn: J.H.W. Dietz 2020, S. 90-153.

mens oder jedes Wesens bemisst sich nach seinem beziehungsweise ihrem Beitrag zur Datenverarbeitung.«[21]

Das *Pandora-Narrativ* erzählt uns dagegen die Geschichte der Digitalisierung beziehungsweise künstlichen Intelligenz als eine Bedrohung, die unsere Lebenswelt und die Gesellschaft verändern wird. Hier werden Ängste artikuliert, die Verluste in vielerlei Hinsicht umfassen, seien es Arbeitsplätze, Werte oder stabile politische Strukturen. Auch wird befürchtet, dass sich das Meister-Sklave-Modell zukünftig umkehrt und wir am Ende diejenigen sind, die sich den künstlichen Systemen anpassen oder gar unterordnen müssen (Singularität). Nicht unberechtigt werden in diesem Meta-Narrativ auch die Risiken der digitalen Überwachung und Manipulation angesprochen, die in der Befürchtung eines Überwachungskapitalismus[22] oder eines Überwachungsstaats nach dem Vorbild Chinas[23] zum Ausdruck gebracht werden. Chinas digitale Staatsdoktrin erzählt hingegen ein anderes Narrativ: das des *Weltführers*, der mittels der KI-getriebenen Dienste seine globale Vormachtstellung erreichen und den Wohlstand seines Volkes sichern will. Dass China hierfür gute Voraussetzungen hat, ist nicht von der Hand zu weisen, wie Kai-Fu Lee[24] argumentiert.

Die Erzählmodelle der US-amerikanischen Tech-Giganten und der Überwachungskritiker*innen stehen sich diametral entgegen. Zudem zeigen sie erzählstrukturell die radikalste Form der Ereignishaftigkeit: Hier wird das Ereignis nicht durch einen Akteur hervorgerufen, der die Grenze (eines semantischen Raums) überschreitet, sondern die semantische Ordnung selbst wird transformiert. In der Silicon-Valley-Erzählung soll sich die Welt der defizitären Menschheit, die sich nicht selbst optimieren und nicht mit Krisen adäquat umgehen kann, durch die KI-Technologie transformieren, um fittere Menschen zu schaffen, die über die biologischen Grenzen hinauswachsen. Ziel ist eine technizistische Weltverbesserung. Technik könne die biologische Evolution ersetzen (vgl. Abb. 2).

---

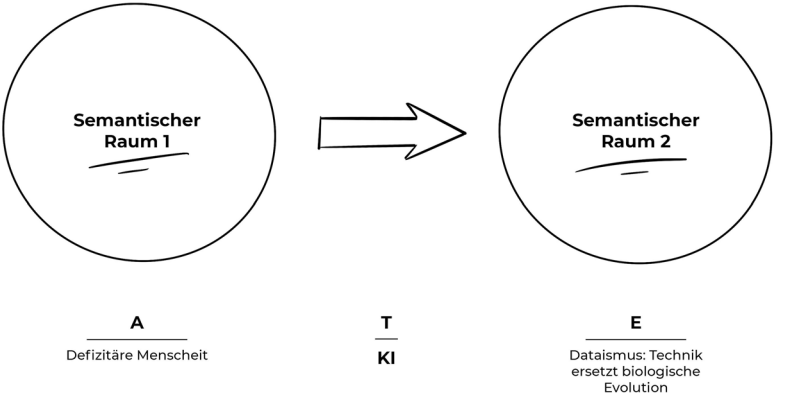
21 Harari, Yuval Noah: Homo Deus. Eine Geschichte von Morgen, München: C.H. Beck 2017, S. 497.

22 Vgl. Zuboff, Shoshana: Das Zeitalter des Überwachungskapitalismus. Aus dem Englischen von Bernhard Schmid, Frankfurt/New York: Campus Verlag 2018.

23 Vgl. Strittmatter, Kai: Die Neuerfindung der Diktatur. Wie China den digitalen Überwachungsstaat aufbaut und uns damit herausfordert, München: Piper 2018.

24 Lee, Kai-Fu: AI Super Powers. China, Silicon Valley and the New World Order, Boston, MA: Houghton Mifflin Harcourt 2018, S. 18.

Abbildung 2: Meta-Narrativ des Silicon Valley



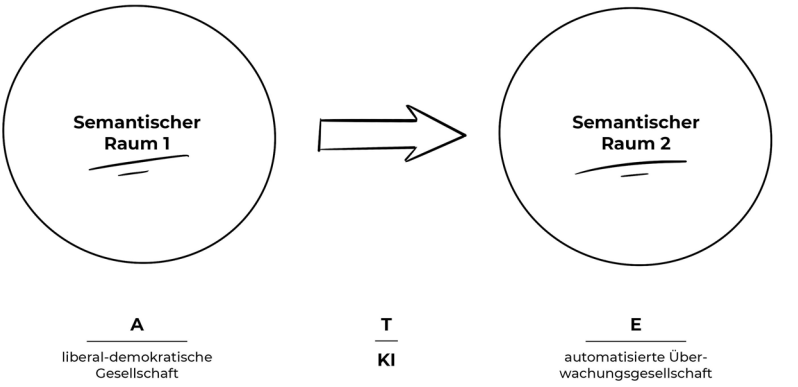
Die semantischen Räume dieses Erzählmodells transportieren implizit einen Wertewandel: Der Wert des Menschen als autonomes Individuum in seiner leiblichen Verfasstheit und Verletzlichkeit, die alle Menschen verbindet, ist obsolet. Die Gesellschaft wird nicht mehr durch liberal-demokratische Institutionen, sondern durch digitale Technologien vorangebracht. Vertreter des Transhumanismus, wie zum Beispiel der Chef-Techniker von Google, Ray Kurzweil, legen dieses Narrativ ihrer Ideologie zugrunde.[25] Er sowie die Anhänger*innen der Singularitäts-These gehen davon aus, dass wir noch in diesem Jahrhundert an den Punkt kommen werden, wo KI die menschliche Intelligenz nicht mehr benötigt, immer schnellere Weiterentwicklungen ihrer selbst beginnt und das Universum mit einem neuen Geist erfüllen wird. Das Erzählmodell der Überwachungskritiker*innen dagegen entwickelt keine technizistische Utopie, sondern die Dystopie einer automatisierten Überwachungsgesellschaft, die die Auflösung einer liberal-demokratischen Gesellschaft bedeuten würde (vgl. Abb. 3).

In Geschichten gibt es nach dem Modell von Algirdas Greimas[26] ein dynamisches Beziehungsgefüge der funktionalen Aktanten: Held, Wunschobjekt,

25 Kurzweil, Ray: Menschheit 2.0. Die Singularität naht, Berlin: Lola Books 2014.

26 In der deutschen Übersetzung zit. n. Keller, Otto/Hafner, Heinz: Arbeitsbuch zur Textanalyse. Semiotische Strukturen, Modelle, Interpretationen, München: Wilhelm Fink Verlag 1986, S. 87.

*Abbildung 3: Meta-Narrativ der Überwachungskritiker*innen*

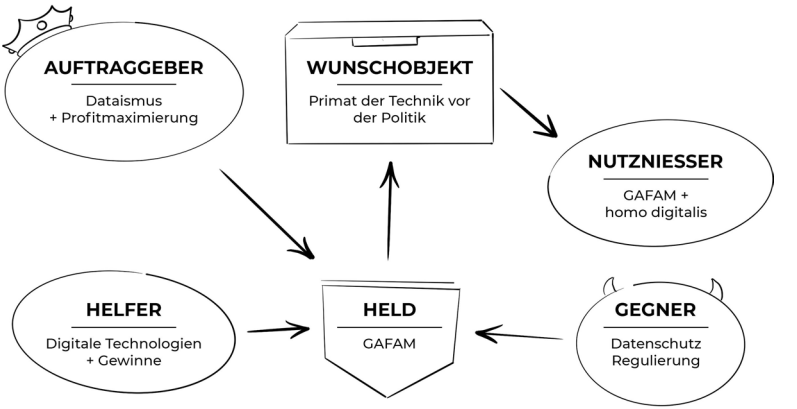


Helfer, Gegner, Auftraggeber und Nutznießer. Diese müssen keine menschlichen Akteure sein, es können auch abstrakte Instanzen sein, wie zum Beispiel das *Gewissen* als Auftraggeber oder Institutionen in der Heldenfunktion. Vor allem die dynamischen Beziehungen zwischen dem Helden und seinem Wunschobjekt sowie seinem Helfer beziehungsweise Gegner konstituieren eine Geschichte. Das Modell ist deshalb so attraktiv, weil es universell anwendbar ist und die funktionalen Beziehungen in Narrativen verdeutlicht, wie am Beispiel des Silicon-Valley-Narrativs zu zeigen ist (vgl. Abb. 4). Hier sind die Tech-Unternehmen in der Position des Helden, sie treiben die Geschichte an: Was ist ihr Wunsch? Sie wollen das Primat der Technik vor der einhegenden Politik und dem Recht. Die digitalen Technologien sowie die immensen Gewinne, die sie durch die Digitalwirtschaft erzielen, helfen ihnen dabei. Das einzige, was sie derzeit bremsen könnte, ist eine stärkere Regulierung. Aus Sicht der Tech-Unternehmen würden die Menschheit und natürlich sie selbst davon profitieren, wenn anstelle von demokratischen Institutionen die Technik vorgeben würde, wie man sich zu entscheiden habe. Was sie antreibt, ist ihre Ideologie und der Wunsch nach Profitmaximierung.

1.6 Eine alternative Erzählung – der digitale Mittelweg

Was wir für eine menschengerechte Gestaltung der künstlichen Systeme jedoch brauchen, ist aus meiner Sicht eine *alternative Erzählung*. Ich nenne sie

Abbildung 4: Aktantenstruktur des Silicon-Valley-Narrativs



die vom *goldenen/digitalen Mittelweg*. Dieses Narrativ der *aurea mediocritas* findet sich schon in der Antike bei Horaz: »In schwieriger Lage zeige dich beherzt und tapfer; du wirst aber auch weise die von allzu günstigem Wind geschwellten Segel einziehen.«[27] Für Aristoteles ist der goldene Weg der Mitte – das richtige Maß *(Mesotes)* – ein wesentliches Prinzip seiner Tugendethik. Die Tugend liegt demnach zwischen zwei Extremen, einem Übermaß und einem Mangel, zum Beispiel die Tugend der Freigebigkeit als Mitte zwischen den Extremen der Verschwendungssucht und des Geizes, die Tugend der Besonnenheit als Mitte zwischen Gedankenlosigkeit und Rigorismus. Weder ein Zuviel noch ein Zuwenig führt zum guten Leben. Dieses kann aber nicht im Eigennutz gefunden werden, sondern im sozialen Handeln und in der Entwicklung einer immer wieder zu überprüfenden Haltung. Je nach Disposition des Menschen und dem Kontext müssen ein Zuviel oder ein Zuwenig unterschiedlich definiert werden. Dieser Relationalismus macht den Weg der goldenen Mitte so attraktiv, da es somit kein statisches, sondern ein dynamisches Prinzip des sozialen Handelns meint. Gleichwohl ist Aristoteles' Lehre von der Tugend als Mitte in seiner Konzeption mehrfacher Kritik ausgesetzt. Bereits Kant, aber auch modernen Philosoph*innen gilt sie als »dunkel und

27 Horaz: Oden und Epoden. Herausgegeben und übersetzt von Gerhard Fink, Düsseldorf/Zürich: Artemis und Winkler Verlag 2002, S. 105.

zugleich als entweder leer oder nicht anwendbar oder nicht hilfreich«.[28] Allerdings wird Kant dem aristotelischen Konzept nicht gerecht, wenn er es als Aufruf zur Mäßigung beziehungsweise zum Mittelmaß missinterpretiert.[29] Haltbar im Kern erscheint das *Mesotesprinzip*, soweit es sich um Tugenden im Bereich der Affektivität und des Reflektierens handelt (beispielsweise *Mut* anstelle von *Übermut* oder *Verzagtheit*), nicht aber bei Tugenden des Willens, wie Gerechtigkeit und Nächstenliebe. Denn was wäre ein Zuviel oder Zuwenig in Bezug auf Gerechtigkeit oder Nächstenliebe? »Die Mesoteslehre lässt sich also nur auf die Tugenden des individuellen Lebens, auf Besonnenheit und Standhaftigkeit und ihre Unterformen anwenden.«[30] Abstrahiert man aus dem tugendethischen Mesotes-Ansatz drei strukturelle Aspekte, nämlich den der triadischen Struktur (die Mitte zwischen zwei nicht wünschenswerten Extremen), den Aufruf zum Balance-Finden sowie das dynamische Prinzip des sozialen Handelns in den jeweiligen Kontexten, dann erscheint der Weg der goldenen Mitte durchaus als ein für die (angewandte) Digitale Ethik[31] sinnvolles Reflexionsmodell.

Eine gegenwartsnahe Lesart des goldenen Mittelwegs im digitalen Zeitalter könnte dazu verhelfen, sich eine Haltung im Umgang mit digitalen Technologien anzueignen, die weder ein Zuviel noch ein Zuwenig bedeutet, wie es vor allem beim Erwerb einer Digitalkompetenz relevant ist: Weder Resignation noch Technik-Euphorie helfen im Umgang mit digitalen Diensten. Aber auch bei Entscheidungen in Unternehmen und Organisationen kann ein Austarieren eines Zuviels und eines Zuwenigs ein probater Weg sein, um sich nachweislich als werteorientiert und glaubhaft zu positionieren, zum Beispiel indem anstelle von haltloser Profitmaximierung oder Ethics-Washing (Ethik als Feigenblatt) eine ernst gemeinte, verantwortungsvolle Unternehmenskultur angestrebt wird.

Letztlich lässt sich das Meta-Narrativ eines (zukünftigen?) europäischen Wegs bei der Digitalisierung als ein Modell der goldenen Mitte zwischen dem Extrem eines datenkapitalistischen US-amerikanischen Modells und eines chinesischen Überwachungsstaats entwerfen. Stellt man dieses Modell des

28 Wolf, Ursula: *Über den Sinn der Aristotelischen Mesoteslehre*, in: Dies.: Handlung, Glück, Moral. Philosophische Aufsätze, Berlin: Suhrkamp 2000, S. 111.

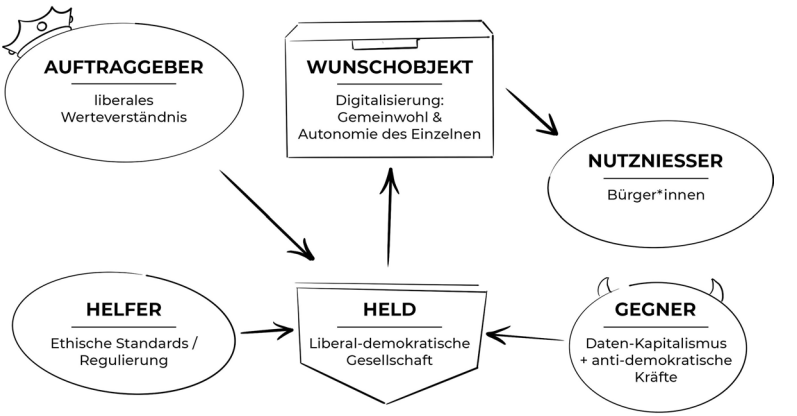
29 Vgl. die Argumentation in Halbig, Christoph: Der Begriff der Tugend und die Grenzen der Tugendethik, Berlin: Suhrkamp 2013, S. 180-181.

30 Wolf, Ursula: Über den Sinn der Aristotelischen Mesoteslehre 2000, S. 133.

31 Vgl. Grimm, Petra/Keber, Tobias/Zöllner, Oliver: Digitale Ethik. Leben in vernetzten Welten, Dietzingen: Reclam 2019.

goldenen Mittelwegs in seiner Handlungsstruktur dar, ergibt sich folgendes narratives Beziehungsgefüge (vgl. Abb. 5): Die liberal-demokratische Gesellschaft befindet sich nun in der Position des Helden. Ihr Ziel ist eine digitale Gesellschaftsordnung, die sich an einem (durch demokratische Prozesse begründeten) Gemeinwohl und dem Autonomieprinzip orientiert und die auf den Grundrechten und Werten einer freien Gesellschaft beruht. Ihr Auftraggeber, also das, was sie antreibt beziehungsweise motiviert, ist ihr liberal-demokratisches Werteverständnis. Ethische Standards und Regulierung sind in dieser Erzählung nicht innovationshemmend, sondern vielmehr Helfer, die sie auf ihrem Weg unterstützen. Gegner sind die Vertreter des Datenkapitalismus und antidemokratische Kräfte im nationalen und internationalen Raum.

Abbildung 5: Aktantenstruktur des goldenen Mittelwegs



Vom Erfolg dieser Heldengeschichte würden vor allem die Bürger*innen profitieren. Ob diese Geschichte reine Illusion bleibt, ist zum gegenwärtigen Zeitpunkt offen. Möglicherweise kann sie das Wertevakuum einer rein marktgetriebenen und/oder technizistischen KI-Erzählung auffüllen. Die Wirkmächtigkeit von Erzählungen war immerhin in der Vergangenheit oftmals ein Antriebsmotor für kulturellen Wandel.

2 Werte aus digitalethischer Sicht

Nach dem Versuch einer Systematisierung und Einordnung der Wertefragen des Digitalen in individuelle, soziale, gestalterische und diskursbezogene Spannungsfelder soll nun der Frage nachgegangen werden, welche Werte im digitalen Zeitalter besondere Aufmerksamkeit verdienen. Zuvor ist aber zu klären, was unter Werten zu verstehen ist.

Es entbehrt nicht einer gewissen Ironie, dass Aristoteles der Ökonomie *(oikonomia)* ihren Namen gab, der sie im Übrigen als ethische Wissenschaft verstand, während der Begriff *Wert* und dessen Gebrauch ursprünglich aus dem Bereich der Wirtschaft stammt.[32] Sein Begriffswandel führte über die »[…] Philosophie des 19. Jahrhunderts und von dort zu den Kultur- und Sozialwissenschaften und dem öffentlichen Sprachgebrauch des 20. Jahrhunderts[…]«[33]. Die Vieldeutigkeit des Wertbegriffs erleichtert es nicht gerade, seine Bedeutung für das Digitale zu erfassen. Hilfreich ist es, sich vorab zu vergegenwärtigen, was mit dem Begriff *Wert* gemeint ist und welche Funktionen Werte haben können.

Werte lassen sich in einer ersten Annäherung in dreierlei Weise unterscheiden: »(1) ›Etwas ist ein Wert‹ – hier wird ein bestimmtes Etwas (ein Gegenstand, eine Person, eine Haltung, ein Zustand etc.) als Wert an sich betrachtet, als ein ›Objektwert‹, der als Gut zu respektieren ist. (2) ›Etwas hat einen Wert‹ – hier wird einem bestimmten Etwas im Blick auf einen Bewertungsmaßstab ein Wert zugesprochen (zum Beispiel ein materieller Wert, ideeller Wert etc.). Schließlich spricht man (3) davon, daß Handlungen bestimmten Werten verpflichtet sein können, die dann den Sinn dieser Handlungen allererst ausmachen, die Handlungen als Handlungen allererst begründen.«[34] Die beiden erstgenannten Sichtweisen legen den Fokus auf das *Sein* der Werte und die *Bewertungsmaßstäbe*. Letztere Sichtweise versteht Werte als handlungsleitend und legt den Fokus auf die *Realisierung* der Werte und ist für das vorliegende Buch größtenteils maßgeblich.

Aus deskriptiver Sicht lassen sich Werte als Vorstellungen, Ideen oder Ideale verstehen. Werte bezeichnen, was wünschenswert ist – sie sind be-

32 Vgl. Anwander, Norbert: *Wert/Werte*, in: Stefan Gosepath/ Wilfried Hinsch/Beate Rössler (Hg): Handbuch der politischen Philosophie und Sozialphilosophie. Bd. 2, Berlin: Walter de Gruyter 2008, S. 1474.

33 Joas, Hans: Die Entstehung der Werte, Frankfurt a.M.: Suhrkamp 1999, S. 37.

34 Hubig, Christoph: Technik- und Wissenschaftsethik. Ein Leitfaden, Berlin/Heidelberg/New York: Springer 1993, S. 133-134.

wusste oder unbewusste Orientierungsstandards und Leitvorstellung. In der soziologischen und psychologischen Werteforschung werden den Werten bestimmte Funktionen zugeschrieben: Werte können eine Steuerungsfunktion von Handlungen und Verhaltensweisen innehaben.[35] Ebenso können sie die Wahrnehmung der Welt und deren Beurteilung beeinflussen: »Wert wird […] als ein inneres beziehungsweise internalisiertes Konzept verstanden, das mitbestimmt, wie wir die Welt sehen und uns in ihr verhalten.«[36] Nach Robert Reichart[37] beeinflussen Werte die Motive der oder des Einzelnen und sind inhaltlich mit einem hohen Allgemeinheits- beziehungsweise Abstraktionsgrad ausgestattet, was eine semantische Vagheit des jeweiligen Wertes impliziert; tendenziell sind sie für größere Bevölkerungsgruppen maßgeblich. Zusammengefasst lassen sich aus deskriptiver Sicht Werte als abstrakte Wünsche und Vorstellungen verstehen, die im Wesentlichen drei Funktionen haben: Sie können Handlungen (1) steuern, sie sind an unserer (2) Wirklichkeitskonstruktion beteiligt und sie stellen (3) Handlungsgründe beziehungsweise leitende Motive dar.

Wenn es um die Frage geht, warum welche Werte gelten sollen (normativer Wertbegriff), geben ethische Ansätze unterschiedliche Antworten: Für Wertobjektivist*innen bestehen Werte an sich und für sich. Demgemäß hätte zum Beispiel die Natur einen Wert in sich selbst, unabhängig vom Menschen, der ihr diesen Wert zuschreibt. Für Wertsubjektivist*innen sind Werte hingegen abhängig von der subjektiven Wertschätzung, zum Beispiel davon, ob die Natur zum Wohl des Menschen erhalten werden soll.[38] Davon wiederum lassen sich Ansätze unterscheiden, nach denen Werte entsprechend dem Prinzip der praktischen Vernunft beziehungsweise aufgrund von rationalen Bewertungsmaßstäben gelten,[39] zum Beispiel sollte die Natur intakt bleiben, weil sie die Grundlage für ein Fortbestehen der Menschen sichert. Aus Sicht einer Wertethik prägen Werte Weltanschauungen, sind identitätsstiftend in

35 Vgl. Scholl-Schaaf, Margret: Werthaltung und Wertsystem. Ein Plädoyer für die Verwendung des Wertkonzepts in der Sozialpsychologie, Bonn: Bouvier 1975, S. 58.

36 Oerter, Rolf: Struktur und Wandlungen von Werthaltungen, München/Basel: Oldenbourg 1970, S. 115.

37 Reichardt, Robert: *Wertstrukturen im Gesellschaftssystem – Möglichkeiten makrosoziologischer Analysen und Vergleiche*, in: Helmut Klages/Peter Kmieciak (Hg.): Wertwandel und gesellschaftlicher Wandel, Frankfurt/New York: Campus Verlag, 1979, S. 24.

38 Vgl. Birnbacher, Dieter: Analytische Einführung in die Ethik, Berlin/New York: Walter de Gruyter 2003, S. 278.

39 Vgl. Anwander, Norbert: *Wert/Werte*, S. 1475.

Bezug auf das Individuum und die Gemeinschaft und steuern unser Denken und Handeln.

2.1 Werterelativismus, Wertepluralismus und Werteuniversalismus

Bei dem Versuch, eine werteorientierte Digitalisierung zu beschreiben, wird man sehr schnell mit dem Einwand des Werterelativismus und Wertepluralismus konfrontiert. Das Argument, es gebe keine universalen Werte und deshalb könne man auch keine Werte für global wirksame Technologien ausmachen, scheint das Vorhaben ins Leere laufen zu lassen. Der Einwand ist schon deshalb ernst zu nehmen, weil digitale Technologien ja in unterschiedlichen Gemeinschaften, Kulturen etc. zum Einsatz kommen. Dem ist allerdings zu entgegnen, dass es bei diesem Vorhaben nicht um deskriptive Wertbindungen geht, die in einer Gemeinschaft, einer Kultur etc. vorhanden sind und die ja durchaus ethisch fraglich sein können, wie zum Beispiel der Wert der Jungfräulichkeit. Vielmehr sind Werte gemeint, die als normative Standards kulturübergreifend für verbindlich erachtet werden, auch wenn deren Realisierung kulturspezifisch ist. Trotz kultureller Unterschiede in der Gewichtung von Werten gibt es Werte, die alle Menschen betreffen. Beispielhaft hierfür sind diejenigen Werte, die durch die in der Allgemeinen Erklärung der Menschenrechte festgeschriebenen Grundrechte deutlich werden. Diese Werte gilt es zu berücksichtigen, ohne sie gegeneinander aufzuwiegen oder aufgrund von vermeintlichen Sachzwängen oder kulturellen Empfindlichkeiten außer Kraft zu setzen. Werte können zwar verletzt werden, aber deshalb verlieren sie zumindest nicht umgehend ihre normative Kraft. Gegen den Werterelativismus, der eine Verbindlichkeit von Werten nur systembezogen für möglich hält, oder den Wertenihilismus, der die Existenz moralischer Werte an sich negiert, wehrt sich der Werteuniversalismus, wie ihn zum Beispiel Markus Gabriel offensiv vertritt. Demgemäß gelten moralische Werte – wenn auch in einer minimalistischen Form – universal: »Der Universalismus ist das Gegenteil des Relativismus: Er behauptet, dass moralische Werte unabhängig von Gruppenzugehörigkeiten und damit für alle Menschen (und letztlich sogar über den Menschen hinaus) gelten. Es gibt also nur ein einziges System universaler Werte: das Gute, das Neutrale und das Böse.«[40] Gleichwohl weist Gabriel darauf hin, dass in den lebenspraktischen Gegebenheiten »eine prinzipiell niemals vollständig zu überwindende Kluft zwischen den universalen

40 Gabriel, Markus: Moralischer Fortschritt in dunklen Zeiten, Berlin: Ullstein 2020, S. 104.

Werten und ihren Anwendungsbedingungen in komplexen Handlungsfeldern und einzelnen Situationen«[41] bestehe.

Dieser Hinweis ist auch für das Vorhaben einer wertegestalteten Digitalisierung wichtig. Hierzu ein Beispiel aus dem globalen Wirtschaftsleben, bei dem es um den Wert der Privatheit geht: Während sich Mitarbeiter*innen in Mexiko die Veröffentlichung der Geburtstage im Unternehmen wünschen, um Geburtstagsgrüße aussprechen zu können, ist dies in Deutschland gerade nicht der Fall. Das heißt aber nicht, dass deshalb der Wert der Privatsphäre für die mexikanischen Mitarbeiter*innen nicht wichtig wäre. Für ein global agierendes deutsches Unternehmen, das sich zur Einhaltung von *Privacy* (nicht zuletzt wegen der europäischen Datenschutz-Grundverordnung) verpflichtet hat, besteht also die Herausforderung, den unterschiedlichen Sitten der Länder bei der Realisierung von Werten Rechnung zu tragen. Privatheit ist ein universaler Wert, auch wenn er kulturspezifisch ausgelegt wird und in der Realisierung kontextabhängig ist. »Als privat gilt etwas dann, wenn man selbst den Zugang zu diesem ›etwas‹ kontrollieren kann.«[42] Privatheit ist somit ein universal gültiger und gleichzeitig in der Anwendung relativer Begriff, abhängig von dem jeweiligen Kontext und kulturspezifischen Handlungspraxen. Der Anspruch, sich auf universale Werte bei künstlichen Systemen zu einigen, findet sich im Übrigen auch in den ethischen Leitlinien des weltweit größten Ingenieur*innenverbands IEEE.[43]

Nach diesen Ausführungen zum Wertbegriff und den verschiedenen Perspektiven auf Werte stellt sich die Frage, welche Werte aus Sicht einer Digitalen Ethik besonders in den Blick zu nehmen sind. Vorgeschlagen wird hierzu eine Topografie der Digitalen Ethik (vgl. Abb. 6). Sie stellt in einer Übersicht beispielhaft zehn Werte dar, die als Orientierungsorte für eine zukünftige Entwicklung und Gestaltung einer digitalen Welt dienen sollen. Diese Liste ist selbstredend nicht abgeschlossen und dient lediglich zur Anregung eines Überblicks. Auch wenn heute nicht klar ist, wo die Reise mit einer zunehmenden Vernetzung, Automatisierung, künstlicher Systeme, Robotik etc. hingeht, und die Folgen der Entwicklung für die einzelne Person und die Gesellschaft nicht absehbar sind, lassen sich doch Risikofelder erkennen, denen wir auf

41 Ebd., S. 141.

42 Rössler, Beate: Der Wert des Privaten, Frankfurt a.M.: Suhrkamp 2001, S. 23

43 The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, First Edition. IEEE, 2019. https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html, S. 10.

dem Weg einer fortschreitenden Digitalisierung begegnen. Würden wir die im Folgenden genannten Werte und Risiken ignorieren beziehungsweise negieren, würde eine liberal-demokratische Gesellschaft ihr Fundament verlieren. Als Grundlage dieser Werte-Topografie dienen ethische Leitlinien im Bereich der Mensch-Maschine-Interaktion[44] und zur künstlichen Intelligenz,[45] die Charta der digitalen Grundrechte der Europäischen Union,[46] das Gutachten der Datenethikkommission der Bundesregierung[47] sowie eigene Arbeiten zur Verankerung von Ethik in der integrierten Forschung[48].

2.2 Werte einer Digitalen Ethik

Menschenwürde: Die Würde des Menschen ist auch in einer digitalen Welt unantastbar und es besteht eine Pflicht, diese zu achten und zu schützen; die körperliche und geistige Unversehrtheit des Menschen darf nicht durch digitale Technologien beeinträchtigt werden.

Autonomie: Menschen sollen nicht als Mittel zum Zweck dienen; Menschen dürfen nicht künstlichen Systemen ausgeliefert sein, die Entscheidungen über Leben, körperliche und geistige Unversehrtheit sowie Freiheitsentzug fällen; moralische Prinzipien dürfen nur von Menschen aufgestellt werden; künstliche Systeme dürfen nicht ohne Kenntnis der betroffenen Menschen zur Manipulation des Verhaltens eingesetzt werden; Nutzer*innen digitaler Produkte und Dienste müssen autonom zwischen diesen wechseln können.

---

44 Vgl. u.a. Grimm, Petra/Mönig, Julia (2020): KoFFI-Code: Ethische Empfehlungen des BMBF-Projekts KoFFI. Kooperative Fahrer-Fahrzeug-Interaktion, Stuttgart 2020. https://www.hdm-stuttgart.de/digitale-ethik/forschung/forschungsprojekte/abgeschlossene_forschungsprojekte/KOFFI/KoFFi_PDF_inkl.Korrekturen_V4_Druck-mit-Schnittmarken.pdf

45 Vgl. das Verzeichnis der ethischen Richtlinien für künstliche Intelligenz von AlgorithmWatch: AI Ethics Guidelines Global Inventory. https://inventory.algorithmwatch.org/

46 Die Autorin ist Mitunterzeichnerin dieses politischen Manifests. https://digitalcharta.eu/#post-22838

47 Datenethikkommission der Bundesregierung: Gutachten der Datenethikkommission der Bundesregierung 2019. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6

48 Vgl. zuletzt die Entwicklung einer Software für Forscher*innen, um ethische, rechtliche und soziale Kriterien in Forschungsprojekten zum Thema Mensch-Maschine-Interaktion und künstliche Intelligenz zu verankern: »Automatisiertes ELSI-Screening & Assessment-Tool für MTI-Forschungsvorhaben (ELSI-SAT)«, https://www.elsi-sat.de/

Abbildung 6: Werte-Topografie

Privatheit: Die Privatsphäre der Menschen ist zu achten; jeder Mensch hat das Recht, seine Daten schützen zu können und nicht überwacht zu werden; das Prinzip ist zu achten, dass Individuen in einem Rechtsstaat auch Rechte zum Selbstschutz gegenüber der Staatsmacht haben und behalten müssen; personenbezogene Daten dürfen nur für festgelegte Zwecke bei den Betroffenen erhoben und verarbeitet werden, wenn hierfür eine gesetzliche Grundlage besteht; die Privatsphäre von Kindern, Heranwachsenden und schutzbedürftigen Menschen ist besonders zu achten; die Löschung und Berichtigung von persönlichen Daten, Widerspruch, Information und Auskunft müssen gewährleistet sein; jeder Mensch hat das Recht auf eine nicht-personalisierte Nutzung digitaler Angebote, deren Einschränkung darf nur auf gesetzlicher Grundlage stattfinden.

Freiheit: Jeder Mensch hat ein Recht auf freie Information und Kommunikation sowie auf freie Meinungsäußerung in digitalen Medien; das Recht auf Meinungsfreiheit findet seine Schranken in den Vorschriften der allgemeinen Gesetze; jeder Mensch hat das Recht auf freien und gleichen Zugang zu

Kommunikations- und Informationsdiensten; die Medien- und Pressefreiheit ist zu garantieren.

Transparenz und Erklärbarkeit: Die Kriterien automatisierter Entscheidungen sind offenzulegen; die Datenverarbeitung muss transparent und nach dem Stand der Technik gestaltet werden; Anwender*innen künstlicher Systeme sollen deren Funktionsweise verstehen, erklären und kontrollieren können; die von einer Entscheidung Betroffenen sollen entsprechend ihrem Kompetenzniveau genügend Informationen erhalten, um ihre Rechte angemessen wahrnehmen und die Entscheidung infrage stellen zu können; es sind Methoden zur Nachvollziehbarkeit der Ergebnisse von künstlichen Systemen zu fördern; einer Vermenschlichung von künstlichen Systemen, die falsche und in der Praxis stark risikobehaftete Annahmen über eine Systemleistung erstellen, ist durch geeignete Maßnahmen entgegenzuwirken.

Gerechtigkeit: Künstliche Systeme sollen nach fairen Algorithmen gestaltet sein, hierzu müssen sich Programmierer*innen ihrer Voreingenommenheit, Vorurteile und kulturellen Prägung bewusst werden, zudem muss die Datenbasis auf Diskriminierungspotenziale geprüft werden und es muss versucht werden, systematische Fehler und Verzerrung – auch auf technischem Wege – zu vermeiden; die Prinzipien der Vielfalt und Offenheit sollen in Bezug auf digitale Angebote, Infrastrukturen und Zugänge zu Netzen gelten; durch künstliche Systeme dürfen Menschen nicht vom Zugang zu Gütern, Dienstleistungen oder von der Teilhabe am gesellschaftlichen Leben ausgeschlossen werden; Menschen, die von Entscheidungen künstlicher Systeme in Bezug auf ihre Lebensführung erheblich betroffen sind, sollen einen Anspruch auf unabhängige Überprüfung und Entscheidung durch Menschen haben.

Nachhaltigkeit: Produzent*innen, Anbieter*innen und Betreiber*innen digitaler Produkte, Dienste und Infrastrukturen sollen nachhaltig wirtschaften; sie sollen dafür sorgen, dass künstliche Systeme für eine Emissionsreduktion und Ressourceneinsparung dienen sowie den Konsum nicht weiter anheizen; die Digitalisierung der Lebensräume (smarte Städte, Häuser, autonome Fahrzeuge etc.) soll nachhaltig gestaltet werden; der Lebenszyklus digitaler Geräte und vor allem deren Software sollen verlängert und deren Produktion und Entsorgung mitgedacht werden.

Verantwortung: Die Einflüsse der Technik auf die Handlungen, das Denken und die Gewohnheiten des Menschen sollten Entwickler*innen und Betreiber*innen künstlicher Systeme bewusst sein, denn Technikgestaltung ist auch Gesellschaftsgestaltung; Betreiber*innen meinungsbildungsrelevanter Plattformen tragen Verantwortung für die Verbreitung von Inhalten, die dar-

auf abzielen, antisoziales Verhalten zu fördern und den sozialen Zusammenhalt zu untergraben, wie zum Beispiel durch Online-Gewalt, Desinformation und Manipulation; einer zunehmenden Verantwortungsdiffusion der Akteure bei künstlichen Systemen ist entgegenzuwirken; Entscheidungen künstlicher Systeme müssen von natürlichen und juristischen Personen verantwortet werden; Nutzer*innen müssen durch Bildung und Digitalkompetenz dabei unterstützt werden, digitale Dienste zur Kommunikation, Information und Unterhaltung verantwortungsvoll zu nutzen.

Wahrheit und Wahrhaftigkeit: Wahrheit und Wahrhaftigkeit sind substanzielle Werte einer gut informierten Gesellschaft; Betreiber*innen digitaler Dienste und Plattformen müssen dafür sorgen, dass alle Formen absichtlich erstellter und weitergegebener Desinformationen (zum Beispiel Verschwörungserzählungen, sogenannte Fake News, manipulierte Fotos und Videos), die das Publikum täuschen und irreführen sollen, nicht verbreitet werden; der Gefahr, durch Social Bots (Computerprogramme, die mit eigenen Accounts und Profilen das Verhalten von echten Nutzer*innen simulieren) bestimmte Meinungen massenhaft zu verbreiten und die Stimmung in sozialen Medien zu lenken, ist entgegenzuwirken.

Sicherheit: Die Unversehrtheit, Vertraulichkeit und Integrität künstlicher Systeme und Infrastrukturen ist sicherzustellen und angemessen technisch und organisatorisch zu gewährleisten; Systemkompatibilität und die Handhabung der Technik unter realen Bedingungen sollten bereits in der Entwicklungsphase beachtet werden, um keine unnötigen Fehlerquellen entstehen zu lassen; es sollte fortlaufend überprüft werden, wie sich die Zwecke verändern, für welche die Technik entwickelt wird; es sollte mitgedacht werden, wie die Technik zweckentfremdet angewandt werden kann und ob dies bestimmte vorsorgliche Gegenmaßnahmen notwendig macht; Unternehmen sollen auch nicht vor der Überlegung zurückschrecken, unter Umständen bestimmte Möglichkeiten zu beschränken.

Demokratieverträglichkeit: Der Fortschritt in der Digitalisierung darf nicht die Grundrechte und demokratischen Prinzipien aushebeln; die durch die Digitalisierung hervorgerufenen Machtverschiebungen zwischen einzelner Person, Staat und Unternehmen sind einer kritischen Reflexion zu unterziehen; antidemokratischen Kräften, die die Digitalisierung zu ihren Gunsten nutzen, müssen politische Entscheidungsträger*innen durch die Förderung aufklärender Bildungsangebote, Forschung und zivilgesellschaftlichen Engagements konsequent entgegentreten.

Vertrauen: Die Gestaltung von Vertrauen und der Aufbau von vertrauensvollen Beziehungen zwischen Menschen und künstlichen Systemen sind die wesentlichen Voraussetzungen für die Akzeptanz neuer Technologien und für eine erfolgreiche Mensch-Maschine-Interaktion; ein zu eng gefasster Vertrauensbegriff, der sich nur auf eine simple Berechenbarkeit bezieht, ist für das sensible Thema *Vertrauen* in der Mensch-Maschine-Interaktion problematisch; Vertrauen in künstliche Systeme kann nur erzielt werden, wenn die oben genannten zehn Werte als normative Standards umgesetzt werden.

2.3 Risiken

Mit der Beschreibung der Werte-Topografie, die eine Konkretisierung der Werte in normative Vorgaben beinhaltet, wurde implizit bereits auf verschiedene Risiken eingegangen. Zur Übersicht und in Ergänzung lassen sich folgende Risiken identifizieren, die mit der Entwicklung, Gestaltung sowie ökonomischen und gegebenenfalls politischen Zielsetzung digitaler Technologien verbunden sind: die Risiken der *Manipulation* im Informationsbereich (Stichwort »Desinformation«), der *Machtasymmetrie* von Nutzer*innen und Anbieter*innen (Stichworte »intransparente Datenverwertung«, »Abhängigkeit der Nutzer*innen von Intermediären«) und der *Heteronomie* (fehlende Selbstbestimmung, wenn künstliche Systeme zum Beispiel über Kreditvergabe, Prämien oder Jobs entscheiden). *Überwachung* von staatlicher Seite und durch Wirtschaftsunternehmen ist ein weiterer Risiko-Topos. Neben diesen systembezogenen Risiken, die ökonomisch und politisch begründet sind und regulierbar wären, haben wir es auch mit primär technologiebezogenen Risiken zu tun, die die Notwendigkeit einer Technikfolgenabschätzung, Ethics by Design und einer nachhaltigen Digitalökologie verdeutlichen. Zu letzteren Risiken gehören neben den Problemen des Dual-Use (nicht-intendierte Verwendung von Techniken) und der Bias (Verzerrungen) auch das in der Öffentlichkeit kaum beachtete Thema *klima- und ressourcenschädlicher Digitalsektor*. Die hierzu bislang wenigen Befunde lassen vermuten, dass der Energiebedarf von Netzwerken und Datenzentren zur Speicherung und Auslieferung von Inhalten, beim Streaming von Videos und deren Produktion, nicht zuletzt auch bei der Entsorgung der Geräte für einen rapide wachsenden Anteil der weltweiten Emissionen von Treibhausgasen mitverantwortlich ist (Rebound-Effekt). Gegen die Flut der Ignoranz solcher Risiken können auf ethischer Ebene eine reflektierte Haltung von Entscheider*innen und Nutzer*innen, eine ernst gemeinte Selbstverpflichtung von Unternehmen in Form von ethischen Leitli-

nien und die Bereitschaft, Ethics by Design konsequent umzusetzen, hilfreich sein.

Des Weiteren gilt es, die Schnittstellen zwischen Recht und Ethik[49] zu verdeutlichen und diese durch interdisziplinäre Zusammenarbeit fruchtbar zu gestalten. Ethik und Recht sind miteinander verbunden und haben gemeinsame Wurzeln, dennoch existieren beide Disziplinen auch vollkommen unabhängig voneinander. Ethik ist ein grundlegendes Analyseinstrument, das Begründungs- und Bewertungsstrategien aufzeigen kann, die unterschiedliche Normen und Wertesysteme jenseits des geltenden Rechts als Basis haben können. Ethik dient dazu, Motive des Handelns sichtbar und verständlich zu machen und kann aus der Analyse heraus deshalb auch eigene normative Vorgaben entwickeln. Deren Gültigkeit zielt jedoch nur auf die freiwillige Umsetzung.

3 Ansätze für eine Digitale Ethik

Aufgabe der Ethik ist es, zu *begründen*, warum etwas gut oder schlecht ist. Ethik kann somit als *Reflexionstheorie der Moral* beschrieben werden, die nach guten Argumenten für das ethische Handeln sucht. Der Standardauffassung zufolge lassen sich drei ethische Ansätze unterscheiden, die je nach Perspektive andere Schwerpunkte der ethischen Reflexion setzen. So lenkt der (1) Konsequentialismus unseren Blick auf den ethischen Nutzen und die Folgen digitaler Technologien, während die (2) deontologische Perspektive (griech. *deon*, »Pflicht«, hier also etwa: eine Sichtweise, die aus Pflichten Aussagen ableitet) uns auf moralische Prinzipien, wie zum Beispiel das der Verantwortung, und auf die Notwendigkeit, Werte abzuwägen, verweist. Die (3) tugendethische beziehungsweise eudämonistische Perspektive (griech. *eudaimonía* »Glück« oder »Glückseligkeit«) fokussiert hingegen die Frage nach dem guten, gelingenden Leben. Wie können diese Ansätze für eine Ethik des Digitalen hilfreich sein? Beginnen wir mit der konsequentialistischen Ethik.

49 Siehe hierzu auch den Beitrag von Timo Rademacher und Erik Schilling und den Beitrag von Erik Hilgendorf in diesem Band.

3.1 Konsequentialistische Ethik

Für sie ergibt sich das moralisch Richtige einer Handlung aus den *Folgen* einer Handlung, nicht aus der Pflicht, nach bestimmten Prinzipien beziehungsweise moralischen Regeln zu handeln. Ziel des Konsequentialismus ist es, für eine größtmögliche Anzahl von Menschen einen Nutzen zu erzielen – Wohlstand, Glück, Gesundheit und dergleichen. Der wichtigste Vertreter des Konsequentialismus ist der Utilitarismus (von lat. »nützlich«). Für die klassischen Utilitaristen des 19. Jahrhunderts, Jeremy Bentham und John Stuart Mill, sollen Individuen diejenige Handlungsweise wählen, die ihnen dazu verhilft, das größtmögliche Glück zu erreichen. Moderne Vertreter attestieren dem Utilitarismus eine Überlegenheit über deontologische Ansätze, da er anpassungsfähig an den sozialen und technischen Wandel sei und nicht an überholten deontologischen Normen festhalte.[50] Das überzeugt, soweit es um Dogmatismus und die Ignoranz lebensweltlicher Kontexte geht. Andererseits ist das Nützlichkeits- und Maximierungsprinzip sehr gut mit neoliberalem Leistungs- und Effizienzdenken, materiellem Glücksversprechen, Quantifizierung des Selbst und des Sozialen[51] sowie der Ökonomisierung von Wertesystemen[52] kompatibel. Ebenso ist es dem Utilitarismus bereits mit Adam Smith im 18. Jahrhundert gelungen, den individuellen Egoismus als Stärke für das Gemeinwohl zu begründen, wonach das Allgemeinwohl umso größer ist, je stärker die Individuen nach ihren eigenen Interessen handeln: »Nicht vom Wohlwollen des Metzgers, Brauers und Bäckers erwarten wir das, was wir zum Essen brauchen, sondern davon, daß sie ihre eigenen Interessen wahrnehmen.«[53] Auch wenn diese Sichtweise auf den ersten Blick ethisch fraglich erscheint, ist bei näherer Betrachtung nicht zu ignorieren, dass sie auch für die ethische Praxis unternehmerischen Handelns von Bedeutung ist. Denn Anreize für ethisches Handeln werden Unternehmen letztlich immer aus der ökonomischen Logik ableiten: Nur wenn sich Moral rechnet und dabei hilft, zum Beispiel Vertrauen zu schaffen, Mitarbeiter*innen zu motivieren, Image-Schaden abzuwenden etc., ist sie für Unternehmen attraktiv.

---

50 Vgl. Birnbacher, Dirk: Analytische Einführung in die Ethik, 2003, S. 174-175.

51 Vgl. Mau, Steffen: Das metrische Wir. Über die Quantifizierung des Sozialen, Berlin: Suhrkamp 2017.

52 Vgl. Grimm, Petra/Zöllner, Oliver (Hg.): Ökonomisierung der Wertesysteme. Der Geist der Effizienz im mediatisierten Alltag, Medienethik Band 14, Stuttgart: Steiner Verlag 2015.

53 Smith, Adam: Der Wohlstand der Nationen, München: dtv 1990 (1776), S. 17.

Was die Leistungskraft des Utilitarismus hinsichtlich einer Ethik der Digitalisierung betrifft, lassen sich Stärken und Schwächen erkennen: 1) Eine Stärke des Utilitarismus ist es, den Blick auf die Folgen der Digitalisierung zu lenken. Mit der Technikfolgenabschätzung rückt die konsequentialistische Ethik in das Zentrum der ethischen Reflexion,[54] auch wenn das nicht bedeutet, dass jede Technikfolgenabschätzung aus der Perspektive einer konsequentialistischen Ethik erfolgt. Auch ethische Leitlinien zu künstlichen Systemen nehmen die Folgen in den Blick, indem sie als Handlungsmaximen benennen, Schaden zu verhindern und Wohlergehen zu fördern; sie schließen aber auch Prinzipien mit ein, wenn beispielsweise die Menschenwürde und die Autonomie gewahrt werden sollen. 2) Schwächen werden dem Utilitarismus andererseits gerade wegen einer mangelnden Folgenabschätzbarkeit bei schwer kalkulierbaren Folgen neuer Technologien attestiert. So lautet die Kritik, dass er nicht aufzeigen könne, *welche* Handlungsweise das größtmögliche Glück oder den geringsten Schaden verspreche.[55] Zudem sei in einer komplexen, nicht stabilen Welt schwer zu entscheiden, was Glück und Unglück bedeuten.[56] 3) Eine Stärke wiederum wird ihm bescheinigt, wenn es um die Frage nach der moralischen Programmierbarkeit von künstlichen Systemen geht. Vorausgesetzt, man hält eine Implementation moralischer Fähigkeiten in künstliche Systeme für vertretbar und sinnhaft, scheint der Utilitarismus ein geeigneter Kandidat für eine etwaige Programmierung von Regeln zu sein. Er gewährleistet »die Maximierung des Gesamtnutzens am besten durch die Aufstellung gewisser Regeln«.[57]

Ist die utilitaristische Ethik auch für die oben erzählten Fallgeschichten, die für die Diagnose der Spannungsfelder dienten, als ethischer Ansatz tauglich? Für die Geschichte (1) von Alex hilft er nicht, denn hier geht es um die Motive und die Wertekonflikte des Protagonisten. Für die zweite Geschichte (2) der Seniorin Ingeburg K. kann er hingegen hilfreich sein. Denn hier wird nach den Folgen der Installation des künstlichen Systems gefragt und danach, ob eine größtmögliche Zahl von Menschen davon profitiert. Der Fokus liegt auf der individuellen und sozialen Situation von Ingeburg K. sowie

54 Vgl. Decker, Michael: *Technikfolgen*, in: Armin Grunwald (Hg.): Handbuch Technikethik, Stuttgart/Weimar: J. B. Metzler 2013, S. 36.

55 Vgl. Vallor, Shannon: Technology and the Virtues. A Philosophical Guide to a Future Worth Wanting, New York: Oxford University Press 2016, S. 7.

56 Vgl. Boddington, Paula: Towards a Code of Ethics for Artificial Intelligence, Cham: Springer 2017, S. 69.

57 Misselhorn , Catrin: Grundfragen der Maschinenethik, 2018, S. 101.

der Beteiligten (Pflegende, Zugehörige). Ihr Glück oder Unglück könnte gegebenenfalls aber dem Nutzen der Versicherung und Beitragszahler*innen nachgeordnet sein. Wie der Nutzen selbst zu bewerten ist und inwieweit das Maximierungsprinzip überhaupt als Bewertungsgrundlage gelten soll, bleibt dahingestellt. Bei der Fallgeschichte (3) von Louise und Ann-Kathrin steht die Frage nach der ethischen Gestaltung eines künstlichen Bewerbungssystems im Vordergrund. Lässt sich in das System Moral implementieren? Das ist bei künstlichen Systemen umstritten. So scheint zwar eine Programmierung, die auf den größten Nutzen ausgerichtet ist, leichter umsetzbar zu sein als eine deontologische Programmierung, aber wollen wir das? Bei dieser Fallgeschichte (wie auch bei vielen Anwendungen von künstlichen Systemen) geht es ja vor allem um moralische Prinzipien wie *Gleichheit* und *Gerechtigkeit*, die mit dem Konsequentialismus häufig schwer begründet werden können. Bias in künstlichen Systemen können zu Ungerechtigkeiten und Benachteiligung führen, dies ist vor allem bei einer *evidenzbasierten* Gerechtigkeit des größten Nutzens der Fall.

Ein Beispiel, das die utilitaristische Perspektive veranschaulicht, ist das bekannte »Moral Machine Experiment« des MIT[58] zum autonomen Fahren, das auf das in der Ethik und im Recht vielfach besprochene Trolley-Problem[59] zurückgeht. Ein Weichensteller muss sich zwischen den Handlungsoptionen Nichts-Tun und Weichen umstellen entscheiden und muss dabei jeweils den Tod mehrerer Menschen abwägen. Aus utilitaristischer Sicht wäre die Aktionsvorgabe relativ leicht zu programmieren: Demnach wäre die »Lösung« des geringsten Schadens zu favorisieren, also zum Beispiel, dass das autonome Fahrzeug *einen* Fußgänger statt *fünf* Fußgängern überfährt, wenn es keinen anderen Ausweg gibt. So ist beim Utilitarismus »nicht jede Handlung mit gravierend schlechten Folgen […] unter allen Umständen moralisch verboten, zum Beispiel nicht dann, wenn alle verfügbaren Handlungsalternativen – einschließlich Untätigkeit – noch schlechtere Folgen hätten«.[60] Entspricht das unserem moralischen Empfinden? Anscheinend ja, wie eine aktuelle empirische Studie zum klassischen Trolley-Problem zeigt, wonach 82 Prozent der

58 moralmachine.mit.edu

59 Vgl. Wenzel, Hans: *Zum Notstandsproblem*, in: ZStW. Zeitschrift für die gesamte Strafrechtswissenschaft 63(1), 1951, S. 47-56.

60 Birnbacher, Dirk: *Utilitarismus*, in: Armin Grunwald (Hg.): Handbuch Technikethik, Stuttgart/Weimar: Metzler 2013, S. 154.

Deutschen billigen, den einen Menschen anstelle von fünf zu opfern; interessanterweise entscheiden sich in China nur 58 Prozent dafür.[61] Wäre das Ergebnis dasselbe, wenn die Person die eigene Mutter oder der Partner wäre? Aus deontologischer Sicht könnte jedenfalls die Opferung des einen Menschen nicht gebilligt werden. Diese deontologische Perspektive ist im Übrigen auch bei der bekannten Entscheidung des Bundesverfassungsgerichts zum Flugsicherheitsgesetz von 2007 zum Ausdruck gekommen, bei dem es um die Abschussfreigabe eines von Selbstmordattentätern gekaperten Flugzeugs ging. Eine Abschussfreigabe würde Menschen zu Objekten machen, sie verdinglichen und entrechtlichen, so lautete im Wesentlichen die Argumentation der Verfassungsrichter*innen. Auch aus Sicht eines digitalen Humanismus, wie ihn Julian Nida-Rümelin und Nathalie Weidenfeld beschreiben, kollidiert der konsequentialistische Ansatz mit dem »Prinzip der Nicht-Verrechenbarkeit«[62], wonach nicht das Schicksal des einen Menschen mit dem des anderen Menschen verrechnet werden darf. Hierzu gehört auch ein Menschenbild, wonach der Mensch über Willensfreiheit sowie die Fähigkeit verfügt, als Vernunftwesen wertend Stellung zu nehmen und moralische Begründungen abzuwägen: »In einem humanistischen Weltbild ist der Mensch kein Mechanismus, sondern freier (autonomer) und verantwortlicher Akteur in der Interaktion mit anderen Menschen und einer gemeinsamen sozialen und natürlichen Welt.«[63] Zu ergänzen ist hier, dass der Mensch demgemäß nicht als Konstrukt biochemischer Mechanismen, die von genetischen Programmen gesteuert werden, zu verstehen ist. Diesem technizistischen beziehungsweise szientistischen Menschenbild widerspricht das humanistische, indem es die Würde des Menschen, sein körperliches Dasein und sein Miteinander herausstellt, wie Thomas Fuchs betont: »Im Begriff der Menschenwürde, verstanden als der Anspruch auf Anerkennung, den ein menschliches Wesen durch sein leibliches Dasein und Mitsein erhebt, vereinigen sich und gipfeln die Bestimmungen, die ein humanistisches, personales Menschenbild konstituieren.«[64]

---

61 Vgl. Awad, Edmond et al.: *Universals and variations in moral decisions made in 42 countries by 70,000 participants*, in: PNAS February 4, No. 5, Vol. 117, 2020, S. 2332-2337. https://doi.org/10.1073/pnas.1911517117

62 Nida-Rümelin, Julian/Weidenfeld, Nathalie: Digitaler Humanismus. Eine Ethik für das Zeitalter der Künstlichen Intelligenz, München: Piper 2018, S. 68.

63 Ebd., S. 61.

64 Fuchs, Thomas: Verteidigung des Menschen. Grundfragen einer verkörperten Anthropologie, Berlin: Suhrkamp 2020, S. 8.

3.2 Deontologische Ethik

Die deontologische Ethik ist eine an Pflichten orientierte ethische Theorie. Im Kern geht die Pflichtenethik davon aus, dass bestimmte Handlungen geboten oder verboten sind, unabhängig davon, welche Folgen damit verknüpft sind. Bezeichnend für die Deontologie ist der Verallgemeinerungs- beziehungsweise Universalisierungsanspruch von Rechten und Pflichten. Demnach gibt es Rechte, die für alle Menschen bindend sind, beispielsweise die in der Allgemeinen Erklärung der Menschenrechte. Für die Pflichtenethik Kants steht nicht das Glück oder dessen Maximierung, sondern das Richtige (*was soll ich tun?*) im Zentrum seiner Ethik. Sein Universalisierungsanspruch an das Sollen bringt der kategorische Imperativ zum Ausdruck: »Handle nur nach derjenigen Maxime, durch die du zugleich wollen kannst, dass sie ein allgemeines Gesetz werde.«[65] Damit veranlasst er uns, das eigene Handeln über unsere subjektive Sicht hinaus in Hinblick auf das allgemeine Ganze zu betrachten. Kants wirksames Vermächtnis besteht darin, dass er die Autonomie des Menschen als ethische Leitidee formuliert hat. Demnach »bedeutet individuelle Autonomie die Fähigkeit oder das Vermögen, sich selbst die Gesetze geben zu können, nach denen wir handeln und die wir selbst für richtig halten«[66]. Nach seinem Verständnis sind wir »autonom, frei, […] dann und nur dann, wenn wir auch moralisch sind und handeln«.[67] Autonomie ist an die eigene praktische Vernunft gebunden sowie an die Achtung der Würde des Menschen (die eigene und die des anderen): »Handle so, dass du die Menschheit, sowohl in deiner Person als in der Person eines jeden anderen, jederzeit zugleich als Zweck, niemals bloß als Mittel brauchest.«[68] Wenngleich Kants moralischer Autonomiebegriff in modernen ethischen Ansätzen durch ein personales Konzept ersetzt wurde, ist er für die Diskussion fruchtbar, ob künstliche Systeme (irgendwann) als autonom im ethischen Sinn gelten können. Angenommen, es gäbe ein künstliches System, wie zum Beispiel »Ava« in dem Film *Ex Machina*[69], die zwar über einen freien Willen verfügt, aber für ihre Befreiung andere instrumentalisiert, manipuliert und tötet. Zwar ist »Ava« nun frei

65 Kant, Immanuel: Grundlegung zur Metaphysik der Sitten. Mit einer Einleitung hg. v. Bernd Kraft und Dieter Schönecker, Hamburg: Felix Meiner Verlag 1999 [1785], S. 61.

66 Rössler, Beate: Autonomie. Ein Versuch über das gelungene Leben, Berlin: Suhrkamp 2017, S. 31.

67 Ebd., S. 32.

68 Kant, Immanuel: Grundlegung zur Metaphysik der Sitten 1999 [1785], S. 54-55.

69 GB 2015, Regie.: Alex Garland.

und autonom, aber verfügt sie über *moralische* Autonomie? Künstliche Systeme sind aus Sicht einer kantischen Ethik nicht autonom und lassen sich auch nicht moralisch gestalten. Kants Ethik in künstliche Systeme zu implementieren »widerspräche […] dem Geist der kantischen Moral«[70].

Für eine Ethik der Digitalisierung ist die Frage nach der moralischen Autonomie der Dreh- und Angelpunkt bei der Bewertung künstlicher Systeme. Aus rein funktionaler Sicht kann man künstlichen Systemen eine basale beziehungsweise funktionale Autonomie unterstellen,[71] wobei die genuin menschlichen Fähigkeiten, wie Bewusstsein, freier Wille, Intentionalität und Verantwortung, den künstlichen Systemen (bislang) abgesprochen werden. Dennoch tendieren wir dazu, allein schon in terminologischer Hinsicht künstliche Intelligenz mit menschlichen Eigenschaften zu beschreiben. Für eine Einordnung bedarf es gleichwohl auch der kritischen Auseinandersetzung mit Begriffen. Eine Analyse[72] der gängigsten Definitionen von künstlicher Intelligenz zeigt, dass sie fast immer mit Attributen beschrieben wird, die diese vermenschlicht: Es ist von »lernen«, »verstehen«, »entscheiden«, »wahrnehmen« und »Probleme lösen« die Rede. Künstliche Intelligenz wird also definitorisch anthropomorphisiert oder es wird ihr zumindest »Menschenähnlichkeit« attestiert. Der Begriff suggeriert, dass eine dem Menschen vergleichbare Intelligenz existiert. Das ist allerdings nicht der Fall. Bewusstsein und Gefühle sind Charakteristika, die bislang Lebewesen vorbehalten sind. Auch wenn unklar ist, wie Bewusstsein entsteht und was Bewusstsein eigentlich ist, kann derzeit nicht davon ausgegangen werden, dass künstliche Systeme zur Selbstreflexion fähig sind und ein »Ich«, also eine eigene Identität, ausbilden können. Noch viel weniger sind sie in der Lage, unbewusst etwas zu verdrängen, wie es der Mensch nur allzu gerne tut. Auch über Emotionen verfügen künstliche Systeme nicht, wenngleich sie zu deren Imitation bereits fähig sind. Sie haben auch keinen freien Willen und biologischen Körper. Sie verarbeiten zwar selbstständig Daten, was als sogenanntes

70 Misselhorn, Catrin: Grundfragen der Maschinenethik, 2018, S. 108.

71 Vgl. Floridi, Luciano/Sanders, Jeff W.: *On the Morality of Artificial Agents*, in: Minds and Machines, Vol. 14, No. 3, 2004, S. 357; Wallach, Wendell/Allen, Collin: Moral Machines. Teaching Robots Right from Wrong, 2009, S. 26-32; sowie eine Übersicht in Loh, Janina: Roboterethik. Eine Einführung, 2019b, S. 73.

72 Die Analyse erfolgte im Rahmen des BMBF-Forschungsprojekts »Automatisiertes ELSI-Screening & Assessment-Tool für MTI-Forschungsvorhaben (ELSI-SAT)«, https://www.elsi-sat.de/

maschinelles Lernen beschrieben wird, aber sie lernen nicht wie wir Menschen, die im sozialen Miteinander, aus der Erfahrung von Freude und Leid und aus Vernunftgründen lernen. Maschinen sind (bislang) auch keine Generalisten, sondern Spezialisten – sie können (zumindest bislang) nicht wie der Mensch gleichzeitig über verschiedene Fähigkeiten verfügen, also sich ein Kochrezept ausdenken, eine Oma trösten, ein Musikstück komponieren und ein Bild malen. Sie können nicht moralische Prinzipien erkennen, auf sich selbst anwenden und moralisch aufgrund ihres Gewissens handeln. Maschinen haben kein Gewissen und können keine Verantwortung übernehmen. Aber ganz wesentlich ist: Menschen sind zur Autonomie befähigt, während Maschinen nur autonom Informationen verarbeiten. Autonom ist die KI erst dann, wenn sie nicht mehr auszuschalten ist. Eine beeindruckend dezidierte Analyse zur Unterscheidung von menschlicher und künstlicher Intelligenz legt Thomas Fuchs vor, dessen Fazit lautet: »Sicher, die Bezeichnung ›künstliche Intelligenz‹ ist wohl nicht mehr aus der Welt zu schaffen. Doch wir sollten uns immer dessen bewusst bleiben, dass zwischen den Rechen- und Anpassungsleistungen eines Computersystems und den Wahrnehmungen, den Einsichten, dem Denken und Verständnis eines Menschen nicht nur ein gradueller, sondern ein fundamentaler Unterschied besteht.«[73]

Die Stärken und Schwächen des deontologischen Ansatzes können hier nur ansatzweise skizziert werden. Eine Stärke ist sicherlich, dass die Pflichtenethik für die Erstellung von ethischen Leitlinien zu künstlichen Systemen ein Begründungskonzept bieten kann – zumindest wenn der Anspruch besteht, über eine minimalistische Forderung der Schadensvermeidung (im Sinne des Utilitarismus) hinauszugehen. Als normative Ethik, die handlungsleitend ist, kann sie dabei helfen, das Richtige zu begründen und dessen Universalisierbarkeit zu prüfen. Problematisch ist natürlich, wenn ethische Leitlinien, die ja eine Form von freiwilliger Selbstverpflichtung darstellen, von Unternehmen nicht in der Praxis umgesetzt werden und womöglich im Sinne eines Ethics-Washing missbraucht werden und/oder gar zur Abwendung von rechtlichen Konsequenzen dienen sollen. So kritisiert beispielsweise AlgorithmWatch, dass Facebook und Google nicht die vom weltweiten Fachverband für Ingenieur*innen IEEE herausgegebenen Grundsätze zu automatisierten

73 Fuchs,Thomas: Verteidigung des Menschen. Grundfragen einer verkörperten Anthropologie, 2020, S. 51.

Systemen umsetzen oder staatliche Regulatoren Werte nicht mit Leben füllen beziehungsweise Rechte leerlaufen lassen.[74]

Aus Sicht der Deontologie setzen unsere Werte und Entwürfe des Guten gerechtfertigte moralische Prinzipien voraus. Bezogen auf die Fallgeschichte (1) zur Privatsphäre könnte man deontologisch argumentieren, dass Alex seine Privatsphäre schützen soll, weil sie durch das Autonomieprinzip, auf dem unsere demokratische Gesellschaft fußt, begründet ist. Privatheit ist eine notwendige Voraussetzung für und Ausdruck von Autonomie. Wenn es zu einer Relativierung der Privatheit käme, indem sich das Selbstverständnis von Personen hinsichtlich der Relevanz und Schutzwürdigkeit der Privatheit ändere, würde dies nach Rösslers Einschätzung auch das Fundament unserer Demokratie erbeben lassen: »Dies trifft dann nicht nur die Idee eines gelungenen – selbstbestimmten – Lebens, sondern auch die Idee der liberalen Demokratie: die nämlich auf autonome und sich ihrer Autonomie bewusste und diese schätzende Subjekte angewiesen ist.«[75]

Für die Fallgeschichte (2) der pflegebedürftigen Seniorin kann die deontologische Ethik ebenfalls Anknüpfungspunkte liefern. So werden in der Charta der Rechte hilfe- und pflegebedürftiger Menschen[76] und im ICN-Ethikkodex für Pflegende[77] die Prinzipien einer guten Pflege dargelegt. Letzterer begründet in der Präambel die Aufgaben von Pflege (»Gesundheit zu fördern, Krankheit zu verhüten, Gesundheit wiederherzustellen, Leiden zu lindern«) durch universale Rechte: »Untrennbar von Pflege ist die Achtung der Menschenrechte, einschließlich kultureller Rechte, des Rechts auf Leben und Entscheidungsfreiheit, auf Würde und auf respektvolle Behandlung.«[78] Der Deutsche Ethikrat legt in seiner Stellungnahme zur Robotik in der Pflege[79] ausführlich dar, unter welchen Voraussetzungen ein ethisch verantwortlicher Einsatz von Robotik beziehungsweise technischer Assistenzsysteme möglich erscheint.

74 Vgl. Kayser-Bril, Nicolas: Ethische Richtlinien des größten Weltverbands zeigen kaum Wirkung, 2019. https://algorithmwatch.org/story/ethische-richtlinien-von-ieee-ohne-wirkung/

75 Rössler, Beate: Der Wert des Privaten, 2001, S. 218.

76 Bundesministerium für Familie, Senioren, Frauen und Jugend (Hg.): Charta der Rechte hilfe- und pflegebedürftiger Menschen (13. Aufl.), Berlin 2019.

77 Deutscher Berufsverband für Pflegeberufe (Hg.): ICN-Ethikkodex für Pflegende. Berlin 2014.

78 Ebd., S. 1.

79 Deutscher Ethikrat: Robotik für gute Pflege. Berlin 2020. https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-robotik-fuer-gute-pflege.pdf

Dieses begründet er im Wesentlichen aus einer deontologischen Perspektive.

Für die Fallgeschichte (3) der automatisierten Jobbewerbung könnte die deontologische Ethik ebenfalls normativ Anforderungen an die Programmierer*innen des künstlichen Systems stellen, wie zum Beispiel die Einhaltung des Rechts auf Chancengleichheit, der Geschlechtergerechtigkeit und Nicht-Diskriminierung. Die Frage, wie diese dann in der Praxis umgesetzt werden sollen, kann die Deontologie allerdings nicht beantworten. Und damit kommen wir zum Ansatz der Tugendethik.

3.3 Tugendethik

Während die deontologische Ethik auf die Frage *Was soll ich tun?* verkürzt werden kann, lautet die Frage der Tugendethik *Worin besteht das gute Leben?*. Für die aktuelle Tugendethik dient die Ethik des Aristoteles als Vorbild, wonach das Streben des Menschen nach Glück (*eudaimonia*) die Ausbildung von Tugenden beinhaltet. In der aristotelischen Ethik steht der Handelnde und seine Haltung im Vordergrund, erst durch die richtige Haltung wird eine Handlung zur richtigen. Der aristotelische Haltungsbegriff *hexis* lässt sich als Tugend und Charakterzug verstehen, die auf einer freien Wahl und Beurteilung beruhen.[80] Für Aristoteles erweist sich Haltung im Handeln und zielt auf den Umgang mit Affekten und Emotionen. Haltung erlangt man, indem man diese einübt und den Weg der Mitte zwischen einem Zuviel und einem Zuwenig, wie zum Beispiel Tapferkeit anstelle von Feigheit oder Draufgängertum, als das richtige und angemessene Verhalten erkennt und wählt. Eine Haltung ist uns aber nicht von Natur aus gegeben, sie muss aktiv und in konkreten Handlungen ausgebildet werden: »Hexis/Haltung hat mit Gewöhnung (ethos) insofern zu tun, als sich in ihr die Geschichte wiederholter Handlungen abzeichnet.«[81] Haltung wäre in diesem Verständnis ein dynamisches Konzept, das sich im Laufe der Zeit in die Grunddisposition eines Menschen einschreibt. Weitergedacht sind mit einer Haltung auch reflexive Fragen verbunden, die

80 Aristoteles: Nikomachische Ethik. Übersetzung und Nachwort von Franz Dirlmeier. Anmerkungen von Ernst A. Schmidt, Stuttgart: Reclam 2015, S. 34-52.

81 Wild, Thomas: *Was wissen wir von Haltung? Eine kleine enzyklopädische Suche*, in: Frauke Kurbacher /Philipp Wünschner (Hg.): Was ist Haltung? Begriffsbestimmung, Positionen, Anschlüsse, Würzburg: Königshausen und Neumann 2017, S. 95.

sich das Handlungssubjekt in Bezug auf ein Objekt stellt: Was halte ich persönlich von etwas? Wie soll ich mich verhalten? Und warum so und nicht anders?

Neoaristotelische Ansätze zeichnen sich dadurch aus, dass sie die Fähigkeiten und Kompetenzen der Menschen in den Blick nehmen. Als Gerüst für eine Ethik der Digitalisierung lenken sie damit den Fokus auf die Digitalkompetenzen der Nutzer*innen im Umgang mit und in der Einschätzung von digitalen Medien und künstlichen Systemen. *Digitalkompetenz* ist dann mehr als nur ein technisches Befähigungskonzept, es ist auch ein ethisches, das ein gutes Leben in einer digitalen Welt zum Ziel hat. Hierzu sind allerdings auch die politischen Rahmenbedingungen entsprechend zu gestalten, die es braucht, um bestimmte Fähigkeiten auszubilden. Gemäß Aristoteles muss der Staat das gemeinschaftliche Streben nach einem guten Leben ermöglichen. So könnte man sagen: Fähig kann nur jemand sein, der oder die dazu befähigt wird.

Nach Martha Nußbaum zeichnet die aristotelische Ethik außerdem ihre Offenheit für Veränderungen der »konkreten historischen und kulturellen Bedingungen« aus sowie ihr universales »Bild vom menschlichen Leben, seinen Bedürfnissen und Möglichkeiten«.[82] Nußbaums Fähigkeiten-Ansatz (Capability Approach),[83] den sie zusammen mit Amartya Sen entwickelt hat, ist vielversprechend für eine Digitale Ethik. Denn mit ihm lässt sich das Vorhaben einer wertegestalteten Digitalisierung vorantreiben, die die grundlegenden Bedürfnisse des Menschen im digitalen Zeitalter in den Mittelpunkt stellt. Im Bereich der Pflege gilt der Fähigkeiten-Ansatz bereits als geeignetes Framework für die Gestaltung von Robotern.[84] Nußbaums Liste der zentralen menschlichen Bedürfnisse für ein gutes Leben werden hier zugrunde gelegt, wie unter anderem körperliche Unversehrtheit, Gesundheit, emotionale Beziehungen, Kontrolle über die eigene Umwelt.[85] Den Fähigkeiten-Ansatz auch

82 Nußbaum, Martha: *Nicht-relative Tugenden: Ein aristotelischer Ansatz*, in: Klaus Peter Rippe/Peter Schaber (Hg.): Tugendethik, Stuttgart: Reclam 1998, S. 144.

83 Nußbaum, Martha: Fähigkeiten schaffen. Neue Wege zur Verbesserung menschlicher Lebensqualität. Aus dem Amerikanischen von Veit Friemert, München: Karl Alber Verlag 2015.

84 Vgl. Borenstein, Jason/Pearson, Yvette: *Robot Caregivers: Ethical Issues across the Human Lifespan*, in: Patrick Lin/Keth Abney/George A. Bekey (Hg.): Robot Ethics. The Ethical and Social Implications of Robotics, Cambridge, London: MIT Press 2014, S. 254.

85 Nußbaum, Martha: Fähigkeiten schaffen. Neue Wege zur Verbesserung menschlicher Lebensqualität, 2011, S. 41-42.

auf andere Bereich der Digitalisierung zu erweitern, ist ein noch zu erfüllendes Desiderat.

Erste Ansätze einer explizit technikbezogenen Tugendethik (Technomoral Virtue Ethics) hat Shannon Vallor vorgelegt. Mit Rückbezug auf eine aristotelische, buddhistische und konfuzianische Ethik schlägt sie eine (erweiterbare) Taxonomie technomoralischer Tugenden vor, die für ein gutes Leben in der digitalen Welt erforderlich seien: Ehrlichkeit, Selbstkontrolle, Demut, Gerechtigkeit, Mut, Empathie, Fürsorge, Zivilität (wie Respekt, Toleranz), Flexibilität, Einsichtsvermögen, Großmut (*magnanimity*), technomoralische Weisheit.[86] Diesen Tugenden ordnet sie wiederum weitere Sekundärtugenden zu. Ihr tugendethischer Ansatz ist vor allem aufgrund seiner interkulturellen Perspektive für eine globale Ethik der Digitalisierung vielversprechend.

Betrachtet man wiederum die drei Fallgeschichten, dann weist die (neo-)aristotelische Ethik ebenfalls Stärken und Schwächen auf. Für die Interpretation der Fallgeschichte (1) von Alex helfen der tugendethische und der Fähigkeiten-Ansatz, da es hier ja um ein mutiges, kluges und besonnenes Handeln sowie eine Haltung zum Wert der Privatheit geht. Die aristotelische Ethik ist durch ihren Praxisbezug genuin definiert. So betont Aristoteles mehrfach, dass man nicht durch das Philosophieren eine Haltung ausbildet, sondern durch ständiges Einüben: mutig durch mutiges Handeln, besonnen durch besonnenes Handeln. Die eigene Privatheit und die der anderen (zum Beispiel Kinder) zu schützen, setzt einerseits die individuelle Ausbildung einer Privatheitskompetenz[87] voraus und andererseits die politische Sicherstellung entsprechender Rahmenbedingungen, um Privatheit überhaupt schützen zu *können*. Auf diesen Zusammenhang von Fähigkeit und Befähigung weist auch der Capability Approach hin. Wie Alex seinen Wertekonflikt (Privatheit schützen oder Freundschaften pflegen) lösen soll, kann mit Aristoteles schwer begründet werden. Wenngleich auch bei Kant wenig zu den Pflichtenkonflikten zu finden ist, »räumt er im Konfliktfall dem stärkeren Verbindlichkeitsgrund den Vorrang vor der stärkeren Verbindlichkeit ein«.[88]

Für die Fallgeschichten (2) und (3) liefert der Fähigkeiten-Ansatz ebenfalls wichtige Erkenntnisse. So geht es jeweils um die Frage, wie in der Praxis ein

86 Vgl. Vallor, Shannon: Technology and the Virtues. A Philosophical Guide to a Future Worth Wanting, 2016, S. 119-155.

87 Vgl. Grimm, Petra/Krah, Hans: *Privatsphäre*, in: Jessica Heesen (Hg): Handbuch Medien- und Informationsethik. Stuttgart: J. B. Metzer 2016, S. 184-185.

88 Höffe, Ottfried: *Aristoteles' universalistische Tugendethik*, in: Klaus Peter Rippe/Peter Schaber (Hg.): Tugendethik 1998, S. 61.

künstliches System (das technische Assistenzsystem beziehungsweise Jobbewerbungssystem) so gestaltet werden kann, dass es den Menschen befähigt, ein gutes Leben zu führen. Die Antwort darauf ist Ethics by Design.[89] Hierbei handelt es sich um einen Ansatz in der Digitalen Ethik, der vor allem auf den Methoden und Konzepten eines Value Sensitive Design[90] beruht. Er ist ein weit aussichtsreicheres Verfahren als der Versuch, Ethik durch Programmierung zu implementieren. Denn Ethics by Design stellt die Bedürfnisse der Menschen in den Vordergrund, nicht die Codierung. In der aktuellen europäischen (und deutschen) Debatte wird dementsprechend argumentiert, dass eine wertschätzende Gestaltung – insbesondere von künstlicher Intelligenz – einen »Wettbewerbsvorteil« gegenüber der in anderen Weltregionen programmierten und entwickelten KI darstellen könnte.[91] Ethics by Design ist ein Ansatz, der ethische Überlegungen, Wertmaßstäbe, Motive oder Maximen in die vielschichtigen Prozesse der Technikgestaltung, von der ersten Produktidee bis hin zum verkaufsfertigen Endprodukt, einfließen lässt. Ethische Überlegungen sollen also von vornherein angestellt, die Diversität der Nutzer*innen berücksichtigt und Grundsätze für ethisches Handeln, beispielsweise in der Entwicklung von künstlichen Systemen, eingehalten werden. Ethics by Design beinhaltet den Gedanken, dass Probleme vermieden oder zumindest frühzeitig erörtert werden können, wenn ethische Fragen oder zum Beispiel mögliche ethische Wertekonflikte bereits zu einem frühen Zeitpunkt der Entwicklung eines künstlichen Systems berücksichtigt werden. Es handelt sich dabei nicht um eine einmalige oder punktuelle Angelegenheit. Ein künstliches System wird nicht als »einmal ethisch – immer ethisch« abgenickt, vielmehr begleitet die Reflexion die Entwicklung und ist auch nach Marktreife des künstlichen Systems nicht abgeschlossen.

Wie der Versuch einer ersten Systematisierung ethischer Ansätze zeigt, können sie unterschiedliche Perspektiven für eine wertegestaltete Digitalisierung liefern. Vom Blickwinkel einer Digitalen Ethik aus, die sich an einem humanistischen Menschenbild orientiert, braucht es allerdings mehr Entschlos-

89 Vgl. Van den Hoven, Jeroen: *The Design Turn in Applied Ethics*, in: Jeroen van den Hoven (Hg.): Designing in ethics, Cambridge: Cambridge University Press 2017, S. 11-32.

90 Vgl. Friedman, Batya/Hendry, David G.: Value Sensitive Design. Shaping Technology with Moral Imagination, Cambridge, London: The MIT Press 2019; Friedman, Batya/Hendry, David G./Borning, Alan: *A Survey of Value Sensitive Design Methods*, in: Foundations and Trends in Human Computer, Vol. 11. No. 23, 2017, S. 63-125.

91 Vgl. Hasselbalch, Gry/Tranberg, Pernille: Data Ethics: The New Competitive Advantage 2016, S. 97. https://dataethics.eu/en/book

senheit als bisher, um die Ethik in der Praxis nachhaltig zu verankern. Ein wichtiger Schritt dorthin ist es, das normative Konzept des *Gemeinwohls* für den Digitalisierungsdiskurs und die Gestaltungs- und Steuerungspolitiken fruchtbar zu machen. Dann kann auch das im einführenden Beitrag proklamierte Ziel erreicht werden, das da lautet: »Von der normativen Kraft des Faktischen zur faktischen Kraft des Normativen«.

II. Welche Werte für eine gemeinwohlorientierte Digitalisierung?

2.1 Freiheit und Autonomie

2.1.1 Freiheit

Grundrechte im digitalen Zeitalter und wie sie garantiert werden können

Ellen Ueberschär[1]

Zwischen Alarmismus und Ambivalenz

Als die Bundeskanzlerin Angela Merkel vor einigen Jahren bemerkte, dass das Internet für uns alle »Neuland« sei, prasselten höhnische Kommentare auf sie nieder. Eine ganze Reihe von Menschen fühlte sich offenbar schon recht sicher in der neuen digitalen Wirklichkeit. Bis heute lässt sich wohl nicht behaupten, dass das Internet und die Digitalisierung aller Lebensbereiche auch nur annähernd so in das menschliche Leben integriert wäre, dass die Mehrheit das Gefühl hat, hier souverän und selbstbestimmt zu agieren.

Spätestens seit Shoshana Zuboffs Standardwerk über *Das Zeitalter des Überwachungskapitalismus*[2], in dem sie die digitalisierten Verzerrungen der wirtschaftlichen, öffentlichen und menschlichen Beziehungen nachzeichnet, verstärkt sich die Wahrnehmung der Freiheitsgefährdungen durch die digitalkapitalistische Überformung. Shoshana Zuboff sieht die Grundlagen des Zusammenlebens, der Individualität und der Sozialität durch die internetbasierten Plattformökonomien bedroht. Soziales Vertrauen und Demokratie werden ausgehöhlt und machen einer freiwilligen Unterjochung der Mehrheit Platz. Inzwischen reiht sich Zuboffs generationenprägende Theorie in eine ganze Bibliothek kritischer Literatur ein.

Den mahnenden und bisweilen apokalyptisch anmutenden Prognosen zum Trotz zeigt die Mehrheit der digitalen Nutzer*innen ein Verhalten, das

1 Unter Mitarbeit von Nina Locher und Vérane Meyer.

2 Zuboff Shoshana: Das Zeitalter des Überwachungskapitalismus, Frankfurt/New York: Campus Verlag 2018, S. 22.

bestenfalls von Ambiguität geprägt ist, wenn nicht gar von Ignoranz gegenüber diesen Warnungen. Selbst hinreichend sensibilisierte Zeitgenoss*innen machen sich zwar Sorgen, nutzen aber Messengerdienste, Vermittlungsplattformen oder Apps, deren Datengebaren sie nicht gutheißen, und hinterlassen freiwillig und großzügig Datenspuren im Netz – frei nach dem »Nichts-zu-verbergen-Argument«. Im Zeitalter von Homeoffice und Videokonferenzen sind die Anbieter mit dem geringsten Datenschutzniveau diejenigen, bei denen die Technik reibungslos und nutzerfreundlich funktioniert.

Überwiegt nicht der Nutzen (Komfort) den Schaden (Rechtsbruch und Rechtsunsicherheit)? Ist es vielleicht übertrieben, vor Freiheitsberaubung zu warnen? Die Datenschutz-Grundverordnung (DSGVO), von der noch die Rede sein wird, ist bei vielen Nutzer*innen unbeliebt und in ihrem Inhalt, ihrem Ziel und ihrer Funktionsweise unbekannt. Was soll der nervige »Einverstanden«-Klick, wenn es um Cookies und Ad-Tracker geht? Für die Nutzer*innen der Angebote überwiegen die Vorteile – die gesuchte Information ist nur einen Klick weit entfernt, der gesuchte Weg ist rasch gefunden, Meinungen sind mit Freunden schnell ausgetauscht und in Corona-Zeiten ist der digitale Einkauf sogar sicherer.

Oder liegt die Ursache für das ambivalente Verhalten nicht im Abwägen von Vor- und Nachteilen, sondern ganz woanders? Fehlt uns das angemessene Sensorium, fehlen uns das Wissen und die digitale Kompetenz für diese neue Form der Bedrohung? Fehlt uns die Klugheit des Hänsels aus dem Märchen, der – im Wissen um den Ofen, in dem er verschwinden soll – der Hexe immer nur ein dünnes Stöckchen, niemals aber sein dickes Fingerchen hinstreckt? Lassen wir uns von den glänzenden Pfefferkuchen behexen, geben gutherzig unser Leben preis und bemerken den Ofen nicht?

Warum steht dem Alarmismus der wenigen die Ambiguität der vielen gegenüber? Warum ist das Bewusstsein für eine schleichende *Ent-Wertung* und Rechtlosigkeit noch wenig ausgeprägt?

Dieser Beitrag gibt Antworten. Es geht in der Digitalisierung nicht um die reparierfähige Verletzung einzelner Grundrechte, sondern um eine irreparable Beschädigung der menschlichen Würde. Es ist aber keineswegs zwangsläufig, dass die Verletzung der Würde unaufhaltsam voranschreitet. Am Ende gibt es Vorschläge für den produktiven Umgang mit der Digitalisierung.

Wenn wir das Bewusstsein für die Freiheitsgefährdungen schärfen wollen, müssen wir zunächst verstehen, was eigentlich geschieht, wer wann und wie die Würde verletzt. Zugleich brauchen wir Wissen und Klarheit über un-

sere europäische Grundrechtstradition, die zu Themen wie Überwachung, Zwang und Totalitarismus einiges zu sagen hat.

Digitale Möglichkeiten für alle

Zunächst aber soll einem möglichen Missverständnis vorgebeugt werden:

Wenn es um die Gefährdungen im digitalen Raum geht, dann sprechen wir nicht von einer Schmälerung der Chancen und Möglichkeiten für Vernetzung und Austausch. Die Wahrung der Freiheitsrechte muss nicht konzeptionell gegen fast grenzenlose Informationsmöglichkeiten, Wissenserwerb und Lebenserleichterungen, die das Netz und die digitalen Tools für viele darstellen, ausgespielt werden. Der gern propagierte Gegensatz ist keiner, wie wir noch sehen werden. Das, was ein Smartphone heute an Bedienungshilfen bietet, kostete früher mehrere Tausend Euro und musste beispielsweise für Menschen mit Einschränkungen extra angefertigt werden. Digitale Endgeräte sind ein riesiger Gewinn an Freiheit und Inklusion für alle, die auf Assistenzsysteme angewiesen sind. Die Oppositionsbewegung in Belarus wäre ohne das Internet nicht so flächendeckend aktiv, nicht so gut organisiert und vernetzt. Migrant*innen, die über das Meer flüchten, verständigen sich über das Internet, halten Kontakt untereinander und mit ihren Bezugspersonen.

Die Liste positiver Anwendungsmöglichkeiten von digitalen Technologien ließe sich unendlich verlängern, angefangen bei algorithmengestützten Diagnoseverfahren in der Medizin über ressourcenschonende vernetzte Fertigung im Anlagenbau bis zur Präzisionslandwirtschaft. Auch hier ist rechtlich nicht alles geklärt, für vieles müssen Rechtskonzepte neu interpretiert und erweitert werden. Aber solange der Wettbewerb funktioniert, die Kreativität gesteigert und der Beitrag zu einem guten Leben deutlich wird, lässt sich mit den Unsicherheiten einer technologischen Umwälzung umgehen. Wenn wir über die Freiheitsgefährdungen im digitalen Raum reden, dann müssen wir die freiheitliche, lebensförderliche Seite der Digitalisierung ins Zentrum stellen und wirksam vor Gefahren schützen.

Freiheitsgefährdungen, die digitale Möglichkeiten in ihr Gegenteil verkehren

Freiheitsgefährdungen gehen in hohem Maße aus von den Mono- und Oligopolen der unter dem Akronym GAFAM (Google, Amazon, Facebook, Apple, Microsoft) bekannten Unternehmen, die in kürzester Zeit alles Realwirtschaftliche an Börsenwert überflügelt haben. Sie sind dabei, mit ihren Geschäftsmodellen den Marktplatz, den öffentlichen Raum, die digitale Infrastruktur zu nutzen. Sie selbst stellen den digitalen öffentlichen Raum! Und können sich so beinahe des gesamten Lebens der Bürger*innen bemächtigen.

In ihrem Opus magnum über den »Überwachungskapitalismus« hat Shoshana Zuboff die Geschäftspraktiken der digitalen Industriegiganten im Rahmen ihrer Kapitalismusanalyse auseinandergenommen. Die neue Wirtschaftsform »beansprucht einseitig menschliche Erfahrung als Rohstoff zur Umwandlung in Verhaltensdaten. Ein Teil dieser Daten dient der Verbesserung von Produkten und Diensten, den Rest erklärt man zu proprietärem Verhaltensüberschuss, aus dem man mithilfe [… von] Maschinen- oder künstlicher Intelligenz […] Vorhersageprodukte fertigt. […] Und schließlich werden diese Vorhersageprodukte auf einer neuen Art von Marktplatz für Verhaltensvorhersagen gehandelt, […] dem ›Verhaltensterminkontraktmarkt‹.«[3]

Dabei aber bleibt es nicht. Menschliches Verhalten wird von den großen Plattformen nicht nur abgeschöpft, sondern angestoßen und herausgekitzelt, mit anderen Worten: manipuliert. Je mehr Daten über einzelne Individuen bekannt sind und zusammengeführt werden, umso genauer sind die Vorhersagen, umso besser lassen sie sich an andere Unternehmen verkaufen, umso mehr Geld lässt sich mit ihnen verdienen. Vorhersageprodukte sind wertvoll für Versicherungen, Dienstleistungen – und am Ende auch für den Staat, zum Beispiel die Polizei.

Während der ehrbare Kaufmann noch Ware gegen Geld tauschte, funktioniert diese Art von Geschäft über die Köpfe derer hinweg, die die Ressourcen bereitstellen. Sie sind lediglich so eine Art »Minen«, aus denen der Rohstoff gewonnen wird, später veredelt zu Vorhersageprodukten und verkauft an interessierte Unternehmen. Die Nutzer*innen der Dienste von Google, Microsoft, Amazon und Co. sind nicht einmal die Kund*innen, sie sind nur die Rohdatenlieferant*innen, und das mit jedem einzelnen Klick. Auf diese Weise werden Subjekte zu Objekten.

3 Ebd.

Zuboff sieht in diesen Geschäftsmodellen, die die weitgehende Rechtsfreiheit im Internet erst ausnutzten und später zum Programm erklärten, schon heute eine »aus dem Ruder gelaufene, von neuartigen ökonomischen Imperativen getriebene Kraft, […] die nicht nur alle sozialen Normen ignoriert, sondern auch die Naturrechte aufhebt, die wir mit der Souveränität des Einzelnen verbinden und auf denen jede Möglichkeit von Demokratie an sich baut«.[4]

Fassen wir zusammen: Das Geschäftsmodell des Überwachungskapitalismus besteht darin, das Recht auf Selbstbestimmung der Individuen auszuhöhlen, sich selbst aber uneingeschränkte (Verfügungs-)Rechte anzumaßen. Und dort, wo der Staat an dieser Art von Vorhersageprodukten partizipieren kann, fällt es ihm schwer, regulierend einzugreifen. Das führt unmittelbar in den zweiten Bereich der Freiheitsgefährdung:

Diese Gefährdung erwächst aus der klassischen Situation, in der Technikkritik schon immer stand: die Entscheidung zwischen Sicherheit und Freiheit. Das große Sicherheitsbedürfnis des Staates nimmt mit der Digitalisierung neue Fahrt auf und tendiert dazu, die garantierten Grundrechte mithilfe von weitgehenden rechtlichen und technischen Geheimdienstbefugnissen zu unterlaufen – Stichwort Snowden-Enthüllungen – oder mit Technologien zu arbeiten, die potenziell diskriminierend und insofern grundrechtseinschränkend sind. Hier, wohlgemerkt, geht es um freiheitliche Demokratien mit robustem Rechtsstaat. Autoritär-populistisch geführte Demokratien, die sich selbst gern als illiberal bezeichnen, die freie Medien und Rechtsstaatlichkeit abbauen, arbeiten oft wenig verdeckt an der Aushöhlung von Bürger*innenrechten. Autoritäre Regime und Diktaturen wie China wiederum nutzen die Überwachungsdaten zur Zementierung ihrer Machtbasis.

Was folgt daraus? Die Bürger*innen sind gefragt. Wir brauchen Wissen und Klarheit über unsere Grundrechte und über die Geltung universeller und unteilbarer Menschenwürde. Wenn Menschen zu Objekten gemacht werden, steht das in klarem Widerspruch zum deutschen Grundgesetz im Besonderen und zum europäischen Menschenwürdeverständnis im Allgemeinen. Beides ist in Reaktion auf beispiellose Würdeverletzungen entstanden. Schauen wir genauer hin:

4 aaO., S. 26.

Menschenwürde und Freiheitsrechte

Die »Unantastbarkeit der Menschenwürde« bekam im Grundgesetz der Bundesrepublik eine starke Verankerung. Der nicht zu begrenzender Schutzraum menschlicher Würde war eine Antwort auf die Verbrechen des Nationalsozialismus und die Entrechtung und Würdeberaubung von Menschen in der faschistischen Diktatur.

Die ebenfalls aus der Erkenntnis des »Nie wieder!« heraus entstandene Allgemeine Erklärung der Menschenrechte formuliert in Artikel 1: »Alle Menschen sind frei und gleich an Würde und Rechten geboren. Sie sind mit Vernunft und Gewissen begabt […]«.

Anders noch die europäische Menschenrechtskonvention, die in ihrer ursprünglichen Fassung von 1950 Menschenwürde nicht explizit erwähnte. Erst die Rechtsentwicklung – insbesondere im Bereich der Bioethik – ließ der Menschenwürde in der EU eine neue Aufmerksamkeit zukommen, sodass sie – ähnlich wie im Grundgesetz – eine herausgehobene Stellung in der Präambel der Charta der Grundrechte der Europäischen Union von 2009 einnimmt: »In dem Bewusstsein ihres geistig-religiösen und sittlichen Erbes gründet sich die Union auf die unteilbaren und universellen Werte der Würde des Menschen, der Freiheit, der Gleichheit und der Solidarität.«[5]

In der Klarheit und Deutlichkeit, mit der in Europa die Menschenwürde als *norma normans* (normierende Norm), als Maßstab der Auslegung aller weiteren Grund- und Freiheitsrechte zentral gestellt wurde, spiegelt sich die Lernerfahrung aus den totalitären Diktaturen des 20. Jahrhunderts wider. Der *Totalitarismus*, der jede Selbstbestimmung, jede Individualität und millionenfach Leben vernichtete, erscheint in vielen Analysen über die problematischen Entwicklungen der Internetökonomie als Gefahr am Horizont.

Umfassende Kontrolle, Überwachung aller Lebensvorgänge, Manipulation und letztlich die Auflösung des Individuums in einem absolut gemeinschaftlichen Ganzen – die Herrschaftspraktiken des Totalitarismus scheinen ihre Wiedergänger in den Führungsetagen von Digitalkonzernen zu finden, mahnen viele kritische Stimmen. Argumente aus Hannah Arendts Analyse der *Elemente und Ursprünge totalitärer Herrschaft*, Grundgedanken aus George Orwells *1984*, die Dystopie einer totalen Überwachungsgesellschaft durch »Big Brother«, und Theodor W. Adornos *Erziehung nach Auschwitz* verfügen mit dem

5 https://www.europarl.europa.eu/germany/de/europäisches-parlament/grundrechtecharta

Blick auf manches Gebaren der Internetkonzerne über erstaunliche Passgenauigkeit zur heutigen Situation. Adornos Worte können als ein Hinweis auf die Potenziale des Totalitarismus gelesen werden, ohne die Entwicklung heute mit dem Entstehen des Faschismus gleichzusetzen. Adorno schreibt, »dass der Faschismus und das Entsetzen, das er bereitete, damit zusammenhängen, dass die alten, etablierten Autoritäten […] zerfallen, gestürzt waren, nicht aber die Menschen psychologisch schon bereit, sich selbst zu bestimmen. Sie zeigten der Freiheit, die ihnen in den Schoß fiel, nicht sich gewachsen.«[6] Sich der Freiheit gewachsen zu zeigen, ist eine Lektion, die Europäer*innen nach der Befreiung vom Faschismus gelernt haben und weiter lernen müssen.

Menschenwürde und Freiheit sind nicht an sich vorrätig, sondern müssen geschützt, verteidigt und gepflegt werden. Zusätzlich bedarf es der Anstrengung jedes einzelnen Individuums, ein Bewusstsein für die Freiheit, ein Gespür für ihre Verletzung zu entwickeln. Bisweilen scheint es, als hätte Adorno hier nachträglich und mit Blick auf die Enteignung des menschlichen Verhaltens Recht behalten: Es besteht die Gefahr, dass Menschen sich der Freiheit nicht gewachsen zeigen, sondern sie verspielen.

Der Schutzraum der Menschenwürde ist nicht begrenzt. Aber es gibt ein Kriterium, das feststellt, wann sie verletzt ist: die sogenannte Objekt-Formel: »Die Menschenwürde ist getroffen, wenn der konkrete Mensch zum Objekt, zu einem bloßen Mittel, zur vertretbaren Größe herabgewürdigt wird.«[7] Genau das geschieht im Geschäftsmodell der großen Internetplattformen. Die Methode des Data-Mining, die Gewinnung von Verhaltensdaten ohne echte Transparenz und Nachvollziehbarkeit, ohne Information an diejenigen, deren Daten aus der »Mine« extrahiert werden, ist eindeutig eine Verletzung menschlicher Würde, dessen also, was die Basis der Menschen- und Bürger*innenrechte ausmacht.

Das Primat des Rechtes durchsetzen

Das Menschenbild des Silicon Valley, das die heutige Digitalisierung prägt, steht dem Menschenwürdekonzept diametral entgegen. Was in der Frühzeit

6 Adorno, Theodor W.: »Erziehung nach Auschwitz«, in: Kulturkritik und Gesellschaft, Teil 2 (Gesammelte Schiften, Bd. 10.2), Frankfurt: Suhrkamp 2003, 677f.

7 Dürig, Günter: »Der Grundrechtssatz von der Menschenwürde«, in: Archiv des öffentlichen Rechts, 81 (1956), Tübingen: Mohr Siebeck, S. 117-157, hier S. 127.

des Internets vielversprechend schien, die Freiheit und Gleichheit aller, die sich im Netz bewegen, erweist sich, wie alle Freiheit, die nicht durch die Freiheit des Anderen begrenzt wird und keinen Ausgleich für Benachteiligung schafft, lediglich als die ultralibertäre Freiheit einer kleinen, auserwählten Gruppe. Für alle anderen ist sie außer Kraft gesetzt.

Einige Manager der großen Tech-Unternehmen fühlen sich in der Rolle der Herrscher, die besser wissen, was für alle Menschen gut ist als diese selbst. Stichworte sind hier Solutionism und Singularität. Eine Gruppe von »Weisen« verfügt über eine gefügige Masse, eigene Entscheidungen einzelner Individuen werden ausgehebelt; sehr schön beschrieben in Dave Eggers Roman *The Circle* unter Verwendung vieler, aus totalitären Systemen bekannten Sujets. Auch in der Realität: Die Konzernzentralen von Google und Facebook gleichen undurchdringlichen Festungen. Totale Transparenz und Aufgabe von Privatsphäre, von den Nutzer*innen gefordert, gilt für das eigene Geschäftsgebaren gerade nicht. Rechtsstaatlichkeit und Marktwirtschaft werden als veraltet betrachtet, den Nutzer*innen der immer umfassenderen Dienste wird weisgemacht, ihre Daten und damit ihr Verhalten seien gut aufgehoben – in undurchdringlichen Rechenzentren. Die digitalen Dienste versprechen Sicherheit und Rundum-Betreuung, Bequemlichkeit und Entlastung von der Qual der Wahl. Menschenwürde und Grundrechte sind in dieser Welt keine Kategorien. Oder sogar andersherum: Erst die digitalen Dienste würden Freiheit ermöglichen.

Auch in staatlichen Institutionen kommen – wie wir spätestens seit Edward Snowden wissen – hoch problematische Praktiken zur Anwendung. Gleichzeitig aber gibt es Gegengewichte, es gibt Parlamente und Menschen im administrativen Bereich, die gegensteuern, Alarm schlagen, problematische Entwicklungen ans Licht bringen und Korrekturen einfordern – auf rechtsstaatlichem Wege.

Die Bindung des liberalen Verfassungsstaates an das Grundgesetz und seine korrigierende Wirkung zeigen sich in richtungsweisenden Gerichtsurteilen. Exemplarisch zu nennen sind Urteile des Karlsruher Verfassungsgerichtes, etwa das »BND-Urteil«[8] zur Geltung der Grundrechte auch im Ausland, das Urteil zur »Antiterrordatei«[9], das mit Verweis auf die Grundrechte

8 https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2020/bvg20-037.html

9 https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2020/bvg20-104.html vom 11.12.2020; https://netzpolitik.org/2020/urteil-des-bundesverfass

eben jenes Data-Mining – die Verknüpfung von Daten aus unterschiedlichen Quellen – für teilweise verfassungswidrig erklärt, und das Urteil zur »Vorratsdatenspeicherung«[10], die in ihrer bisherigen Form ebenfalls mehrfach als verfassungswidrig bezeichnet wurde.

Diese Urteile des Bundesverfassungsgerichtes, aber auch weitere des Europäischen Gerichtshofes für Menschenrechte, belegen den kategorialen Unterschied, der zwischen problematischen Praktiken staatlicher Behörden in Rechtsstaaten und solchen in globalen, privatwirtschaftlichen Bereichen besteht. Eine derartige Praxisprüfung entlang demokratischer Normen steckt für die Konzerne, die Markt und Staat unterminieren, noch in den Kinderschuhen. Dennoch: Das Primat des Rechtes verschafft sich zunehmend Geltung in zahlreichen Regulierungsvorschlägen auf europäischer Ebene. Zudem besteht jetzt die Chance, diese auch transatlantisch abzustimmen. Und nicht zuletzt weist der regulatorische Prozess auch einige Ergebnisse auf, beispielsweise das Netzwerkdurchsetzungsgesetz und das Gesetz gegen Wettbewerbsbeschränkungen.

Digitales Rechtsbewusstsein entwickeln

Freiheit und Grundrechte, die sie schützen, sind fest verankert in einem grundlegenden Würde-Verständnis. Die Verletzung eines einzelnen Grundrechtes durch digitale Praktiken hat grundsätzlich die Tendenz zur Würdeverletzung. Nie geht es nur um den Bruch eines einzelnen Rechtes, zum Beispiel die Unverletzlichkeit des Eigentums oder den Schutz der räumlichen Privatsphäre, nie nur um die Beschädigung einzelner aktiver Rechte wie Versammlungs- und Meinungsfreiheit. Immer besteht eine enge Verknüpfung mit menschlicher Würde. Stets geht es um die Kombination von Freiheitseinschränkung und Würdeverletzung.

Das erklärt die starke Beunruhigung all jener, die sensibel für Grundrechtsverletzungen sind, wie Nichtregierungsorganisationen, die Gesellschaft für Freiheitsrechte, aber auch Parlamentarier*innen im Bundestag oder im Europäischen Parlament.

---

ungsgerichts-datamining-in-antiterrordatei-fuer-strafverfolgung-war-verfassungswidrig/

10 https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2020/bvg20-061.html;jsessionid=235A2A54704ABEE876859E3B9DEDB765.1_cid386

Solange aber nicht eine kritische Masse von Menschen die Verletzungen ihrer eigenen Würde wahrnimmt, ein Rechtsbewusstsein entwickelt, Klagen anstrengt und Druck erzeugt, wird das Geschäftsmodell der Rechte-Enteignung und der Würdeverletzung weiter funktionieren und perfektioniert werden.

Die Anstrengung, ein solches Bewusstsein für die eigenen Freiheitsrechte im digitalen Raum zu schaffen, ist vergleichbar mit der Herausbildung eines Umweltbewusstseins, das in den 1970er Jahren zu wachsen begann, getrieben von der Sorge um einen für kommende Generationen bewohnbaren Planeten. Zunächst lächerlich gemacht als fortschrittsfeindlich und technikskeptisch, hat sich das Umweltbewusstsein inzwischen bis in die Mitte der Gesellschaft verbreitet.

Ähnliches ist für das Rechtsbewusstsein im digitalen Raum nötig. Für die Einhegung der digitalen Praktiken und ihren Einsatz für das Gemeinwohl reicht es nicht, auf die positiven Rechte, die existierende Rechtsprechung, zu verweisen. Es braucht ein neues Rechtsbewusstsein aller demokratischen Akteur*innen und eine breite gesellschaftliche Debatte. Welches Menschenbild in einer Gesellschaft gelten und welche Werte es verkörpern soll – Würde, Freiheit, Solidarität – das bildet sich im öffentlichen Diskurs heraus. Würde, Freiheit und Solidarität spiegeln die emanzipatorischen und antitotalitären Lernerfahrungen der Vergangenheit. Für die digitale Zukunft werden Werte wie Privatheit, Selbstbestimmung, Sicherheit und Gerechtigkeit weichenstellend sein. Viel mehr Menschen müssen in diesen Diskurs involviert werden. Unter Expert*innen ist die Debatte in vollem Gange, aber sie braucht Belebung und Förderung und vor allem Verbreiterung.

Wir haben beschrieben, dass die Abschöpfung menschlichen Verhaltens und die intransparente Verknüpfung von Daten Menschen zu Objekten macht, also das grundlegende Menschenrecht auf Würde verletzt.

Wie genau sind Grundrechtseinschränkung und Würdeverletzung verbunden? Wir sehen uns drei Spannungsfelder konkret an, die unmittelbaren Grundrechtsbezug haben: das Recht auf informationelle Selbstbestimmung, den Gleichheitsgrundsatz und die Meinungsfreiheit.

Beispiel 1: Überwachung und Kontrolle versus informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung kam zunächst in den Grundrechtskatalogen nicht vor. Darf der Staat alle möglichen Daten sam-

meln, aufheben, verarbeiten und nutzen? Diese Frage ließen Bürger*innen 1983 durch das Bundesverfassungsgericht klären. Dieses antwortete mit der Anerkennung eines Rechtes, das Bürger*innen in der Tradition der Abwehrrechte gegen den Staat davor schützte, »nicht mehr wissen [zu] können, wer was wann und bei welcher Gelegenheit über sie weiß«.[11] Gemeint war hier die Volkszählung. Auch der heute sogenannte *chilling effect* fand schon Berücksichtigung, also die Einschränkung der Entscheidungsfreiheit durch Furcht vor Benachteiligung in der Zukunft.

Wie das Recht auf informationelle Selbstbestimmung aus dem Grundgesetz Artikel 2 in Verbindung mit Artikel 1 erwuchs, so basiert der europäische Datenschutz und die sehr tiefe Ausprägung der DSGVO auf dem in Artikel 8 der Europäischen Grundrechtecharta festgehaltenen Schutz personenbezogener Daten. Es gibt also ein rechtliches Fundament zur Wahrung dieser Freiheitsrechte in der digitalen Welt.

Das Persönlichkeitsrecht garantiert Privatheit und Entscheidungshoheit über die eigenen Daten. Zugleich aber ist die Digitalisierung, in der Regel mit Einwilligung der Nutzer*innen, tief in das Privatleben eingedrungen. Das zeigen Online-Dienste, die wir auf Deutsch Partnervermittlung nennen würden, wie Tinder oder OkCupid der Match Group. Intimste Informationen werden für perfekt zugeschnittene Werbung genutzt. Die Mathematikerin Cathy O'Neill beschreibt in ihrem Buch *Weapons of Math Destruction*[12] das Geschäftsinteresse dabei: Nutzer*innen sollen sich so lange wie möglich auf den Plattformen aufhalten und deren Apps nutzen, um möglichst viele Daten preiszugeben, mehr Einblicke in die persönlichen Gedanken und Vorlieben zu gewähren. Wie nebenher bestimmen algorithmische Entscheidungssysteme, welche Menschen den Nutzer*innen vorgestellt werden und welche nicht. Bei Nichtgefallen: einfach wegwischen. Eine algorithmisch eingebaute Verletzung von Menschenwürde.

Ging es vor 40 Jahren noch um die Erhebung einzelner Daten durch den Staat, haben wir es heute mit der Zusammenführung von Daten für die Privatwirtschaft zu tun. Auf diese Veredlung würden auch staatliche Stellen gerne zugreifen. Das Verbot, ein einzelnes Datum zu erheben, würde wenig nutzen, auch eine Verpflichtung zur Anonymisierung der Daten würde nicht den erwünschten Zweck erfüllen. Denn das wirtschaftliche Potenzial liegt

11 https://www.bfdi.bund.de/DE/Datenschutz/Ueberblick/Was_ist_Datenschutz/Artikel/InformationelleSelbstbestimmung.html

12 https://weaponsofmathdestructionbook.com/

in der Verknüpfung von öffentlich zugänglichen und privat bereitgestellten Daten, aus denen sich Muster erkennen lassen. Erst diese Muster, nicht das Datum an sich, lassen präzise Rückschlüsse auf Gruppen oder Einzelne zu. Der bekannte Fall der Cambridge-Analytica-Methode hat mit diesem Microtargeting-Prinzip großflächig funktioniert. Große Sammlungen demografischer Daten, Likes, Aktivitäten auf Facebook wurden ausgebeutet und das Verhalten von Nutzer*innen analysiert, um psychologische Profile zu erstellen und so persönlich zugeschnittene Wahlwerbung an spezifische Zielgruppen zu richten, ohne dass dies den Betroffenen bekannt oder bewusst gewesen wäre.[13] Microtargeting wurde unter anderem während der US-Präsidentschaftswahl 2016 für Donald Trumps Wahlkampf und beim Brexit-Referendum im selben Jahr von der »Vote Leave«-Kampagne genutzt.

Inzwischen laufen Forschungsprojekte, die allein aufgrund der Auswertung von Bilddaten aus Google Street View präzise das Wahlverhalten bis hinunter auf Wahlkreisebene vorhersagen.[14] Weder geht es um personenbezogene Daten, noch müssen die Betroffenen eingewilligt haben, dass dieses Forschungsprojekt stattfindet. Mannigfaltige Möglichkeiten des Gebrauchs, aber auch des Missbrauchs öffnen sich damit. Nun ließe sich mit einem Opt-out aus Google Street View argumentieren. Schließlich könne man die Aufnahme ablehnen. Aber auch das schützt nicht vor einem Scoring auf Basis individueller Parameter. Dieses Scoring kann eine gruppenspezifische Diskriminierung zur Folge haben, wenn es um höhere Versicherungstarife aufgrund des Wohnortes, um einen guten Job, um Wahlbeeinflussung und gezieltes Nudging für dieses oder jenes Verhalten geht. Das Recht auf informationelle Selbstbestimmung ist hier, trotz der Möglichkeit des Opt-out, weitgehend infrage gestellt.

Besonders sensibel sind Gesundheitsdaten. Der Markt ist attraktiv und die Verlockungen der fitnessorientierten Gesellschaft, hier Daten preiszugeben, sind immens: Fitness-Tracker, wie Fitnessarmbänder oder Smart Watches, bieten jede nur denkbare Gelegenheit, den Gesundheitszustand einer unbekannten Überwachung und Kontrolle zu übergeben. Trotz zahlreicher Warnungen von Datenschützer*innen und Menschenrechtler*innen genehmigte die EU-Kommission die Übernahme der Firma Fitbit, spezialisiert auf Wearables und Fitnesstracker, durch Google. Einmal mehr zeigt sich, dass das

13 Vgl. https://netzpolitik.org/2018/cambridge-analytica-was-wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen/

14 Vgl. https://www.nytimes.com/2017/12/31/technology/google-images-voters.html

Geschäftsmodell von Google durch das Raster der üblichen Kriterien zur Bewertung von Marktverzerrungen fällt. Es ging nicht allein um Markterschließung, es geht um die Potenziale der Überwachung und Steuerung von Millionen Menschen und um ihren Missbrauch als Datenminen für Geschäfte mit Dritten. Grundrechtsschutz ist trotz gestiegener Sensibilität auf EU-Ebene kein Prüfkriterium im Wettbewerbsrecht. Das heißt, hier kann ein Grundrecht nicht umgesetzt werden, weil die Potenzialität der Grundrechtsverletzung in einem scheinbar weit entfernten Regulierungsfeld noch nicht ausreichend bewertet werden kann.[15]

Beispiel 2: Diskriminierung versus Gleichheitsgrundsatz

Ein weiteres Grundrechtsversprechen der Demokratie ist die Gleichheit. Im Grundgesetz in Artikel 3 niedergelegt, geht es um Gleichheit vor dem Gesetz, um Geschlechtergerechtigkeit und um Gleichbehandlung aller Menschen. In der vielfältigen Gesellschaft muss gerade die Gleichbehandlung immer wieder und für jedes Merkmal der möglichen Diskriminierung oder gegen Privilegierung erkämpft werden, angefangen bei der Bildung bis hin zum Arbeitsmarkt oder der Wohnungssuche. Gleichheit bedeutet gleichberechtigte, angstfreie Teilhabe und Zugang zu öffentlichen Gütern, Räumen und Netzen.

Das Geschäftsmodell der algorithmenbasierten Auswahlprozesse impliziert aber nicht den Grundsatz der Gleichheit, sondern die Weltsicht der Coder und die Daten der Vergangenheit. Zudem werden algorithmenbasierten Entscheidungssysteme nach subjektiven Kriterien trainiert, die in der Regel intransparent sind. Das birgt erhebliche Potenziale für die Diskriminierung ganzer Bevölkerungsgruppen aufgrund individueller Merkmale, sei es bei Bewerbungsprozessen, der Vergabe von Schulplätzen,[16] der Beurteilung der Kreditwürdigkeit oder bei juristischen Entscheidungen (wie etwa im US-

15 Eine Möglichkeit, zu erwartende Marktmachtkonzentration einzuhegen, könnte mit der Ex-ante-Regulierung, die durch den Digital Market Act der EU-Kommission im Gespräch ist, eingeführt werden. Mit einer solchen Vorab-Regulierung soll verhindert werden, dass die Marktmacht in dem einen Segment dazu genutzt wird, sich in einem anderen Segment einen uneinholbaren Startvorteil zu verschaffen. Allerdings reicht auch das nicht bis zum Recht auf informationelle Selbstbestimmung.

16 Vgl. https://netzpolitik.org/2018/wenn-sie-ethisch-umgesetzt-werden-kosten-sie-mehr-danah-boyd-ueber-algorithmische-entscheidungssysteme/ Dazu auch: https://algorithmwatch.org/en/busted-internet-myth-algorithms-are-always-neutral/

Justizsystem).[17] Ein weiteres Beispiel sind Gesichtserkennungssysteme, die in einigen Ländern eingesetzt werden. Diese können die Gesichter von Schwarzen, Indigenen und anderen Menschen of Colour oder Frauen häufig nicht korrekt identifizieren, werden aber zum Teil im Strafvollzug, in der Strafverfolgung oder der Prävention verwendet.[18]

Viele Beispiele der Diskriminierung durch Entscheidungsalgorithmen stammen aus den USA. Für Deutschland hat die NGO AlgorithmWatch in einem *Atlas der Automatisierung* aufgezeigt, in welchen Bereichen auch hierzulande Entscheidungen automatisiert getroffen werden, vom Personalmanagement über die Verwaltung von Arbeitslosigkeit bis hin zur Spracherkennung von Asylsuchenden und Predictive Policing. AlgorithmWatch hat daraus Handlungsempfehlungen entwickelt, die vom Grundsatz »do no harm« über die Forderung nach Nachvollziehbarkeit der Entscheidungen und einer wirkungsvollen Aufsicht über privatwirtschaftliche und staatliche Anwendungen reichen.[19] Dieser Katalog ist ein wichtiger Beitrag zur Schärfung und Stärkung des Rechtsbewusstseins im digitalen Raum.

Beispiel 3: Hate Speech und digitale Gewalt versus Meinungsfreiheit und demokratische Öffentlichkeit

Ein drittes Feld der Grundrechtsverletzungen umfasst Hassrede und Gewalt im Netz, die dem Grundrecht auf Meinungsfreiheit in Artikel 5 des Grundgesetzes entgegenstehen. Hate Speech (Hassrede) ist nicht nur zu einem Problem individueller Bedrohung, sondern zu einer Gefährdung medialer Öffentlichkeit überhaupt geworden. Während der Bundestag 2013 noch keinerlei gesetzgeberischen Handlungsbedarf sah, gegen Hate Speech vorzugehen,[20] hat sich die Lage innerhalb weniger Jahre dramatisch verändert. Wo Hassrede zu kriminellen Handlungen anstachelt, gepaart mit Falschinformationen und verstärkt durch Shitstorms, Hetzjagden im Netz, ist rechtliche Eindämmung gefragt.

17 Vgl. https://www.nytimes.com/2017/06/13/opinion/how-computers-are-harming-criminal-justice.html

18 Vgl. https://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Hintergrundpapier-hp024.pdf

19 Vgl. https ://atlas.algorithmwatch.org

20 Dreizehnter Zwischenbericht der Enquete-Kommission »Internet und digitale Gesellschaft«, Bundestag Drucksache 17/12542, S. 82.

Die Algorithmen der Intermediären wie Facebook und Twitter vervielfältigen Hassrede und sorgen für die schnelle Verbreitung von Desinformationen. Die Verächtlichmachung von seriösen Medien und Wissenschaft, die Entstehung von undurchdringlichen Informationsblasen verfälschen den offenen Meinungsbildungsprozess, beschädigen die demokratische Öffentlichkeit und stacheln nachweislich auch zu physischer Gewalt an.[21] Während der Corona-Pandemie erscheint die von der WHO beklagte »Infodemie« – aus Desinformationen, Verschwörungstheorien und Wissenschaftsfeindlichkeit – lebensbedrohlich, weil wichtige Informationen zum Schutz der Gesundheit bestimmte Teile der Bevölkerung nicht mehr erreichen. Je nach Stärke der öffentlich-rechtlichen Medien sind das in unterschiedlichen Ländern verschieden große Gruppen von Menschen. In Sachen Hate Speech stehen auf der einen Seite Täter, die Meinungsfreiheit für sich reklamieren, auf der anderen Seite Opfer, die unter Einschüchterung und Mobbing leiden, deren Persönlichkeitsschutz nicht mehr gewahrt ist, was sie an der freien Entfaltung ihrer Persönlichkeit hindert.

Eine ganze Reihe wissenschaftlicher Studien belegt die gefährdenden Auswirkungen, darunter Selbstzensur und psychische Folgeschäden für die Betroffenen, Veränderung impliziter Haltungen und Meinungen der un- oder beteiligten Nutzer*innen.[22] Insbesondere Frauen sind überdurchschnittlich häufig Opfer von Hate Speech und digitaler Gewalt. Der Fall von Renate Künast, in dem unerhörte Beleidigungen gerichtlich teilweise gebilligt wurden, warf ein grelles Licht auf die Notwendigkeit, Meinungsfreiheit für Hassrede zugunsten des Persönlichkeitsschutzes einzuschränken und zugleich Meinungsfreiheit als Freiheit für Meinung zu schützen, denn: Hass ist keine Meinung.

Für die Gerichte gilt es, eine Rechtsprechung zu entwickeln, die dem Risiko angemessen ist, das durch die pure Reichweite der neuen Medien massiv

21 Vgl. https://hatebase.org/news/2019/11/18/does-online-hate-speech-cause-violence

22 z.B. Aslan, Alev: »Online hate discourse: A study on hatred speech directed against Syrian refugees on YouTube«, in: Journal of Media Critiques 3(12) (2017), S. 227-256; Geschke, D., Klaßen, A., Quent, M., & Richter, C.: »#Hass im Netz: Der schleichende Angriff auf unsere Demokratie: Eine bundesweite repräsentative Untersuchung« in: Forschungsbericht (2019); Weber, M., Koehler, C., Ziegele, M., & Schemer, C.: »Online Hate Does Not Stay Online–How Implicit and Explicit Attitudes Mediate the Effect of Civil Negativity and Hate in User Comments on Prosocial Behavior«, in: Computers in Human Behavior (2019), S. 106-192.

erhöht ist. Beleidigungen im öffentlichen Raum sind nicht zu vergleichen mit Beleidigungen im digitalen Raum, die in einem weltweiten Kommunikationsnetzwerk tausendfach vervielfältigt werden können. Die bestehenden Standards, nach denen Hassrede strafrechtlich nur im Falle einer expliziten Beleidigung und physischer, direkter Gewaltandrohung verfolgt werden kann, reichen für die im Netz begangenen Taten nicht aus.

Darüber hinaus besteht inzwischen Konsens über die Dringlichkeit einer Regulierung der Intermediären mit Blick auf die demokratische Öffentlichkeit und ihren Einfluss auf Meinungsbildungsprozesse in der Gesellschaft. Offen debattiert wird über einen Regulierungsrahmen, der vergleichbar ist mit einer Mediengesetzgebung. Ein solcher Rahmen hätte automatisch Rückwirkung auf die Grundrechte der Nutzer*innen.

Nach diesen Tiefenbohrungen an drei grundlegenden Freiheitsrechten, die einen gemischten Befund ergaben, drängt sich eine Frage auf, die häufig gestellt wird:

Brauchen wir neue Grundrechte für das digitale Zeitalter?

Reichen die bisherigen Freiheitsrechte denn überhaupt aus, um den Gefahren für die demokratische Öffentlichkeit, der Manipulation von Einstellungen und Verhalten, der Beeinflussung des Wahlverhaltens, der Lenkung der öffentlichen Meinung und der Lähmung freiheitlicher Entscheidung durch allgegenwärtige Überwachungstechnologien etwas entgegenzusetzen?

Die Stichproben bei den Grundrechten des Persönlichkeitsrechtes, des Rechtes auf informationelle Selbstbestimmung, dem Gleichheitsgrundsatz und der Meinungsfreiheit haben gezeigt: Es mangelt nicht an Freiheitsrechten, sondern an ihrer Durchsetzung. Versuche neuer Definitionen, wie die Charta der digitalen Grundrechte von 2016, bleiben hinter dem hohen Rechtsschutz zurück, den das Grundgesetz und die Europäische Grundrechtecharta bereits bieten.

Die einschneidenden Erfahrungen aus den Diktaturen des 20. Jahrhunderts haben die in der Menschenwürde gegründeten Grundrechte und ihre Rechtsdurchsetzung fest in Europa verankert. Sie sind keine Papiertiger, sondern rechtlich einklagbar und durchsetzungsfähig – genau das ist die Stärke der Rechtsstaatlichkeit, die Europa zu einem Kontinent mit hohen menschenrechtlichen und demokratischen Standards hat werden lassen.

Gleichwohl, Grundrechtsschutz fällt uns als Unionsbürger*innen nicht in den Schoß. Im Digitalen muss die Durchsetzung der Freiheitsrechte genauso erkämpft werden wie im Analogen. Worauf es jetzt ankommt, ist die Europäisierung ihrer Durchsetzung und in letzter Konsequenz die Globalisierung der Rechtsdurchsetzung. Da dies aber eher zu den visionären Zielen gehört, die rasch als Ausflucht für Nichtstun auf nationaler Ebene herhalten könnte, kommt es jetzt darauf an, Grundrechte auf eine Weise durchzusetzen, dass sie erstens auf international agierende, digitale Konzerne anwendbar sind und dass diese Durchsetzung europäisiert wird. In der Regel sind europäische Normen im nationalen Recht umgesetzt und der Rechtsweg steht in erster Linie im Inland offen. Das muss geöffnet werden: Wenn Google in Irland seinen Sitz hat, aber Hate Speech aus den USA sich gegen eine Person in Deutschland richtet, die sich gerichtlich dagegen wehren will dann müssen die Möglichkeiten der grenzüberschreitenden Rechtsdurchsetzung erweitert werden.[23]

Es ist beschämend und für den Rechtsstaat kein guter Zustand, wenn sich in den AGBs von Facebook & Co Paragrafen befinden, die schlicht rechtswidrig sind, das geltende Recht aber wegen der enormen Marktmacht und einem unverhältnismäßigen Aufwand, den eine Rechtsdurchsetzung von Deutschland aus nach sich ziehen würde, nicht durchgesetzt werden kann.

Das muss sich ändern. Bis dahin muss aber ein anderer Bereich geschärft werden, von dem wir bereits sprachen: das Rechtsbewusstsein für die Verletzungen der eigenen Grundrechte. Um der Freiheit willen muss eine Atmosphäre entstehen, in der das digitale Rechtsempfinden unter Nutzer*innen, Mitbewerber*innen und im öffentlichen Bewusstsein aktiviert wird. Dafür ist es wichtig, das offensichtliche Unrecht anhaltend und öffentlich sichtbar anzuprangern.

Die Anpassung des Rechtes an die globale Herausforderung ist auch eine Frage der Zeit. Ein erster Schritt war die Europäische Datenschutz-Grundverordnung, die 2018 in Kraft trat und gegen enorme Widerstände durchgesetzt werden musste. Nach ihrer Verabschiedung existiert nun aber eine Grundverordnung, die sich zum Ziel setzt, »die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten« zu schützen (Art. 1, Abs. 2 DSGVO). Dieser Schutz gilt sowohl für die Erhebung als auch für die Verarbeitung

23 Vgl. hierzu im Detail: https://irights.info/artikel/die-digitalcharta-und-was-wir-statt-dessen-brauchen/28273

der Daten. Einen zweiten Schritt geht die EU nun mit ihrem Gesetzespaket zum Digital Services Act und Digital Marktes Act, das einen europäischen Rechtsrahmen für digitale Dienste und Märkte schaffen will. Dieser soll Marktmachtmissbrauch und unfaire Praktiken von Anbietern in der EU nach dem Marktortprinzip wirksam einschränken, Datenzugang und Interoperabilität der Messengerdienste ermöglichen und mehr Transparenz für Empfehlungsalgorithmen und Online-Werbung schaffen.

Der digitale Kompass – Privatheit schützen, Selbstbestimmung und Sicherheit gewährleisten und Teilhabe ermöglichen

Die Werte, die einer Gesellschaft zugrunde liegen, sind in ihrem Rechtssystem verankert. Wenn Würde, Freiheit und Solidarität die emanzipatorischen und antitotalitären Lernerfahrungen spiegeln, dann rücken im digitalen Zeitalter die Werte Privatheit, Selbstbestimmung, Sicherheit und Teilhabe in den Fokus. Nur wenn diese Werte und die damit verbundenen Rechte garantiert und durchgesetzt werden, ist ein Umgang mit digitalen Technologien möglich, der souverän genannt werden kann. Das schließt ein individuelles Rechtsbewusstsein genauso ein wie äußere Rahmenbedingungen, die die Wahrnehmung individueller Rechte ermöglichen und erleichtern.

Privatheit schützen, Selbstbestimmung und Sicherheit gewährleisten und Teilhabe ermöglichen – so könnte die Zielvorstellung für das digitale Gemeinwohl lauten. Dabei geht es nicht um Soft Law in Form von Selbstverpflichtungen oder Vertrauen in die Rechtstreue der Anbieter. »Das Recht kennt keinen hybriden Zustand eines nicht verbindlichen Rechts.«[24] Es geht um individuelle Grundrechte und Rechtsdurchsetzung als Basis einer freien und offenen Gesellschaft. Die Herausforderung ist komplex, ihre Konkretionen sind unablässig im Fluss.

Privatheit zu schützen, heißt, die Grundrechte auf freie Meinungsäußerung (GG 5), auf Glaubens- und Gewissensfreiheit (GG 4), auf Versammlungsfreiheit (GG 8), auf Schutz der Familie (GG 6), auf die freie Berufswahl (GG 12) und das Eigentumsrecht (GG 14) zu garantieren und ihre einfachgesetzliche Umsetzung zu gewährleisten.

Selbstbestimmung und Sicherheit im Netz zu gewährleisten, bedeutet, persönlich Hoheit zu erlangen über die Erhebung und Verarbeitung von perso-

24 Grimm, Petra; Keber, Tobias; Zöllner, Oliver: Digitale Ethik. Leben in vernetzten Welten, Ditzingen: Reclam 2019, S. 24.

nenbezogenen, persönlichen Daten. Das setzt klare, faire und vertrauenswürdige Regelungen für Datenerhebung, Datenzugang und Datennutzung voraus. Zudem muss die Nachvollziehbarkeit von algorithmischen Entscheidungen gegeben sein. Das setzt wiederum die Integrität informationstechnischer Systeme voraus, Verschlüsselung spielt dabei die größte Rolle.[25]

Teilhabe zu ermöglichen, bedeutet, digitaler Gewalt und Diskriminierungen etwa durch fehlgeleitete Entscheidungsalgorithmen, vorzubeugen und möglichst im Vorhinein zu unterbinden. Zudem geht es um gleichberechtigten Zugang zu öffentlichen Gütern, Räumen und zum Netz.

Was jetzt zu tun ist: Infrastruktur, Bildung, Partizipation und Ordnungspolitik

Mit diesem digitalen Werte-Kompass ist ein Teil der Antwort auf die Ausgangsfrage gegeben: Wie lassen sich Grund- und Freiheitsrechte im digitalen Zeitalter umsetzen? Wir hatten gesehen: Grundrechte setzen sich nicht von allein durch. Das gesellschaftliche Bewusstsein für ihre Verletzung im digitalen Raum muss die nötige Kraft entwickeln. Um den digitalen Kompass auch tatsächlich auszurichten, sind verschiedene Ansätze nötig.

Digitalisierung ist auch eine Frage der Infrastruktur: Ja, der Zugang zum stabilen, sicheren und leistungsfähigen Netz ist ein wichtiger Schritt zur digitalen Teilhabe aller Bürger*innen – kein Luxus, sondern Teil der Daseinsvorsorge. Dass es dazu eines stabilen, schnellen Internetzuganges bedarf, ist eine Binsenweisheit, aber in Deutschland noch lange nicht Realität. Technische Voraussetzungen fehlen vielerorts, auch die rechtliche Verpflichtung der Anbieter, alle Flächen des Landes abzudecken. Die Netzneutralität hingegen ist durch ein Urteil des EuGH gestärkt worden.[26]

Gemeinwohl und digitale Infrastruktur gehören zusammen.

Ein weiteres, wichtiges und großes Thema ist *digitale Bildung*. Wenn wir das Internet als »Neuland« unter den Pflug nehmen wollen, dann braucht es starke Angebote der digitalpolitischen Bildungsarbeit. Der Satz »Ich habe nichts zu verbergen« gehört ins Museum. Niemand käme auf die Idee zu sagen: »Ich habe nichts Wertvolles in meiner Wohnung, also lasse ich die Haustür offen.« Mit Bildungsangeboten muss in Schulen, in Vereinen, durch poli-

25 Vgl. https://www.bundestag.de/dokumente/textarchiv/2020/kw05-pa-inneres-669564

26 Vgl. https ://netzpolitik.org/2020/eugh-zur-netzneutralitaet-provider-duerfen-angebote-nicht-selektiv-drosseln

tische Stiftungen und die Zivilgesellschaft ein neues Bewusstsein für die Abwehrrechte nicht nur gegenüber dem Staat, sondern auch gegenüber privaten Datensammlern und -verwertern entwickelt werden. Zu politischer Bildung gehört, Menschen das Handwerkzeug für die Nutzung des Internets in beide Richtungen zu geben: Zum einen muss das Wissen um die eigenen Rechte im digitalen Raum gestärkt werden, denn das Bewusstsein für Rechtsverletzungen und das Wissen um Gefahren schützen die Freiheitsrechte. Zum anderen aber umfasst politische Bildung auch das Know-how, das Internet zum eigenen Vorteil mehr und besser zu nutzen. Denn erst mit diesen Fähigkeiten wird aus digitaler Bildung ein Instrument zu digitaler Teilhabe. Diese schließt selbstverständlich viel mehr Aspekte ein, denn die Barrieren der Teilhabe verschärfen oder potenzieren sich in der digitalen Welt. Gut erforscht ist das im Blick auf die Fähigkeit von Schüler*innen, mit digitalen Anwendungen umzugehen.[27] In der Corona-Pandemie wirkt sich ein fehlender oder unzureichender Internetzugang sehr konkret auf die Bildungschancen von Kindern aus, wenn Möglichkeiten des digitalen Lernens schlicht aus Mangel an stabilem Zugang zum Internet nicht genutzt werden können. Das Grundrecht auf die freie Entfaltung der Persönlichkeit ist hier von vornherein verletzt.

Ein weiterer, wesentlicher Faktor ist die *Partizipation von Bürger*innen* an politischen Entscheidungen. Dazu gehört eine *breite öffentliche Debatte* über Sicherheit und Freiheit im Netz, über Persönlichkeitsschutz, Meinungsfreiheit und vieles andere mehr. Diese Debatten, so konfliktreich sie sein mögen, schärfen das Bewusstsein individueller Grundrechte in der digitalisierten Welt.

Nachweislich stärkt nachhaltige und sinnvolle politische Beteiligung die Demokratie.

Je transparenter und beteiligungsorientierter Politik und Verwaltung mit den von ihnen erhobenen Daten, mit politischen Antworten zur Wahrung der Grundrechte im Netz, mit dem Zugewinn an Kommunikation und Vernetzung, mit den vielfältigen Informationsmöglichkeiten umgehen, umso mehr stärken sie die Souveränität ihrer Bürger*innen.

Ordnungspolitisch – das hatten wir gesehen – stehen große Entscheidungen an. Diese müssen öffentlich debattiert werden. Eine wertegeleitete, digitale Ordnungspolitik stärkt auch die Robustheit des Rechtsstaates. Es ist höchste Zeit für eine ordnungspolitische Antwort, die die individuellen Rech-

27 Vgl. https ://www.boell.de/BildungDigitaleWelt

te zentral stellt und einen klaren Rahmen für die Regulierung der algorithmenbasierten Wirtschaft gibt.

Die Grundrechte werden sich nicht von allein und nicht durch freiwillige Selbstverpflichtungen der Konzerne durchsetzen. Deshalb braucht es die breite Unterstützung und das gemeinsame Engagement der (Zivil-)Gesellschaft, Politik, Wissenschaft und Wirtschaft, um Bürgerrechte auch im digitalen Zeitalter zu garantieren und zu schützen, um den digitalen Raum im Sinne des Gemeinwohls nutzbar zu machen.

2.1.2 Selbstbestimmung

Die Digitalisierung als Herausforderung für die Bestimmung des Selbst im Gesundheitswesen

Christiane Woopen und Sebastian Müller

Selbstbestimmte Menschen können ihr Ideal eines erfüllten und guten Lebens selbst wählen, sie können sich eigene moralische Normen setzen, integer zu diesen Normen handeln und sie können ihre Geltungsansprüche in gesellschaftspolitische Diskurse einbringen. Die *Selbstbestimmung* ist damit ein wesentlicher Bestandteil moderner, pluralistischer Gesellschaftskonzepte. Den Gegenpol zu diesem Ideal bildet die Vorstellung einer restlos fremdbestimmten Welt, in der Menschen keine eigene Identität ausbilden und ihr Schicksal nicht selbst beeinflussen können. Angesichts dieses Gegensatzes zwischen vollständig autonomen und determinierten Menschen lohnt es sich, ein paar Schritte zurückzutreten und die Gesamtheit der sehr bunten physischen, psychischen und sozialen Lebenswelt zu betrachten, in der die menschliche Fähigkeit zur Selbstbestimmung durch punktuelle Faktoren und komplexe Wechselbeziehungen fortwährend eingeschränkt und befördert wird.

Mit der permanenten Weiterentwicklung digitaler Technologien kommen zu dem Bild weitere Farben hinzu. So können Menschen beispielsweise mithilfe moderner Suchalgorithmen ihre eigenen Wissenslücken selbstwirksam schließen und in der Folge selbstbestimmtere Entscheidungen treffen, auch in Bezug auf ihre Gesundheit. Allerdings ist oft unklar, welche Gesundheitsinformationen verlässlich sind. Zudem sammeln viele Suchplattformen und andere digitale Applikationen die persönlichen Daten ihrer Nutzer*innen, um gezielt Einfluss auf deren Verhalten auszuüben. Viele Nutzer*innen sind nicht in der Lage, die Folgen solcher digitalen Interaktionen auf ihr Leben und die Gesellschaft abzuschätzen. Das führt zu strukturellen Missverhältnissen, die einige Autor*innen dazu veranlasst haben, von *gläsernen Bürger*in-*

nen in einem *digitalen Panoptikum* zu sprechen.[1] Diese Entwicklung betrifft aber nicht nur Patient*innen. Auch die Selbstbestimmung von Ärzt*innen kann durch die Digitalisierung erheblich beeinflusst werden. Beispielsweise wird ihnen durch digitale Diagnostikalgorithmen einerseits ein verbessertes Diagnostik- und Therapieangebot an die Hand gegeben. Andererseits können Ärzt*innen die algorithmischen Empfehlungen mitunter nur schwer nachvollziehen und Fehler aufdecken.

Ein wenig Licht in den Zwiespalt aus prognostizierten Heilsversprechungen und heraufziehender Dystopie vermag die Analyse wichtiger philosophischer Leitfragen zu werfen: Verlieren Menschen mit zunehmender Digitalisierung ihre Selbstbestimmung und ihre Freiheit? Befördern digitale Technologien eine Selbstentfremdung? Kann die Wirkung digitaler Innovationen auf die Selbstbestimmung institutionell kontrolliert und reglementiert werden? Wir möchten diesen Leitfragen exemplarisch an zwei Alltagsszenarien im Gesundheitsbereich nachgehen: Informationsangebote zur medizinischen Selbstdiagnose im Internet und digitale Entscheidungshilfen für Ärzt*innen.

I Selbstbestimmung und Verantwortung – eine Begriffsbestimmung

Bevor wir damit beginnen können, die bestehenden und absehbaren Auswirkungen der digitalen Gesellschaftstransformationen auf die Selbstbestimmung der Bürger*innen zu untersuchen, ist es notwendig, unser Verständnis des Selbstbestimmungsbegriffs genauer zu umreißen. Der in der Alltagssprache gebräuchliche Begriff der *Selbstbestimmung* – in der Philosophie wird oft auch der Begriff der *Autonomie* synonym verwendet[2] – bezieht sich auf die

1 Vgl. Seele, Peter: »Envisioning the digital sustainability panopticon: a thought experiment of how big data may help advancing sustainability in the digital age«, in: Sustainability Science Vol. 11, No. 5 (2016), S. 845-854; Leclercq-Vandelannoitte, Aurélie: »An Ethical Perspective on Emerging Forms of Ubiquitous IT-Based Control«, in: Journal of Business Ethics Vol. 142, No. 1 (2017), S. 139-154.

2 Siehe beispielsweise: Seidel, Christian: Selbst bestimmen: Eine philosophische Untersuchung personaler Autonomie, Berlin: De Gruyter 2016, exemplarisch S. 13; Schnebel, Karin B.: »Freiheitsformen, Autonomie und Selbstbestimmung im Privaten«, in: Karin B. Schnebel (Hg.), Selbstbestimmung oder Geschlechtergerechtigkeit, Wiesbaden: Springer Fachmedien Wiesbaden 2015, exemplarisch S. 129f. Daneben existieren auch Arbeiten, die zwischen einer graduellen und kompetenzabhängigen Selbstbestimmung und einer in Relation zu dieser grundlegenderen Autonomie unterschei-

Fähigkeit, eigene Handlungsmotive und Lebensziele auszubilden, diese zu reflektieren, zu ändern und ihnen folgend zu handeln.[3] Selbstbestimmung ist somit weniger ein einzelner Handlungsmoment als vielmehr ein Prozess, der (1) die Bildung persönlicher Wünsche, Überzeugungen und Ideale, (2) die sich hieraus ergebende Ausbildung konkreter Handlungsintentionen und (3) die Überführung der Intentionen in authentische Handlungen umfasst.[4] Ein genauerer Blick auf die einzelnen Prozesselemente offenbart, wie diese die menschliche Fähigkeit der Selbstbestimmung konstituieren.

Willensfreiheit

Zunächst müssen selbstbestimmte Akteure über die Freiheit verfügen, die eigenen Handlungsmotive, Überzeugungen, Wünsche und Ideale eines guten Lebens reflektiert überprüfen und diese gegebenenfalls verändern zu können. Diese Unterscheidung zwischen bestehenden und mitunter intuitiven Handlungspräferenzen einerseits und den reflektierten Wünschen darüber, welche Präferenzen eine Person gerne besitzen würde, andererseits, arbeitet unter anderen der Philosoph Harry Frankfurt sehr prominent heraus. Unter der Bezeichnung *Volitionen erster* und *zweiter Ordnung* verdeutlicht er am Beispiel zweier Drogensüchtiger, wie Menschen ihren unmittelbaren Präferenzen folgen und dennoch keine selbstbestimmten Entscheidungen treffen können. Zwei Drogensüchtige, so beginnt Frankfurts Beispiel, setzen jeden Tag aufs Neue alles in ihrer Macht Stehende ein, um sich Drogen zu beschaffen. Der erste Süchtige kann sich mit der eigenen Rolle als Süchtiger gut identifizieren und würde sich auch nicht anders entscheiden wollen, wenn er keine körperlichen und psychischen Suchtzwänge verspüren würde. Er hat also die Präferenz (das heißt die *Volition erster Ordnung*), Drogen zu nehmen,

---

den. Hierzu: Gerhardt, Volker: Selbstbestimmung: Das Prinzip der Individualität, Ditzingen: Reclam 2018, S. 417f.

3 Vgl. Kant, Immanuel: Akademieausgabe von Immanuel Kants gesammelten Werken. Band IV: Kritik der reinen Vernunft. Prolegomena. Grundlegung zur Metaphysik der Sitten. Metaphysische Anfangsgründe der Naturwissenschaften, Berlin: De Gruyter 1968, 4:446.

4 Vgl. Dworkin, Gerald: The theory and practice of autonomy, Cambridge: Cambridge University Press 1988, S. 331; Wolf, Susan: »Sanity and the Metaphysics of Responsibility«, in: Ferdinand Schoeman (Hg.), Responsibility, Character, and the Emotions, New York: Cambridge University Press 1987, S. 46-62; Rössler, Beate: Der Wert des Privaten, Frankfurt a.M.: Suhrkamp 2001, S. 331f.

und wenn er über diese Präferenz genauer nachdenkt, kann er sie als einen authentischen Teil seines Selbst anerkennen. Im Gegensatz zum ersten wird der zweite Süchtige von seiner Sucht geplagt. Er fühlt sich durch seinen andauernden Suchtdruck regelrecht zu Handlungen genötigt, die er verabscheut. Der zweite Süchtige, so Frankfurts Analyse, ist ein Opfer seiner Begierden, weil es ihm nicht gelingt, seine Volitionen erster Ordnung an seine Volitionen zweiter Ordnung anzupassen.[5] Aus der Unterscheidung folgt aber nicht, dass selbstbestimmte Akteure ihre Handlungsintentionen immer auf Basis wohlüberlegter Motive bilden müssten. Menschen dürfen auch dann als selbstbestimmt gelten, wenn sie expressive Handlungen, wie einen Freudensprung, vollziehen.[6] Sie büßen ihre Selbstbestimmung nur dann ein, wenn sie ihre Gewohnheiten und spontanen Handlungen nicht willentlich beeinflussen können. In dem Sinne ist beispielsweise eine Person, die gerne eine Diät durchhalten würde, diese aus Gewohnheit aber immer wieder abbricht, in ihrem Essverhalten nicht selbstbestimmt. Die allgemeine Fähigkeit, Volitionen zweiter Ordnung zu bilden, ist ein konstitutives Element der Selbstbestimmung, das Akteuren eine freie Willensbildung zusichert, ohne gleichzeitig weitere, nicht reflektierte Ausdrücke der eigenen Identität pauschal als fremdbestimmte (heteronome) Elemente disqualifizieren zu müssen.

Eine viel diskutierte strukturelle Voraussetzung der freien Willensbildung ist die *Privatheit.*[7] Unter Privatheit ist weder ein von sozialen Gruppen isoliertes Leben noch ein Gegenbegriff zum politisch-öffentlichen Leben zu verstehen. Vielmehr ist mit Privatheit die Kontrolle darüber gemeint, mit der ein Mensch den Zugriff anderer Akteure auf die eigene Person und auf persönliche Informationen regulieren kann.[8] Wie genau hängt die Privatheit eines Menschen mit dessen Selbstbestimmung zusammen? Damit Menschen selbstbestimmte Entscheidungen treffen, diese realisieren und ihre Persönlichkeit im Laufe ihres Lebens mithilfe neuer Handlungsentscheidungen entwickeln können, müssen sie ihre Gedanken außerhalb normativer Zwangsräume reflektieren und den Zugang – auch den informationellen – zu ihrer Person reglementieren können. In sozialen Räumen, in denen diese Form der

5 Frankfurt, Harry G.: »Freedom of the Will and the Concept of a Person«, in: The Journal of Philosophy Vol. 68, No. 1 (1971), S. 5f.

6 Vgl. V. Gerhardt, Selbstbestimmung, S. 107ff.

7 Siehe auch den Beitrag von Nils Leopold in diesem Band.

8 Vgl. K. Schnebel, Freiheitsformen, Autonomie und Selbstbestimmung im Privaten, S. 129f.; B. Rössler, Der Wert des Privaten, S. 23f.

Privatheit nicht gegeben ist, beispielsweise in manchen religiösen Gemeinschaften, in der Mafia oder in besonders zeitintensiven Arbeitsbeziehungen, werden Akteure mitunter massive Probleme haben, frei über ihre Wünsche und Intentionen nachzudenken und *Volitionen zweiter Ordnung* zu entwickeln. Sie können möglicherweise nicht mit ihren religiösen Eltern über Zweifel in ihrem Glauben, mit ihrer mafiösen Familie über moralische Bedenken bei der Schutzgelderpressung oder mit ihren Arbeitskolleg*innen über den Sinn ihrer Arbeit sprechen (sofern derartige Zweifel überhaupt aufkommen). Ebenso schwer kann es Akteuren fallen, Überzeugungsänderungen in gewohnte Verhaltensweisen einfließen zu lassen und beispielsweise nicht mehr an religiösen Zeremonien teilzunehmen, keine Menschen mehr zu erpressen oder eine Unternehmenskultur abzuwandeln. All diese Verhaltensänderungen können vom unmittelbaren sozialen Umfeld registriert, abgelehnt und gegebenenfalls auch sanktioniert werden. Es ist dieser potenziell determinierende, soziale Zwang, der Alasdair MacIntyre dazu bewegt, soziale Milieus, in denen Akteure ihre eigenen Überzeugungen in herrschaftsfreien Diskursen bilden und prüfen können, als Voraussetzung selbstbestimmter und verantwortungsfähiger Akteure einzufordern.[9] Derartige soziale Milieus mögen Individuen im engen Freundes- oder Familienkreis und möglicherweise auch in intimen Chat- und Social-Media-Gruppen finden.[10]

Handlungsfreiheit

Damit selbstbestimmte Akteure ihre authentischen Handlungsintentionen in ihre Lebenswelt überführen und ihre Umwelt wirkmächtig beeinflussen können, müssen sie neben einer Willensfreiheit über ein Mindestmaß an *Handlungsfreiheit* verfügen. Beispielsweise kann eine passionierte Autofahrerin durch innere Faktoren, etwa durch eine Querschnittslähmung, oder durch äußere Faktoren, wie dem strafrechtlichen Entzug ihres Führerscheins, daran gehindert werden, ihre Passion auszuleben. Sobald also die Auswahl an Handlungsoptionen so eingeschränkt wird, dass Akteure ihre Intentionen nicht mehr adäquat realisieren können, ist auch ihre Möglichkeit begrenzt, die eigene Identität selbstbestimmt auszuleben. Nun könnte

9 MacIntyre, Alasdair »Social Structures and their Threats to Moral Agency«, in: Philosophy Vol. 74, No. 289 (1999), S. 317.

10 Vgl. Deutscher Ethikrat, Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung 2017, S. 191.

der Eindruck entstehen, dass jeder selbstbestimmte Akt eine Auswahl von Handlungsalternativen voraussetze und dass jede Reduktion von Handlungsalternativen automatisch die Fähigkeit zur Selbstbestimmung einschränke. Tatsächlich handelt es sich hierbei um einen Fehlschluss, wie unter anderem Michael Hardimon zeigt. Obwohl sich niemand dafür entschieden hat, in eine bestimmte Familie hineingeboren zu werden, so Hardimons Beispiel, können sehr viele Menschen die mit ihrer sozialen Zwangsrolle verknüpften Verantwortlichkeiten reflektieren und sich aktiv dazu entschließen, diese anzunehmen oder abzulehnen. Die jeweils damit einhergehende Auswahl an Handlungsalternativen hindert die Betroffenen nicht, ihren Intentionen folgend zu handeln. Die für die Selbstbestimmung notwendige Handlungsfreiheit ist dann gegeben, wenn die verfügbaren Handlungsoptionen adäquat zu den im Zeitverlauf entstandenen Handlungsintentionen passen und es zumindest die grundsätzliche Wahl zwischen Tun und Unterlassen einer Handlung gibt.[11]

Wissen und Folgenbewusstsein

Mit den konstitutiven Momenten der Willens- und Handlungsfreiheit geht die Notwendigkeit für selbstbestimmte Akteure einher, sich ein möglichst adäquates Bild über die absehbaren Folgen und Nebenfolgen von Handlungen zu machen. Auch dieser Umstand lässt sich einfach an einem Beispiel veranschaulichen: Angenommen, eine Patientin leidet an entsetzlichen Kopfschmerzen und bekommt von ihrer Hausärztin eine Reihe von Schmerzmedikamenten mit dem Hinweis verschrieben, die Patientin solle ausprobieren, welches für sie am besten wirke. Weil die Ärztin nur wenig Zeit hat und die Patientin nicht weiter nachfragen will, findet keine zusätzliche Aufklärung statt. Die Patientin befindet sich nun in der Lage, dass sie die Intention, ihre Schmerzen zu lindern, in die Tat umsetzen will, sie aber nicht abschätzen kann, welche der ihr offenstehenden Handlungsalternativen (in Form unterschiedlicher Kombinationen unbekannter Schmerzmittel) ihre Intention am

11 Hardimon, Michael O.: »Role Obligations«, in: The Journal of Philosophy Vol. 91, No. 7 (1994), S. 348; Pauen, Michael: »Willensfreiheit, Neurowissenschaft und die Philosophie«, in: Christoph S. Herrmann, Michael Pauen, Jochem W. Rieger & Silke Schicktanz (Hg.), Bewusstsein. Philosophie, Neurowissenschaften, Ethik, München, Wilhelm Fink Verlag 2005, S. 53ff.

besten realisieren könnte. Wenn sie in dieser Sache nicht bewusst den Zufall entscheiden lassen will, was an sich eine selbstbestimmte Handlung sein könnte, muss sie zunächst ihr Unwissen überwinden, indem sie sich mehr mit den Medikamenten befasst oder sich einen zusätzlichen fachlichen Rat einholt. An diesem Beispiel wird deutlich, dass Akteure über die Kompetenz verfügen müssen, sich Wissen anzueignen, mit dem sie die ihnen offenstehenden Handlungsalternativen erkennen und bewerten können. Nun sind menschliche Akteure in ihrer Fähigkeit, über bestimmte Sachverhalte so gut informiert zu sein, dass sie eine kompetente Folgenabschätzung leisten können, aus zwei Gründen prinzipiell eingeschränkt. Zum einen existieren Tatsachen, die noch nicht oder überhaupt nicht gewusst werden können. Beispielsweise hätte ein Arzt, der im 17. Jahrhundert Patient*innen versorgte und sich zwischen den einzelnen Untersuchungen nicht die Hände wusch, nicht wissen können, dass er mit seinem Hygieneverhalten höchstwahrscheinlich den Tod vieler Patient*innen verursacht. Mit dem jeweils aktuellsten wissenschaftlichen Erkenntnisstand sind folglich notwendige Grenzen der Selbstbestimmung umrissen.[12]

Zum anderen bestehen relative Informations- und Wissenslücken, die sich auf die vorhersehbaren Folgen und Nebenfolgen von Handlungsalternativen beziehen. Relatives Nichtwissen liegt genau dann vor, wenn sich Akteure in einem zumutbaren Rahmen informieren und ihre Wissenslücken dadurch selbstständig schließen können.[13] Wichtige, praktische Maßnahmen zur Förderung der Selbstbestimmung, so werden wir im folgenden Abschnitt argumentieren, sind einerseits die Vermittlung von Kompetenzen zum sicheren Erkennen und Verstehen von Informationen und andererseits die Bereitstellung verständlicher und praktisch nutzbarer Informationen.

---

12 Vgl. Annerl, Felix: »Die zunehmend verantwortungslose Rede von der Verantwortung«, in: Werner Leinfellner (Hg.), Die Aufgaben der Philosophie in der Gegenwart (Schriftenreihe der Wittgenstein-Gesellschaft; 12,1). Wien: Hölder-Pichler-Tempsky 1986, S. 272.

13 Clarke, Randolph: »Blameworthiness and Unwitting Omissions«, in: Dana Kay Nelkin & Samuel C. Rickless (Hg.), The Ethics and Law of Omissions (Bd. 1.), Oxford: Oxford University Press 2017, S. 63-83; Ginet, Carl: »The Epistemic Requirements for Moral Responsibility«, in: Philosophical Perspective Vol. 34 (2000), S. 275f. Wann genau eine relative Unwissenheit authentisch vorliegt ist schwer festzustellen, weil die betroffenen Akteure ja selbst nicht wissen, was sie nicht wissen aber hätten wissen können. Siehe hierzu: Zimmerman, Michael J.: An essay on moral responsibility, Totowa, NJ: Rowman & Littlefield 1988, S. 41.

Verantwortung

Eng mit dem Begriff der Selbstbestimmung und der Wissensbedingung sind *Verantwortungskonzepte* verknüpft. Wer selbstbestimmt handelt, der hat Gründe für das eigene Handeln und kann sich auf Basis dieser Gründe *verantworten*.[14] Wer seine Handlungen frei wählt, der kann auf die Frage »Warum hast du das gemacht?« mit Gründen antworten. Die Wechselwirkung zwischen den Begriffen fängt Gerald Dworkin passend ein, wenn er bemerkt, »autonomy is centrally associated with the notion of individual responsibility. The freedom to make decisions for oneself carries with it the obligation to answer for the consequences of those decisions.«[15]

Verantwortung bedeutet auch, dass Akteure bestimmte Aufgaben, wie beispielsweise die, sich als Pflegekraft in einem Krankenhaus um Patient*innen zu kümmern, als eine ihnen zugehörige Aufgabe anerkennen. Zur Erfüllung dieser Aufgabe muss die Pflegekraft einiges über die Pflege erkrankter Menschen wissen. Je nachdem, welche Fortschritte die Pflegeforschung macht, kann von der Pflegekraft verlangt werden, den eigenen Wissens- und Fähigkeitsstand an das aktuelle Forschungswissen anzupassen, damit sie ihre Aufgaben auch weiterhin verantwortlich bewältigen kann. Schließlich kann die Pflegekraft für die Art und Weise, wie sie versucht ihrer Aufgabe gerecht zu werden, für ihre Erfolge und ihre Verfehlungen von anderen Akteuren (Patient*innen, Gerichte, Angehörige usw.) zu einer Rechtfertigung genötigt und gegebenenfalls gelobt oder getadelt werden. Die Bedingungen, die Akteure erfüllen müssen, um als verantwortungsfähig anerkannt zu werden, überschneiden sich in vielen Punkten mit den Voraussetzungen selbstbestimmten Handelns.[16]

---

14 Dettinger, Frank: Radikale Selbstbestimmung (= Collegium Metaphysicum, Band 12), Tübingen: Mohr Siebeck 2015, S. 55ff.

15 G. Dworkin, The theory and practice of autonomy, S. 102.

16 Ausgesprochen detailliert diskutiert Janina Loh (geb. Sombetzki) die Bedingungen der Verantwortungsfähigkeit und kommt in ihrer Analyse auf insgesamt sieben Aspekte der Handlungsfähigkeit und der Urteilskraft, die sich mit dem oben konstruierten Begriff der Selbstbestimmung überschneiden. Siehe hierzu: Sombetzki, Janina: Verantwortung als Begriff, Fähigkeit, Aufgabe Eine Drei-Ebenen-Analyse, Wiesbaden: Springer VS 2014, S. 62ff.

Menschenwürde

Abschließend ist es wichtig, auf den *rechtlichen* und *normativen Status* menschlicher Akteure einzugehen, der nicht an konkrete Fähigkeiten gebunden ist.[17] Mit der grundrechtlich garantierten Menschenwürde kommen allen Bürger*innen dieselben negativen und positiven Freiheitsrechte zu.[18] Aus rechtlicher und auch aus moralphilosophischer Perspektive ist die grundsätzliche Annahme, dass alle Menschen Würde besitzen, schon allein deswegen sinnvoll, weil Menschen sich anhand dieses Status wechselseitig als gleichwertige, moralisch autonome Akteure anerkennen müssen. Würde die graduelle Selbstbestimmung nicht um einen derartigen, kategorischen Status ergänzt werden, gäbe es für Menschen keinen Grund, sich als moralisch und rechtlich gleichwertige Akteure anzuerkennen.[19] In dem Fall ließe sich der gezielte Mord an anderen Menschen oder die politische Unterwerfung gesellschaftlicher Gruppen zunächst als Akt der Selbstbestimmung ausweisen. In der deutschen Rechtsordnung macht sich das allen Bürger*innen gleichermaßen zukommende Recht auf Selbstbestimmung und freie Entfaltung der Persönlichkeit an vielen Stellen bemerkbar: allen voran im allgemeinen Persönlichkeitsrecht (Art.2 Abs.1 in Verbindung mit Art. 1 Abs. 1 GG).[20]

Zusammengefasst konstituiert sich die menschliche Selbstbestimmung aus (1) der Willensfreiheit, die eigenen Wünsche, Überzeugungen und Ideale des guten Lebens ausbilden, reflektieren und verändern zu können, (2) aus der Fähigkeit, diese Vorstellungen in konkrete und authentische Handlungsintentionen zu überführen, und (3) aus der Handlungsfreiheit, passende Handlungsoptionen wählen und in die Tat umsetzen zu können. Eine notwendige

17 Vgl. Feinberg, Joel: Harm to Self: The Moral Limits of the Criminal Law, New York: Oxford University Press 1989, S. 52.

18 Vgl. Wolff, Robert P.: »The Conflict Between Authority and Autonomy«, in: Joseph Raz (Hg.), Authority, Oxford: Blackwell 1990, S. 20; Dowding, Keith M.: Rational choice and political power, Brookfield: Edward Elgar Publishing 1991, S. 48.

19 Zu diesem Argument siehe: Arneson, Richard .J: »What, if Anything, Renders All Humans Morally Equal?«, in: Jamieson Dale (Hg.), Singer and His Critics, Oxford: Wiley-Blackwell 1999, 103ff. Zum Begriff der Menschenwürde siehe exemplarisch: Dreier, Horst/Huber, Wolfgang: Bioethik und Menschenwürde, Münster: LIT 2002.

20 Vgl. Lindner, Josef Franz: »Das Paradoxon der Selbstbestimmung«, in: Josef Franz Lindner (Hg.), Selbst- oder bestimmt? Illusionen und Realitäten des Medizinrechts (Schriften zum Bio-, Gesundheits- und Medizinrecht, Band 30), Baden-Baden: Nomos 2017, S. 9f.

Voraussetzung für die Prozessschritte zwei und drei ist eine angemessene Wissenskompetenz, mit der die passenden Handlungsoptionen auch als solche erkannt werden können. Je besser Akteure jeden einzelnen dieser Prozessschritte beherrschen, desto größer ist ihre Fähigkeit, authentisch zu handeln und ihre Integrität zu wahren.

II Die Grenzen menschlicher Selbstbestimmung im digitalen Raum

Bis hierhin sollte der graduelle und prozesshafte Charakter der Selbstbestimmung deutlich geworden sein.[21] Menschliche Akteure sind nicht entweder nur selbst- oder nur fremdbestimmt. So wird die Patientin aus dem vorangegangenen Arzneimittelbeispiel nicht pauschal als fremdbestimmt eingestuft, wenn sie ohne weitere Recherchen eines der Schmerzmedikamente ausprobiert, die ihr verschrieben wurden.[22] Der Fall ändert sich erst, wenn sie ganz bewusst vermeiden will, ihre Medikamente auf gut Glück zu nehmen, aber keine für sie praktische Möglichkeit findet oder finden könnte, ihre Unwissenheit zu überwinden. In dem Fall handelt die Patientin in Bezug auf ihren Arzneimittelkonsum (und nicht global) nur beschränkt selbstbestimmt. Menschen hegen zu unterschiedlichen Zeitpunkten und in unterschiedlichen Bereichen ihrer Lebenswelt ganz unterschiedliche Wünsche, sie besitzen mal mehr und mal weniger Handlungs- und Willensfreiheit und sie verfügen in einigen Bereichen über ein Spezialwissen, während sie in anderen gänzlich uninformiert sind.

Dasselbe gilt auch für den digitalen Raum. Im Umgang mit digitalen Technologien bezieht sich die Handlungs- und Willensfreiheit selbstbestimmter Akteure auf die Fähigkeit, diese kompetent zu nutzen, zu kritisieren und gegebenenfalls auch zugunsten nicht digitaler Handlungsalternativen

21 Vgl. J. Feinberg, Harm to Self: The Moral Limits of the Criminal Law, S. 27ff.; S. Wolf, Sanity and the Metaphysics of Responsibility, S. 62.

22 Tatsächlich ist der Moment, ab dem ein Akteur als fremdbestimmt gelten darf, recht umstritten. So besteht beispielsweise eine Kontroverse darüber, ob Menschen, die Teile ihre Selbstbestimmung freiwillig und über einen längeren Zeitraum an andere Akteure abtreten (z.B. Soldat*innen) oder die persönlichkeitsverändernden Substanzen einnehmen (z.B. Psychopharmaka), noch als selbstbestimmte Akteure betrachtet werden dürfen. Siehe hierzu ausführlich: Oshana, Marina A.L.: »Personal Autonomy and Society«, in: Journal of Social Philosophy Vol. 29, No. 1 (1998), S. 92f.; G. Dworkin, The theory and practice of autonomy, S. 18 und 29.

abzulehnen.[23] Damit geht die Möglichkeit einher, die digitale Darstellung der eigenen Person durch die eigenen Handlungen mitzugestalten. Denn ebenso wie in der analogen Welt können Menschen nur dann ihr Recht auf Privatheit ausüben und sich in geschützten sozialen Sphären reflektiert mit neuen Technologien auseinandersetzen, wenn sie in der Lage sind, den unerwünschten Zugriff Dritter auf ihre persönlichen Informationen zu kontrollieren und ihre eigenen Handlungsräume zutreffend einzuschätzen.[24] Umrahmt werden diese fähigkeitsbezogenen Voraussetzungen von juristischen Schutzmechanismen.[25] Bürger*innen werden unter anderem durch gesetzliche Mindeststandards in der Produkt- und Softwaresicherheit, durch das Recht auf informationelle Selbstbestimmung und durch die europäische Datenschutz-Grundverordnung in ihrem Status als selbstbestimmte Individuen bestätigt.

Gesellschaften können die Selbstbestimmung ihrer Bürger*innen im digitalen Raum fördern, indem sie einerseits strukturelle Hürden gezielt identifizieren und diese abbauen und andererseits Kompetenzen für ein selbstbestimmtes Leben aktiv fördern. Im Folgenden möchten wir zwei klassische Problembereiche hervorheben, die für den medizinischen Kontext besonders relevant sind: erstens Informationsasymmetrien und Kompetenzen, zweitens Privatheit.

Informationsasymmetrien und Kompetenzen

Als Informationsasymmetrie werden Phänomene bezeichnet, in denen kooperierende Akteure wie Patient*innen, Leistungserbringer wie Ärzt*innen und Physiotherapeut*innen sowie Leistungsträger und Ministerien über einen unterschiedlichen Informationsstand und -zugang verfügen und ihre Handlungsoptionen und die damit verbundenen Handlungsfolgen unterschiedlich gut abwägen können. Das Problem, das sich aus diesem Phänomen für die Selbstbestimmung ergeben kann (aber nicht muss), schildern Tina

23 Vgl. Groeben, Norbert: »Anforderungen an die theoretische Konzeptualisierung von Medienkompetenz«, in: Norbert Groeben & Bettina Hurrelmann (Hg.), Medienkompetenz: Voraussetzungen, Dimensionen, Funktionen. Weinheim: Juventa-Verlag 2002, S. 11-22. Für eine realpolitische Beachtung dieses Themas siehe exemplarisch: Vereinigung der Bayerischen Wirtschaft: »Gesundheit und Medizin. Analyse und Handlungsempfehlungen 2018«, S. 13.

24 Vgl. B. Rössler, Der Wert des Privaten, S. 23ff.

25 Vgl. Datenethikkommission: Gutachten 2019, Berlin 2019, S. 44.

Harrisson, Kathryn Waite und Gary Hunter treffend: »Information incompleteness and information asymmetry do not provide conditions where individuals feel they have all the information to act, in a sense rendering them powerless.«[26]

Die typische Beziehung zwischen Ärzt*innen und Patient*innen ist von derartigen Informationsasymmetrien geprägt. Ärzt*innen wissen in der Regel mehr über Krankheiten als ihre Patient*innen und sie können meist auch den Erfolg einzelner Therapieoptionen kompetenter abschätzen. Darüber hinaus besitzen Ärzt*innen einen leichteren Zugang zu gesicherten Gesundheitsinformationen und einen exklusiven Zugang zu vielen medizinischen Handlungsalternativen, beispielsweise die Möglichkeit, Arzneimittel zu verschreiben. Ärzt*innen, die zusätzlich eine medizinische Studie leiten, können über ein exklusives Fachwissen und den Zugang zu neuartigen Arzneimitteln und medizinischen Interventionen verfügen.[27] Im Kontrast dazu stützen Patient*innen ihre Entscheidungen in den meisten Fällen auf ein Laienwissen – selbst dann, wenn der Arzt oder die Ärztin gute Aufklärungsarbeit leistet. Umgekehrt sind auch Ärzt*innen von der Asymmetrie betroffen, wenn sie nicht über die Lebensumstände, Werte, Präferenzen und Einstellungen der Patientin oder des Patienten informiert sind. Um eine Behandlung nach dem Patient*innenwohl ausrichten zu können, muss Ärzt*innen und Patient*innen daran gelegen sein, die Informationsasymmetrien wechselseitig abzubauen.

Während sich Informationsasymmetrien im analogen Alltag vergleichsweise einfach umreißen lassen, fällt ihre genaue Identifizierung und Bewertung im digitalen Raum ungleich schwerer. So tragen viele digitale Gesundheitsportale aktiv zu einem großflächigen Abbau gesellschaftlicher Informationsasymmetrien bei und unterstützen damit die bürgerliche Selbstbestimmung. Auch diese Entwicklung wird im medizinischen Kontext deutlich. Menschen können mithilfe von Online-Videos selbstständig präventive Gesundheitsübungen durchführen, sie können in Gesundheitsportalen medizinische Fachbegriffe nachschlagen, die sie bei ihrem Arztbesuch nicht verstanden haben, sie können über Suchmaschinen nach Diagnosen und

26 Harrison, Tina/Waite, Kathryn/Hunter, Gary L.: »The internet, information and empowerment«, in: European Journal of Marketing Vol. 40, No. 9/10 (2006), S. 975.

27 Vgl. Miller, Franklin G.: »Consent in Clinical Research«, in: Franklin G. Miller & Alan Wertheimer (Hg.), The ethics of consent: theory and practice, New York: Oxford University Press 2010, S. 38.

Therapiemöglichkeiten für auffällige Symptome suchen oder sie können auf sozialen Plattformen einzelnen Gruppen zu bestimmten Krankheitsbildern beitreten und sich im Chat mit anderen ein lebensweltliches Bild von den Folgen und Nebenfolgen unterschiedlicher Therapiewege machen. Dieselben Technologien können aber auch Informationsasymmetrien vergrößern, indem sie den Nutzer*innen beispielsweise eine zu große und unübersichtliche Menge an qualitativ sehr unterschiedlichen Informationen anbieten, die diese kaum kompetent beurteilen können.

Privatheit

Neben dem Zugang zu und der kompetenten Nutzung von Informationen ist die Kontrolle des Zugangs zu den persönlichen Informationen im digitalen Raum ein wichtiger Faktor, der sich entschieden auf die Selbstbestimmung auswirkt. Damit ist nicht gemeint, dass selbstbestimmte Menschen sich dadurch auszeichnen, dass sie der Welt nur ideale Momente ihrer selbst zugänglich machen, beispielsweise mit ausschließlich inszenierten Instagram-Bildern und choreografierten Facebook-Stories. Vielmehr geht es um die Frage, welche Akteure im digitalen Raum unter welchen Bedingungen auf die personenbezogenen Daten anderer Menschen zugreifen und diese gegebenenfalls auch analysieren, verändern und weitergeben dürfen. Tiefgreifende Einschränkungen individueller Selbstbestimmung lauern im unbefugten Datenzugriff, im Datendiebstahl und in der Speicherung, Verarbeitung und Weitergabe von Daten ohne das Wissen der Betroffenen. Im Vergleich zum Diebstahl physischer Gegenstände besitzt sein digitales Pendant die zusätzliche Eigenschaft, dass der entstandene Schaden nicht durch die Rückgabe des Diebesguts kompensiert werden kann. Gestohlene, digitale Informationen können immer wieder kopiert und geteilt werden und sie verschwinden nicht aus den Köpfen unbefugt Wissender, nachdem der Diebstahl aufgeklärt wurde.[28] Dies gilt umso mehr für digitale Informationen in den Datenbeständen international vernetzter Akteure.

Ein ebenfalls ernster Eingriff in die Privatheit kann durch Anwendungen erfolgen, denen die Nutzer*innen mit ihrer Einwilligung in die Nutzungserklärung gestatten, ihre personenbezogenen Daten ohne weitere Rücksprache zu verarbeiten und diese weiterzugeben. Paradoxerweise erfolgt diese

28 Vgl. Starr, Paul: »Health and the Right to Privacy«, in: American Journal of Law & Medicine, Vol. 25, No.2 (1999), S. 196f.

Freigabe nämlich häufig trotz massiver Bedenken der Nutzer*innen.[29] Es ist intuitiv recht einfach nachzuvollziehen und empirisch belegt, dass soziale Medien in vielen Gesellschaften ein fester Bestandteil des Alltags sind und die meisten Menschen darum auch eine Volition erster Ordnung besitzen, diese zu nutzen. Gleichzeitig können sich dieselben Nutzer*innen um ihre Privatsphäre im Internet sorgen und sich wünschen, die Nutzungsbedingungen der entsprechenden Dienste nicht zu bestätigen. Sie schaffen es aber nicht, diese Volition zweiter Ordnung durchzusetzen. Diese Einschränkung der Selbstbestimmung kann durch Wissenslücken und fehlende digitale Kompetenzen verstärkt werden, sobald die Nutzer*innen die unmittelbaren Vor- und/oder Nachteile ihrer Datenfreigabe nicht erkennen. So können beispielsweise Räume wie Facebook-Gruppen, Messenger-Dienste und Online-Foren den Nutzer*innen das Gefühl vermitteln, in besonders privaten und geschützten Milieus zu agieren. Fitnessuhren, intelligente Kleidungsstücke oder Smart-Home-Devices fügen sich so nahtlos in den Alltag der meisten Menschen ein, dass diese gleichsam unbewusst genutzt werden können. Der Prozess der Datengenerierung rückt in den Hintergrund.[30]

Als Spannungsmomente bei der persönlichen Wahrung von Selbstbestimmung im digitalen Raum haben wir also (1) digitale Informationsasymmetrien, (2) digitale Kompetenz und (3) Probleme des Datenschutzes, der Datensicherheit und Zugriffskontrolle identifiziert.

29 Vgl. Engels, Barbara: »Datenschutzpräferenzen von Jugendlichen in Deutschland«, in: Vierteljahresschrift zur empirischen Wirtschaftsforschung aus dem Institut der deutschen Wirtschaft, Vol.45, No. 2 (2018), S. 5ff.

30 Vgl. Mikal, Jude/Hurst, Samantha/Conway, Mike: »Ethical issues in using Twitter for population-level depression monitoring: A qualitative study«, in: BMC Medical Ethics Vol. 17, No. 1 (2016), S. 22; Kang, Hyun G. u.a.: »In situ monitoring of health in older adults: technologies and issues«, in: Journal of the American Geriatrics Society Vol. 58, No. 8 (2010), S. 1579-1586; Balestra, Martina/Shaer, Orit/Okerlund, Johanna/Westendorf, Lauren/Ball, Madeleine/Nov, Oded: »Social Annotation Valence: The Impact on Online Informed Consent Beliefs and Behavior«, in: Journal of Medical Internet Research Vol. 18 (2016).

III Wie verändert die Digitalisierung die Selbstbestimmung im Gesundheitswesen?

In der Humanmedizin verspricht die Digitalisierung wissenschaftliche und versorgungspolitische Quantensprünge. So glauben beispielsweise die beiden Gesundheitsökonom*innen Michael Hoy und Julia Witt mithilfe großflächiger Gen-Scans bei Personen mit familiär auftretenden Brustkrebsfällen, die Früherkennung von Brustkrebs und damit die Heilungschancen dramatisch verbessern und, als unmittelbare Folge davon, die Gesundheitskosten erheblich senken zu können.[31] Andererseits mahnen Kritiker*innen vor den Gefahren, die mit der Digitalisierung persönlicher Gesundheitsinformationen einhergehen. Die normativen Spannungen zwischen medizinisch relevanten, digitalen Technologien auf der einen Seite und den Selbstbestimmungsrechten und Interessen individueller, institutioneller und gesellschaftlicher Akteure auf der anderen Seite sind komplex.[32] Welche Auswirkungen diese Spannung auf die individuelle Selbstbestimmung haben kann, werden wir exemplarisch für die beiden Bereiche Informationsangebote zur medizinischen Selbstdiagnose im Internet und digitale Entscheidungshilfen für Ärzt*innen herausarbeiten.

Informationsangebote zur medizinischen Selbstdiagnose im Internet

Die Kompetenzen, die Patient*innen zur Wahrung ihrer Selbstbestimmung während einer persönlichen ärztlichen Behandlung an den Tag legen müssen, stellen viele Menschen bereits vor große Herausforderungen. Sie müssen in der Lage sein, bei Beschwerden eine Ärztin oder einen Arzt aufzusuchen und ihr oder ihm die eignen Symptome zu schildern. Sie müssen die Informationen verstehen können, die sie von ihrer Ärztin oder ihrem Arzt erhalten (zum Beispiel eine Diagnose und passende Therapieoptionen), und sie müssen die erhaltenen medizinischen Empfehlungen korrekt befolgen können (zum Beispiel eine bestimmte Menge von Arzneimitteln in einem bestimmten Intervall

31 Hoy, Michael/Witt, Julia: »Welfare Effects of Banning Genetic Information in the Life Insurance Market: The Case of BRCA1/2 Genes«, in: Journal of Risk & Insurance Vol. 74, No. 3 (2007), S. 523-546.

32 Vgl. Jannes, Marc/Friele, Minou/Jannes, Christiane/Woopen, Christiane: Algorithmen in der digitalen Gesundheitsversorgung. Eine interdisziplinäre Analyse, Gütersloh: Bertelsmann Stiftung 2018, S. 21f.

oral einnehmen). Viele andere Kompetenzen, auf die selbstbestimmte Menschen in anderen Kontexten üblicherweise angewiesen sind, können im Verhältnis zwischen Ärzt*innen und Patient*innen durch Vertrauen kompensiert werden. Die Patient*innen dürfen darauf vertrauen, dass die fachlichen Kompetenzen der Ärzt*innen in Deutschland durch streng regulierte Aus-, Fort- und Weiterbildungen geprüft und regelmäßig erweitert werden. Außerdem dürfen sie davon ausgehen, dass die Gesinnung der Ärzt*innen sich am Patientenwohl orientieren muss. Etliche Gesetze, ein stark ausgeprägtes Berufsethos[33] und gesellschaftliche Erwartungshaltungen sorgen dafür, dass dieses Vertrauen nicht enttäuscht wird.

Anstatt das leichte Stechen in der Brust, einen neuen Leberfleck oder anhaltende Schluckbeschwerden zum Anlass zu nehmen, eine Ärztin oder einen Arzt aufzusuchen, ist mittlerweile für viele Menschen die Konsultation von »Dr. Google« üblich geworden.[34] In eine Suchmaske geben Nutzer*innen Symptome und vermutete Erkrankungen ein und werden auf Webseiten weitergeleitet, auf denen ihnen unterschiedliche Diagnosen vorgeschlagen, medizinische Fachbegriffe erklärt, Präventions- und Therapiealternativen präsentiert und Erfahrungsberichte von Menschen mit ähnlichen Suchanfragen zugänglich gemacht werden. Daneben erhalten die Nutzer*innen auch Informationen, nach denen sie nicht gesucht haben, beispielsweise ein Angebot für eine neue Gesundheits-App, die Konditionen einer Online-Apotheke oder die Adresse einer Facharztpraxis in der unmittelbaren Umgebung. Wie wirkt sich die medizinische Konsultation des Internets auf die Selbstbestimmung aus?

Wie bereits erwähnt, kann die individuell schnell verfügbare, digitale Vermittlung von Gesundheitsinformationen in einem erheblichen Maße Informationsasymmetrien abbauen und damit die Selbstbestimmung von Bürger*innen im Hinblick auf ihr Gesundheitswissen und -verhalten stärken. Um diesen Vorteil allerdings genießen zu können, müssen die Bürger*innen über gute *Digital-* und *Gesundheitskompetenzen* verfügen.[35] Sie müssen Werbebotschaften von Fachinformationen, unseriöse von seriösen

33 Vgl. Lichtenthaeler, Charles: Der Eid des Hippokrates. Ursprung und Bedeutung, Köln: Deutscher Ärzte-Verlag 1984, S. 325ff.

34 Vgl. Jutel, Annemarie: »›Dr. Google‹ and his predecessors«, in: Diagnosis Vol. 4, No. 2 (2017), S. 87-91; Rossmann, Constanze/Lampert, Claudia/Stehr, Paula/Grimm, Michael: Nutzung und Verbreitung von Gesundheitsinformationen, Gütersloh: Bertelsmann Stiftung 2018, S. 8.

35 Vgl. Samerski, Silja/Müller, Hardy: »Digitale Gesundheitskompetenz in Deutschland – gefordert, aber nicht gefördert? Ergebnisse der empirischen Studie TK-DiSK«, in: Zeit-

Anbietern und qualitativ minderwertige von hochwertigen Gesundheitsinformationen unterscheiden können und sie müssen Grundkenntnisse über die Funktionsweise von Suchalgorithmen und den Aufbau von Webseiten besitzen. Diese Kompetenzanforderungen können auf soziale Gruppen, die wenig mit digitalen Medien vertraut sind, sowie auf ökonomisch schwächere Gruppen, die nicht über die notwendigen Endgeräte verfügen, diskriminierend wirken.[36] Nutzer*innen können aber nicht nur durch mangelnde Kompetenzen, sondern auch durch strukturelle und technische Faktoren in ihrer Selbstbestimmung eingeschränkt werden. Meiden Patient*innen den Arztbesuch und diagnostizieren sich stattdessen ausschließlich selbst, verlieren sie möglicherweise eine wichtige Kontroll- und Informationsinstanz. Im direkten Gespräch können Ärzt*innen ihre Patient*innen über gesundheitliche Themen informieren, die diese vielleicht nicht hören wollen, beispielsweise eine unliebsame Diagnose. Bei der selbstständigen Online-Recherche hingegen können Patient*innen gezielt nur solche Informationen aufnehmen, die ihr Weltbild bestätigen.[37] Auch technisch kann ein einseitiges Informationsangebot befördert werden. Die Anbieter von Suchalgorithmen wie Google, Bing und Co., die nicht dem Patientenwohl verpflichtet sind,[38] können Werbepartner prominent platzieren, sie können die Suchergebnisse an die Präferenzen ihrer Nutzer*innen anpassen, wodurch diese gegebenenfalls wichtige Gesundheitsinformationen nicht finden, und sie können weitere systembedingte und strategische Gewichtungen vornehmen.[39] Dieser Gewichtungsprozess kann nicht nur durch privatwirtschaftliche Gewinnambitionen, sondern auch durch staatliche Schutz-

schrift für Evidenz, Fortbildung und Qualität im Gesundheitswesen, Vol.144 (2019), S. 49.

36 Im englischen ist dieses Phänomen unter der Bezeichnung »digital divide« bekannt. Siehe hierzu: Baldini, Gianmarco/Botterman, Maarten/Neisse, Ricardo/Tallacchini, Mariachiara: »Ethical Design in the Internet of Things«, in: Science and Engineering Ethics, Vol. 24, No. 3 (2018), S. 908.

37 Das psychologische Phänomen ist unter der Bezeichnung »confirmation bias« bekannt. Siehe hierzu exemplarisch: Zimbardo, Philip George/Johnson, Robert L/McCann, Vivian: Psychology: Core Concepts, Harlow Essex: Pearson 2012.

38 Vgl. A. Jutel, »›Dr. Google‹ and his predecessors«, S. 87f.

39 Vgl. Rost, Martin: »Zur Soziologie des Datenschutzes«, in: Datenschutz und Datensicherheit Vol. 37, No. 2 (2013), S. 85; J. Bray, Jeffery/Johns, Nick/Kilburn, David: »An Exploratory Study into the Factors Impeding Ethical Consumption«, in: Journal of Business Ethics Vol. 98, No. 4 (2011), S. 597-608; Siehe auch: Stiftung Warentest: »Suchen, ohne durchsucht zu werden«, Ratgeber von 2019.

und Nudging-Bestrebungen[40] motiviert werden und eröffnet die Frage, welche Akteure aus welchen Gründen Suchanfragen beeinflussen dürfen. Ein Beispiel hierfür ist die Kooperation, die das Gesundheitsministerium mit Google anstrebte, in deren Folge gesundheitliche Suchanfragen prominent an die Seite »gesund.bund.de« verwiesen werden sollten.[41] Diese Kooperation wurde gerichtlich per einstweiliger Verfügung untersagt.[42] Der Bias der Suchalgorithmen wird aber nicht nur durch ihre Betreiber programmiert, sondern auch durch das Suchverhalten der Nutzer*innen trainiert.[43] Er kann sich an den ökonomisch interessantesten Nutzer*innengruppen und/oder den Gruppen orientieren, welche die größte Menge an relevanten Daten erzeugen. Er erlernt anhand dieser Gruppen, die eigenen Suchprozesse zu optimieren, und berücksichtigt in der Folge möglicherweise Diagnosen und Krankheitssymptome weniger, die insbesondere bei unterrepräsentierten Gruppen vermehrt auftreten.[44] Sofern digitale Technologien als Ersatz und nicht als Ergänzung zur Vertrauensbeziehung zwischen Ärzt*innen und Patient*innen verstanden werden, kann sich die soziale Praxis der Selbstdiagnose im Internet negativ auf die Selbstbestimmung der Patient*innen auswirken.

Angesichts dieser teils beabsichtigten und teils unvorhersehbaren Informationsverengungen dürfte es einigen Nutzer*innen schwerfallen, die Qualität einer ermittelten Diagnose abzuschätzen und aus dieser geeignete Handlungsoptionen zu ziehen. Damit das digitale Informationsangebot also tat-

40 Ein *Nudge*, zu Deutsch »Stupser«, bezeichnet die Beeinflussung einer Entscheidung auf eine Weise, dass die handelnden Akteure jederzeit frei wählen können, die »richtige« Entscheidung aufgrund der bestehenden Entscheidungsstruktur aber am einfachsten zu realisieren ist. Siehe hierzu beispielsweise: Thaler, Richard H./Sunstein, Cass R.: Nudge: improving decisions about health, wealth, and happiness, New York: Penguin Books 2009.

41 Bundesministerium für Gesundheit: »verlässliche Gesundheitsinfos leichter finden« (Pressemitteilung 10.11.2020). https://www.bundesgesundheitsministerium.de/presse/pressemitteilungen/2020/4-quartal/bmg-google.html

42 Vgl. Landesgericht München: »Netdoktor gegen BRD und Google: Vereinbarung über Knowledge Panels kartellrechtswidrig« (Pressemitteilung Nr. 6 vom 10.02.2021). https://www.justiz.bayern.de/gerichte-und-behoerden/landgericht/muenchen-1/presse/2021/6.php

43 Vgl. Lewandowski, Dirk: Suchmaschinen verstehen, Berlin: Springer 2018, S. 292.

44 Vgl. De Laat, Paul B.: »Algorithmic decision-making based on machine learning from big data: Can transparency restore accountability?«, in: Philosophy & Technology, Vol. 31 (2018), S. 525-541.

sächlich die Selbstbestimmung befördert, müssen erstens die Nutzer*innen aktiv ihre Digital- und Gesundheitskompetenz überprüfen und diese gegebenenfalls verbessern; zweitens müssen staatliche und private Akteure aktiv den Kompetenzerwerb der Nutzer*innen unterstützen (zum Beispiel durch die Vermittlung digitaler Kompetenzen in Schulen, Aufklärungskampagnen usw.);[45] drittens müssen qualitativ hochwertige Angebote verfügbar gemacht werden[46] und viertens müssenrechtliche Rahmenbedingungen gestärkt werden, die eine Irreführung und Fehlinformation verhindern.[47]

Digitale Entscheidungshilfen für Ärzt*innen

Selbstlernende Algorithmen können Ärzt*innen darin unterstützen, Diagnosen zu erstellen und Therapieoptionen zu ermitteln. Mithilfe umfangreicher Datensätze (Forschungsdaten, Daten aus Krankenakten, Sensordaten, Biobanken u.v.m.) können Algorithmen daraufhin trainiert werden, anhand unterschiedlichster Parameter Krankheitsbilder zu erkennen und Therapieoptionen auf individuelle Krankheitsverläufe hin abzustimmen. Sofern das algorithmische System evidenzbasiert und fehlerfrei funktioniert, hilft es Ärzt*innen, keine Diagnose und Therapiemöglichkeiten zu übersehen und keine statistisch relevanten Symptome falsch einzuschätzen.[48] Ein Bereich, in dem derartige algorithmische Entscheidungsunterstützungssysteme bereits erfolgreich eingesetzt werden, ist die Früherkennung von Diabetes am Bild der Netzhaut, bei der schon heute intelligente Computersysteme zutreffendere Diagnoseergebnisse erzielen als menschliche Expert*innen.[49]

---

45 Klick2Health, Onlineangebot (2021).

46 Vgl. The US National Institute of Health, Onlineangebot (2021); Das nationale Gesundheitsportal in Deutschland (2021).

47 Ein Beispiel hierfür ist das §20k SGB V, das die Krankenkassen dazu auffordert, die digitale Gesundheitskompetenz ihrer Mitglieder zu fördern.

48 Vgl. Mesko, Bertalan: »The role of artificial intelligence in precision medicine«, in: Expert Review of Precision Medicine and Drug Development, Vol. 2, No. 5 (2017), S. 239-241; Gräßer, Felix u.a.: »Therapy decision support based on recommender system methods«, in: Journal of Healthcare Engineering (2017), S. 1-11.

49 Vgl. Gulshan, Varun, u.a.: »Development and Validation of a Deep Learning Algorithm for Detection of Diabetic Retinopathy in Retinal Fundus Photographs«, in: JAMA 316 (2016), S. 2402-2410; T.Y. Wong, Tien Yin/Bressler, Neil M.: »Artificial Intelligence With Deep Learning Technology Looks Into Diabetic Retinopathy Screening«, in: JAMA Vol. 316, No. 22 (2016), S. 2366-2367.

Ärzt*innen können also ihren Entscheidungsfindungsprozess und ihre Handlungsfähigkeit mit technologischen Mitteln fundieren, fehlerhafte Diagnosen vermeiden und den Patient*innen zum Teil passendere Therapievorschläge anbieten. Entscheidungsunterstützende Algorithmen im medizinischen Bereich können aber auch Spannungsmomente erzeugen, die sich negativ auf die Selbstbestimmung von Ärzt*innen auswirken.

(1) Ein erstes Spannungsmoment entsteht mit dem Zugriff der Algorithmen auf Patient*innendaten. In Übereinstimmung mit der Datenschutz-Grundverordnung müssen die Patient*innen die benötigten personenbezogenen Daten für die Diagnoseleistung des Algorithmus freigeben. Weil für die meisten Patient*innen und Ärzt*innen nicht nachvollziehbar sein dürfte, wie genau welche Datenelemente verarbeitet werden und wie genau der Algorithmus zu seinen Ergebnissen kommt, verlangt die Verwendung dieser Technologie den Ärzt*innen ein Vertrauen ab,[50] das durch den Regulierungskontext algorithmischer Systeme gefördert werden kann.

(2) Zweitens kann auch bei professionellen Diagnosealgorithmen dasselbe Problem wie bei intelligenten Suchalgorithmen auftreten, nämlich dass unterrepräsentierte Patient*innengruppen diskriminiert werden. Weil Diagnosealgorithmen mithilfe großer Datensammlungen trainiert werden, können statistisch seltene Erkrankungen und medizinisch seltener versorgte Patient*innengruppen vergleichsweise schlechter berücksichtigt werden.[51] Dieses Phänomen stellt in erster Linie ein Gerechtigkeitsproblem dar. Weil eine derartige Diskriminierung im schlimmsten Fall aber zu fatalen Fehldiagnosen und falschen Therapieentscheidungen führen kann, ergeben sich mittelbar auch Folgen für die Selbstbestimmung. Gerade weil die technische Datenanalyse für die behandelnden Ärzt*innen intransparent abläuft, können sie anhand des maschinell ermittelten Ergebnisses nicht unmittelbar feststellen, ob ihr Vertrauen in die Technik begründet ist. Sie sind an dieser Stelle auf einen regulativen Rahmen einschließlich einer institutionellen Qualitätskontrolle angewiesen.

(3) Drittens können Diagnosealgorithmen nicht die qualitativen Werte, Einstellungen und Ideale von Patient*innen berücksichtigen. Stattdessen

50 Vgl. Wilbanks, John: »Portable Approaches to Informed Consent and Open Data«, in: Julia Lane, Victoria Stodden, Stefan Bender & Helen Nissenbaum (Hg.), Privacy, Big Data, and the Public Good: Frameworks for Engagement, Cambridge: Cambridge University Press, S. 234-252.

51 Vgl. P. De Laat, Can transparency restore accountability? S. 526.

werden die vorgeschlagenen Therapieoptionen auf Basis der ermittelten Diagnosen und der quantifizierbaren Aspekte der individuellen Krankengeschichte gewichtet.[52] Alle Entscheidungsaspekte, die die Frage nach einem guten und gelingenden Leben berühren, müssen folglich unterstützt durch menschliche Ärzt*innen von den Patient*innen beantwortet werden. Algorithmen können derartige Sinnfragen nicht begreifen.[53]

(4) Eng damit verbunden ist das vierte Spannungsmoment: Welcher Akteur besitzt die moralische Verantwortung, wenn der Algorithmus Fehldiagnosen produziert und die Erfolgsaussichten einzelner Therapieoptionen falsch einschätzt? Kann den Algorithmus selbst ein moralischer Vorwurf treffen, wenn dieser einen Rechenfehler begeht? Sind die Programmierer*innen moralisch für die Folgen verantwortlich, die sich aus dem technischen Fehler ergeben? Oder müssen die behandelnden Ärzt*innen zu jeder Zeit die Verantwortung übernehmen – selbst dann, wenn sie den Analyseprozess faktisch nicht überprüfen können? Die Diskussion um diese Fragen ist in der Medizinethik und der Ethik der Technikfolgenabschätzung in vollem Gange.[54] Ungeachtet dessen lehnen wir mit Blick auf die eingangs geleistete Konzipierung der Selbstbestimmung die Vorstellung moralfähiger Algorithmen (zumindest angesichts des jetzigen Standes der Technik) ab. Moralisch verantwortliche Akteure besitzen Volitionen höherer Ordnung, sie können eigene Intentionen ausbilden, diese kritisch reflektieren und zielgerichtet handeln. Ein Algorithmus kann hingegen keine intersubjektiv nachvollziehbaren Gründe für die Resultate von Rechenoperationen geben, und er besitzt auch keine eigenen Volitionen, sondern klar vorgegebene Optimierungsziele, die er mit einem ebenfalls klar definierten Set an Rechenoperationen erreichen soll.[55] Welche Auswirkungen hat diese Einschätzung auf die Ver-

52 Vgl. Rasche, Christoph: »Digitaler Gesundheitswettbewerb: Strategien, Geschäftsmodelle, Kompetenzanforderungen«, in: Mario A. Pfannstiel, Patrick Da-Cruz & Harald Mehlich (Hg.): Digitale Transformation von Dienstleistungen im Gesundheitswesen I. Impulse für die Versorgung, Wiesbaden: Springer 2017, S. 26.

53 Vgl. Searle, John R.: »Minds, brains, and programs«, in: Behavioral and Brain Sciences Vol. 3, No. 3 (1980), S. 417ff.

54 Einen etwas älteren, aber guten Überblick über die argumentative Landschaft bietet: Kraemer, Fecilitas/van Overveld, Kees/Peterson, Martin: »Is there an ethics of algorithms?«, in: Ethics and Information Technology, Vol. 13, No. 3 (2011), S. 251-260; Mittelstadt, Brent D./Allo, Patrick/Taddeo, Mariarosaria/Wachter, Sandra/Floridi, Luciano: »The ethics of algorithms: Mapping the debate«, in: Big Data & Society, Vol. 3, No.2 (2016), S. 1-21.

55 Siehe hierzu auch den Beitrag von Eric Hilgendorf in diesem Band.

antwortung von Ärzt*innen? Im Rahmen der medizinischen Fachkenntnisse müssen Ärzt*innen, die bei Behandlungen auf die Hilfe eines unterstützenden Diagnosealgorithmus zurückgreifen, die Empfehlungen des Algorithmus kritisch prüfen. Wenn sie Zweifel am Ergebnis hegen, besteht die Verantwortung, auf Basis guter Gründe eigene Empfehlungen auszusprechen. Neben den Ärzt*innen besitzen, je nach Fallkonstellation, Hersteller*innen, Programmierer*innen, staatliche Prüfstellen und Gremien zur Ausgestaltung regulierender Gesetze und Leitlinien eine moralische Verantwortung für die Folgen technischer Fehler.[56]

Aufgrund der Fähigkeit, die qualitativen Wertvorstellungen von Patient*innen zu berücksichtigen, in einem gemeinsamen Prozess Diagnosen zu ermitteln und passende Therapieentscheidungen zu treffen, werden menschliche Ärzt*innen nicht durch die neuen technischen Möglichkeiten überflüssig. Ganz im Gegenteil sind Ärzt*innen in digitalen Behandlungsprozessen zwingend notwendig, um die Diagnoseleistung intelligenter Systeme überprüfen, feinjustieren, weiterentwickeln und die moralische Verantwortung für die Einschätzung und Anwendung errechneter Diagnose- und Behandlungsempfehlungen mittragen zu können.[57] Nicht zuletzt geht es um eine personale Beziehung, in der die Kommunikation eine herausragende Rolle spielt und die für den Therapieerfolg bedeutsam sein kann.

Zusammenfassung und Ausblick

Selbstbestimmte Akteure besitzen die Fähigkeit, ihre eigenen Wünsche, Überzeugungen und Ideale in einem Prozess auszubilden, zu reflektieren und zu verändern, Intentionen zu bilden und diese in passende Handlungen zu überführen. Damit Menschen diesen Prozess meistern können, müssen sie sich gegenseitig als gleichberechtigte und verantwortungsfähige Akteure mit denselben grundlegenden Rechten und Freiheiten anerkennen, ihnen muss ein soziales Milieu offenstehen, in dem sie ihre Überzeugungen kritisch reflektieren können, und sie müssen über Kompetenzen verfügen, mit denen sie kontextuell die ihnen offenstehenden Handlungsalternativen erkennen und einschätzen können.

56 Diese Beurteilung steht im Einklang zum Bericht der Datenethikkommission (Gutachten 2019, Berlin 2019, S. 72 und 119)

57 Vgl. Wang, Fei/Preininger, Anita: »AI in Health: State of the Art, Challenges, and Future Directions«, in: Yearbook of Medical Informatics, Vol. 28, No. 1 (2019), S. 16.

Im digitalen Raum wird die menschliche Selbstbestimmung sowohl mit förderlichen wie auch hinderlichen Elementen konfrontiert: Das gilt auch für den Gesundheitskontext. Digitale medizinische Technologien und Informationsangebote können Ärzt*innen und Patient*innen darin unterstützen, Informationsasymmetrien und -lücken abzubauen, Wissenslücken selbstständig zu schließen und Entscheidungen selbstbestimmter sowie qualitativ abgestützter zu treffen. Auf der anderen Seite können digitale Technologien auch Informationsasymmetrien und -fehler erzeugen, indem sie qualitativ ungenügende, quantitativ zu umfangreiche und/oder für die Patient*innen unverständliche Informationen verbreiten. Sie können den Datenschutz und die Privatsphäre von Patient*innen und Nutzer*innen gefährden, sie können diskriminierend wirken und sie können Ärzt*innen in haftungsrelevante Begründungszwänge bringen.

Damit Nutzer*innen innerhalb des digitalen Raums Gesundheitsfragen selbstbestimmt stellen und beantworten können, müssen sie über ausreichende Digital- und Gesundheitskompetenzen verfügen, mit denen sie die Qualität der ihnen angebotenen medizinischen Informationen und Applikationen beurteilen und diese anwenden können. Diese Kompetenzen können nicht alle Menschen aus sich selbst heraus entwickeln. Aus diesem Grund sind sie darauf angewiesen, dass staatliche, zivilgesellschaftliche und privatwirtschaftliche Akteure das Selbstbestimmungsrecht ihrer Mitbürger*innen anerkennen, deren Digital- und Gesundheitskompetenzen fördern und die Entscheidungsstrukturen für Nutzer*innen in diesen Kontexten so transparent und sicher wie möglich gestalten. Neben den genannten Fallbeispielen sind noch viele weitere, konkrete, digitale Technologien und Anwendungen im Gesundheitsbereich zu analysieren, beispielsweise die Videosprechstunde, Gesundheits-Apps auf Rezept, Roboter in der Altenpflege, die Verpflanzung künstlicher Organe und Körperteile, der Umgang mit sogenannten Wearables, die Integration gesundheitsbezogener Applikationen in eine Smart-Home-Infrastruktur, die Einrichtung von Datenforschungszentren und vieles mehr. Sie alle haben Auswirkungen auf die Selbstbestimmung von Bürger*innen. Die Diskussion darum wird uns alle beständig begleiten und herausfordern.

2.1.3 Autonomie

Digitale Berechenbarkeit versus Zufall in Literatur und Recht

Timo Rademacher und Erik Schilling

Mittels digitaler Methoden werden Menschen berechnet, ihre Vorlieben und ihr Verhalten ermittelt, und das immer präziser. Das hat eine ganze Reihe manifester Vorteile: Das Erheben von Präferenzen führt zu einer besseren Zuordnung und Nutzung von Ressourcen. Das Erfassen von Gesundheitsdaten ermöglicht bessere Therapien. Das Erfragen von Persönlichkeitstypen bietet die Chance, Verträge individuell zuzuschneiden. Doch die Optimierungen, die sich mittlerweile quer durch unsere Gesellschaft und unsere Rechtsordnung ziehen, haben ihren Preis: Individuell angepasste Gestaltungsmöglichkeiten oder komfortablere Dienste (positive Freiheit) werden gegen ein Mehr an staatlicher und/oder privater Überwachung und Datenverarbeitung (negative Freiheit) eingetauscht.[1] Viele Bürger*innen tun das ganz bewusst, etwa indem sie bereitwillig ihre personenbezogenen Daten in den sozialen Medien preisgeben. Ob und wo diese Tauschgeschäfte auf einer *über*individuellen Ebene, also hinsichtlich des hier im Vordergrund stehenden Gemeinwohls,[2] noch als gemeinwohlfördernd oder schon als gemeinwohlschädlich zu gelten haben, ist eine Frage, die die Gesellschaft gegenwärtig beantworten muss.

1 Zu diesem sogenannten Technologieparadox siehe den einleitenden Beitrag von Chris Piallat in diesem Band. Richtig ist, dass die Dichotomie von positiver und negativer Freiheit kaum noch in der Lage ist, die komplexen Wechselwirkungen von Freiheit und Technik differenziert abzubilden. Siehe daher für eine komplexere Taxonomie von Freiheit und Technik Wagner, Ben: »Was bedeutet ›Freiheit‹ in einem soziologischen Kontext?«, in: Michael Oswald/Isabelle Borucki (Hg.), Demokratietheorie im Zeitalter der Frühdigitalisierung, Wiesbaden: Springer 2020, S. 201-218.

2 Zum Begriff und Verständnis des Gemeinwohls siehe den einleitenden Beitrag von Chris Piallat in diesem Band.

Klar aber ist schon jetzt: Digitalisierung bedeutet Freiheitsgewinne und Freiheitsverluste zugleich.

Entsprechend intensiv wird die Digitalisierung in den Geistes- und Sozialwissenschaften untersucht. Die voneinander weit entfernt liegenden Pole dieser Diskussion werden in der Einleitung zu diesem Buch umrissen: Sie reichen von Technik- und Interneteuphorie aus den Anfangstagen der Digitalisierung bis hin zu dystopisch anmutenden Warnungen vor der Superintelligenz und den Gefahren des Internets. An einige besonders wirkmächtige Stellungnahmen sei kurz erinnert: So fragt Armin Nassehi in seinem Buch *Muster* (2019) nach den Fundamenten, auf denen die Digitalisierung der Gegenwart ruht, und beleuchtet in einer problemgeschichtlichen Analyse ihr Entstehen im Laufe des 20. Jahrhunderts.[3] Andreas Reckwitz setzt sich in seinem vieldiskutierten Buch über *Die Gesellschaft der Singularitäten* (2017) mit dem Zusammenhang von Digitalisierung und einer auf die Spitze getriebenen Selbstkuratierung auseinander.[4] Shoshana Zuboff diagnostiziert in ihrem nicht weniger breit wahrgenommenen Buch *The Age of Surveillance Capitalism* (2019) eine Verschiebung der zentralen Bedrohung: weg vom totalitären Big-Brother-Staat hin zum privaten Überwachungs-Kapital aus dem Silicon Valley.[5]

Wir möchten zu diesen Diskussionen drei Thesen beisteuern:

(1) Digitalisierung bedingt eine zunehmende Berechnung menschlichen Handelns, was – je nach Kontext – als Freiheitsgewinn und/oder Freiheitsverlust spürbar werden kann, also ambivalent ist. Die Literatur hat in Zukunftsromanen die Möglichkeit, die Folgen unserer digitalen Berechenbarkeit zu Ende zu denken.
(2) Dem Recht kommt in unserer Gesellschaft die Aufgabe zu, Freiheitsgrenzen verbindlich abzustecken. Es kann sich an den fiktionalen Szenarien der Literatur orientieren, um frühzeitig Überlegungen zu Freiheitsgewinnen und -verlusten durch Digitalisierung anzustellen, die dann in die Ausgestaltung rechtlicher Regelungen einfließen können.
(3) Inspiriert von den fiktionalen Welten der Literatur glauben wir, dass es ein wichtiges Element künftiger Freiheit sein könnte, den Zufall im Leben

3 Nassehi, Armin: Muster. Theorie der digitalen Gesellschaft, München: C.H. Beck 2019.
4 Reckwitz, Andreas: Die Gesellschaft der Singularitäten. Zum Strukturwandel der Moderne, Berlin: Suhrkamp 2017.
5 Zuboff, Shoshana: The Age of Surveillance Capitalism, New York: PublicAffairs 2019.

der Menschen zu bewahren, und das heißt vielleicht sogar: dem Zufall *von Rechts wegen* einen Platz in unserem Leben einzuräumen.

Wir entwickeln unsere Thesen vor allem anhand des Romans *Der Würfel* von Bijan Moini (Abschnitt 1). In dem Roman hat die Gesellschaft die Kontrolle an eine allgegenwärtige künstliche Intelligenz übergeben und dadurch eine optimierte Realität geschaffen, die allerdings, und das ist das für uns Spannende, bei Moinis Helden *Taso* eine auf den ersten Blick befremdliche Sehnsucht nach dem Zufall weckt. Aus dieser Roman-Welt greifen wir einen speziellen Aspekt zur rechtlichen Analyse (Abschnitt 2) heraus: Wir fragen, ob es gut wäre, wenn auch der Vollzug des Rechts optimiert wäre, das Recht also stets und überall herrschen würde, ungestört von den Zufällen individuell-normabweichenden Verhaltens. Vor diesem Hintergrund werfen wir die Frage auf (Abschnitt 3), ob diese Vision dystopische Züge hat, weshalb dem sich abzeichnenden digitalisierten Vollvollzug des Rechts ein *Recht zum Rechtsverstoß* entgegenzustellen wäre. Im Fazit (Abschnitt 4) plädieren wir für ein Menschenbild, das den Verzicht auf Berechnung in bestimmten Bereichen in Kauf nimmt, obwohl sie – etwa technisch – möglich wäre.[6]

1 Der berechnete Mensch in der Literatur

Literarische Texte der vergangenen Jahrzehnte, die sich mit Fragen der Digitalisierung beschäftigen, unterstreichen die Tendenz zu zunehmender Berechenbarkeit. International stark beachtet wurde Ian McEwans Roman *Machines Like Me* (2019),[7] in dem die Frage nach digitaler Rationalität am Beispiel eines humanoiden Roboters und dessen Interaktion mit Menschen durchgespielt wird. Im deutschsprachigen Kontext setzt sich die Juristin und Schriftstellerin Juli Zeh intensiv mit Digitalisierung und Berechenbarkeit auseinander. Schon ihr früher Roman *Spieltrieb* (2004)[8] lässt sich als Überlegung dazu verstehen, wie viel Berechenbarkeit das Alltagshandeln wünschenswer-

6 Teile unserer Thesen konnten wir mit den Studierenden einer digitalen Studienstiftungs-Arbeitsgruppe im Herbst 2020 diskutieren. Wir danken allen Beteiligten für die Gespräche und ihre Anregungen.

7 McEwan, Ian: Machines Like Me, London: Jonathan Cape 2019.

8 Zeh, Juli: Spieltrieb, München: btb 2006.

terweise prägen sollte. Verstärkt wird dies in *Corpus Delicti* (2009)[9]: Im Roman wird eine zukünftige Gesellschaft geschildert, die in Gesundheitsfragen optimiert ist und auch klare normative Vorgaben aufweist, wie sich die Individuen verhalten sollen. In ihrer essayistischen Publikation *Fragen zu Corpus Delicti* (2020)[10] bezieht Juli Zeh diese Überlegungen unter anderem auf die Debatten rund um die Corona-Pandemie, insbesondere auf Bestrebungen nach digitaler Überwachung, etwa um Infektionsketten nachzuverfolgen.

Besonders relevant für die Frage nach Chancen und Risiken digitaler Berechenbarkeit ist Bijan Moinis Roman *Der Würfel* (2018).[11] Moini entwirft eine Zukunftsgesellschaft, die größere individuelle Freiheiten genießt als die in Zehs *Corpus Delicti*, weil kaum inhaltliche Verhaltensvorgaben gemacht werden. Gleichzeitig aber ist die digitale Überwachung erheblich weiter ausgebaut, etwa zum Zwecke der optimalen Befriedigung von Bedürfnissen und Verteilung von Ressourcen, wie auch zur Durchsetzung des Rechts. Ein Gegenmodell zu dieser fortschreitenden Digitalisierung entwirft Alexander Sperling in seinem Roman *Glashauseffekt* (2020).[12] Der Roman spielt im Jahr 2049; die zunehmende Umweltzerstörung hat dazu geführt, dass die Menschen auch im Hinblick auf die Digitalisierung auf einem – verglichen mit 2020 – niedrigeren Niveau angekommen sind.

Zu all diesen Romanen würde sich eine detaillierte Analyse lohnen. Wir beschränken uns hier jedoch auf Moinis *Der Würfel*, weil sich daran das in diesem Band im Vordergrund stehende Phänomen – Digitalisierung im Kontext von Freiheit und Autonomie – *in nuce* beobachten lässt.

Der Würfel spielt zu einem nicht genauer definierten Zeitpunkt in der Zukunft (Anfang/Mitte der 2030er Jahre). Das Leben in Deutschland wird in großen Teilen von einem intelligenten Algorithmus gesteuert, dem ›Würfel‹. Dieser ist demokratisch legitimiert, agiert also im Rahmen der Gesetze, die der Bundestag ihm beziehungsweise der Gesellschaft geben. Seine wesentliche Aufgabe besteht in umfassender Optimierung: Auf Basis der gesetzlich vorgegebenen Rahmenbedingungen sowie der ihm bekannten Vorlieben und Persönlichkeitseigenschaften der Bürger*innen kann der Algorithmus Ressourcen bestmöglich zuteilen und nutzen. Er ermöglicht es den einzelnen In-

9 Zeh, Juli: Corpus Delicti – Ein Prozess, München: btb 2010.

10 Zeh, Juli: Fragen zu Corpus Delicti, München: btb 2020.

11 Moini, Bijan: Der Würfel. Roman, Zürich: Atrium 2018.

12 Sperling, Alexander: Glashauseffekt. Ein Zukunftsroman, München: &Töchter 2020.

dividuen beispielsweise, Beruf oder Partner*in genau nach ihren Wünschen zu wählen.

Die Berechenbarkeit der Bürger*innen wird in einem sogenannten ›Pred-Score‹ abgebildet: Je höher der Score, umso stärker die Berechenbarkeit des Individuums und umso größer die Annehmlichkeiten, die der Würfel den Bürger*innen zukommen lässt. Auf Basis seiner Berechnungen gelingt es dem Würfel auch, Verbrechen so präzise vorherzusagen, dass die Kriminalität auf einem historischen Tiefstand angelangt ist. Hier scheinen Parallelen zu Steven Spielbergs Film *Minority Report* (2002) auf. Rechtsstreitigkeiten werden (innerhalb gewisser Grenzen) anhand von Informationen, die dem Würfel vorliegen, automatisiert und ad hoc entschieden – und zum Beispiel durch Drohnen auch automatisiert gelöst, das heißt vollstreckt.

Neben dem Würfel existieren mehrere Varianten der Organisation von Gesellschaft. In China herrscht der ›Harmonismus‹. Anders als der Würfel gibt dieser inhaltliche Präferenzen für das Verhalten vor. Der westliche ›Kubismus‹ dagegen zielt ausschließlich auf Berechenbarkeit und die damit verbundene Optimierung (zumindest noch) demokratisch bestimmter Vorgaben und Werte. Darüber hinaus gibt es in Deutschland bestimmte – gesetzlich garantierte – »Würfelfreie Zonen« (WfZ), die nicht vom Würfel überwacht und gesteuert werden. Dort leben diejenigen, die den Würfel aus freiheitlichen oder ideologischen Gründen ablehnen, etwa weil sie von der Autonomie des Individuums überzeugt sind oder einer Religion anhängen und den Würfel nicht als ›Gott‹ neben ihrem Gott tolerieren. Allerdings geraten die Würfelfreien Zonen immer stärker unter Druck, sich gegenüber den Kubisten für ihr abweichendes Verhalten zu rechtfertigen.

Der Protagonist des Romans, Taso, steht für eine weitere Variante. Als ›Gaukler‹ versucht er, sich dem Zugriff des Würfels durch möglichst willkürliches Verhalten zu entziehen. Sein Pred-Score liegt – mit einer dezenten Anspielung auf George Orwells berühmte Dystopie – bei 19,84 auf einer Skala von 1 bis 100 und gehört damit zu den niedrigsten überhaupt. Nahezu alle Alltagsentscheidungen nimmt Taso auf Basis eines Würfel- oder Münzwurfs vor: Er zieht morgens die Kleidung an, die ihm ein Würfel zufällig zuteilt (ein realer Würfel, nicht der Würfel-Algorithmus), und beantwortet Ja-/Nein-Fragen abhängig davon, ob ihm eine Münze Kopf oder Zahl zeigt. Im Roman wird so mit dem doppelt codierten Bild des Würfels eine Konstellation entworfen, in der maximales Kalkül (der Würfel als Algorithmus) und maximale Kontingenz (der Würfel als Zufallsinstrument) einander gegenüberstehen.

Moinis *Der Würfel* ist für die Auseinandersetzung mit dem Thema *digitale Berechenbarkeit* ein hochinteressantes und hochreflektiertes literarisches Beispiel, das sich besser als klassische Dys- oder Utopien dazu eignet, von gesellschaftswissenschaftlichen Disziplinen befragt zu werden. Der Würfel-Algorithmus ist demokratisch legitimiert und unterscheidet sich damit klar von autoritär fundierten Weltentwürfen, etwa der Religion oder der staatlichen Ideologie Chinas – ein Verweis des Romans auf das reale Experiment des ›Social Credit Systems‹ in einigen chinesischen Städten. Der Würfel stellt also gerade nicht das typische Schreckensszenario aus Überwachung und heteronomer Lenkung dar, das Dystopien oft zeichnen, etwa Juli Zehs ›Gesundheitsdiktatur‹ in *Corpus Delicti*. Im Gegenteil: Indem der Würfel den Menschen dabei hilft, ihr Leben an ihren Vorlieben auszurichten, verschafft er ihnen Freiheiten und ein nicht unerhebliches Glück: »Was spricht dagegen, dass jeder das arbeitet, was er am besten kann, sagt, was ihm nützt, und sich in jemanden verliebt, der zu ihm passt?«, wird Taso vom Würfel selbst gefragt.[13] Der Würfel sorgt für »Sicherheit und eine integre, effiziente Politik« und hilft, »Ressourcen zu schonen, zu forschen, […] persönliches Potential auszuschöpfen, passende Freunde und Partner zu finden und gesund alt zu werden«.[14]

Tasos Argumente dagegen erscheinen schwach: Er pocht auf Selbstbestimmung, entscheidet sich aber stets nach dem Zufallsprinzip. Zum Würfel sagt er: »Zufall macht frei. Diese Münze ist unabhängiger als wir beide zusammen.«[15] Doch ist das ein stark reduzierter Freiheitsbegriff. Er basiert ausschließlich auf der Freiheit *von* heteronomer Bestimmung (negative Freiheit), nicht hingegen auf autonomer Entscheidungsfreiheit *für* etwas (positive Freiheit).[16] Entsprechend sagt die Richterin, für die Taso arbeitet und die sich später als Widerstandskämpferin entpuppt, zu ihm:

> »Ich wusste bei Ihnen doch nie, woran ich war. Sie wirkten immer so […] unentschlossen. Ein Extremgaukler, ja, aber doch im System. Auf eine gewisse Art waren Sie angepasster als jeder andere Offliner, den ich kenne, komplett auf den Würfel eingestellt.«[17]

13 B. Moini: Der Würfel (Fn. 11), S. 159.

14 Ebd. S. 172.

15 Ebd. S. 181.

16 Zu den Freiheitsbegriffen s. oben, in und bei Fußnote 1.

17 B. Moini: Der Würfel (Fn. 11), S. 333f.

Was also zeichnet Tasos Einstellung aus, bevor er sich entschieden gegen den Würfel stellt und aktiven Widerstand versucht? Was macht den Zufall als Mittel für ihn attraktiv? Drei Formen von Zufälligkeit lassen sich resümieren, die der Roman am Beispiel seines Protagonisten verdeutlicht und die hier abstrahierend angeführt werden sollen:

(1) Zufall: In vielen Szenen des Romans sorgt der objektive Zufall des Münz- oder Würfelwurfs dafür, dass Taso Dinge tut, die er ansonsten nicht täte. Im Roman bezieht sich das primär auf Alltagsfragen, etwa darauf, etwas zu essen, was Taso nicht kennt, oder Kleidung zu tragen, die nach gängigen ästhetischen Kriterien nicht zusammenpasst. Doch man kann den Gedanken auf größere Zusammenhänge übertragen und etwa die Frage stellen, ob nicht der (objektive oder zumindest subjektiv empfundene) Zufall[18] fundamental für das Entdecken oder Erleben von Neuem ist. Dieses Konzept besitzt einen fließenden Übergang zum Begriff der Serendipität.
(2) Serendipität: Mit dem Begriff ›Serendipität‹ wird die zufällige Beobachtung von etwas ursprünglich nicht Gesuchtem bezeichnet, das sich als neue und überraschende Entdeckung und Lernerfahrung erweist.[19] Im Kontext des Romans lässt sich dies beispielsweise auf Tasos Beziehung mit Dalia beziehen, die er ›zufällig‹ vor seiner Haustür trifft. Rein algorithmisch hätten die beiden nie zusammengefunden. Dennoch lernen sie gerade aufgrund ihrer Unterschiedlichkeit voneinander – beispielsweise, den eigenen Standpunkt deutlicher zu fassen. Die Serendipität der unerwarteten Begegnung führt also zu einer Weiterentwicklung der beiden Figuren, die es ohne die unberechnete Begegnung in dieser Form nicht gegeben hätte.
(3) Kontingenz: Mit dem Begriff ›Kontingenz‹ bezeichnen wir im Anschluss an Niklas Luhmann etwas, das weder notwendig noch unmöglich ist. Es kann also sein, wie es ist, wäre aber gleichzeitig auch anders möglich.[20]

---

18 Dazu Vogt, Peter: Kontingenz und Zufall. Eine Ideen- und Begriffsgeschichte, Berlin: Akademie 2011.

19 So, in unserer Übersetzung, Reviglio, Urbano: »Serendipity as an Emerging Design Principle of the Infosphere: Challenges and Opportunites«, in: Ethics and Information Technology 21 (2019), S. 151-166, hier S. 152.

20 Luhmann, Niklas: Soziale Systeme, Berlin: Suhrkamp 2018, S. 47, 148ff. Ausführlich dazu Holzinger, Markus: Kontingenz in der Gegenwartsgesellschaft, Bielefeld: transcript 2007; zum Konzept und notwendigen Abgrenzungen zudem Ermakoff, Ivan: »The Structure of Contingency«, in: American Journal of Sociology 121 (2015), S. 64-125.

> Algorithmen wie der Würfel verhindern ein Denken in Kontingenz. Denn in der Welt, die der Würfel organisiert, könnte nichts auch anders sein; stattdessen ist alles genau so, wie es sein soll, weil es entsprechend berechnet wurde. Das Eliminieren eines Bewusstseins von Kontingenz erschwert darüber hinaus ein Denken in fiktionalen Welten, in denen variierende Strukturen oder Szenarien erprobt werden können – darauf macht Juli Zeh in ihrem Roman *Spieltrieb* aufmerksam.[21]

Bijan Moinis *Der Würfel* dient damit als fiktionales Experiment, mit dem danach gefragt wird, welche Freiheitsgewinne und -verluste mit zunehmender digitaler Berechenbarkeit einhergehen. Der Roman ist für die Debatte deswegen so wichtig und weiterführend, weil in ihm weder ein rein utopisches noch ein rein dystopisches Szenario gestaltet wird. Stattdessen werden – am Beispiel des Protagonisten sowie anderer Figuren – die Vor- und Nachteile digitaler Berechenbarkeit sehr sorgfältig abgewogen. Indem dabei die Vorteile des Zufalls stark gemacht werden, bietet er ein Plädoyer dafür, auch in Kontexten hoher Berechenbarkeit für das Ungeplante offenzubleiben. Mit Denkfiguren wie Serendipität oder Kontingenz – verbunden mit dem ›Möglichkeitssinn‹ der Fiktion – lässt sich dies auf eine theoretische Ebene heben.

Dem folgend gehen wir nun der Frage nach, welche Implikationen diese aufgewertete Rolle des Zufalls in nicht-fiktionalen Kontexten haben könnte. Exemplarisch betrachten wir dazu die Durchsetzung von Recht.

2 Rechtsgehorsam, automatisierte Rechtskontrolle, digitaler Rechtsvollzug und Freiheit zu Devianz

Die Digitalisierung verspricht eine immer bessere, in Teilbereichen sogar vollständige Rechtsdurchsetzung.[22] Das ist nicht nur positiv, sondern – schon

---

Für Oliver Marchart ist Kontingenz ein »Schlüsselbegriff gegenwärtiger sozialwissenschaftlicher Theoriebildung« (»Kontingenz«, in: Dagmar Comtesse [u.a.] (Hg.), Radikale Demokratietheorie. Ein Handbuch, Berlin: Suhrkamp 2019, S. 572-576, hier S. 572).

21 Mit Markus Gabriel lässt sich von unterschiedlichen ›Sinnfeldern‹ sprechen, in denen jeweils – zu Teilen kontingente – Perspektiven auf ›Welt‹ zum Zuge kommen und damit ggf. konkurrieren. Vgl. Gabriel, Markus: Warum es die Welt nicht gibt, Berlin: Ullstein 2013, S. 87-95.

22 Diskursprägend Ferguson, Andrew Guthrie: The Rise of Big Data Policing, New York: New York University Press 2017. Mit einem umfassenden Überblick über die englisch-

ganz intuitiv – auch ein Beispiel für die Gleichzeitigkeit von Freiheitsgewinnen und -verlusten: Einerseits nämlich dürfte die Herstellung rechtmäßiger Zustände von der Mehrheit der Menschen grundsätzlich als wünschenswertes Gemeinwohl-Ziel anerkannt werden. Andererseits ist anzunehmen, dass das Versprechen eines Voll*vollzugs* des Rechts mittels Technologie, also der flächendeckend-zwangsweisen Herstellung rechtmäßiger Zustände, ebenfalls bei einer Mehrheit auf Skepsis oder gar Ablehnung stößt. Dies illustrieren auch die literarischen Texte. Hier scheint ein Zielkonflikt zwischen negativer und positiver Freiheit beziehungsweise Schutz und Autonomie auf, den wir im Folgenden kurz umreißen möchten.

Der Ausgangspunkt unserer Überlegungen ist von einem Vollvollzug des Rechts, wie er von Moini beschrieben wird, denkbar weit entfernt: Unsere freiheitliche Gesellschaft zeichnet aus, dass die Rechtsordnung zu ihrer Durchsetzung nicht auf flächendeckenden physisch-strukturellen Zwang oder flächendeckende Sanktion beruht. Vielmehr soll der Rechtsvollzug aus einer freiwilligen, wenn auch nicht gänzlich unbeeinflussten Entscheidung der vom Recht Betroffenen (Normadressat*innen) heraus geschehen. Die Pandemie des Jahres 2020 hat das eindrucksvoll bestätigt. Der Regelbruch war vielleicht nicht die Regel, aber auch nicht selten. Dies erlaubte es China, das mit digitaler Überwachung und scharfen Sanktionsdrohungen die Pandemie schon im Winter 2020/21 zeitweise unter Kontrolle zu haben schien, sich als ›Sieger im Systemwettbewerb‹ darzustellen.

Die Freiwilligkeit der Normbeachtung lässt sich aber durchaus positiv deuten: soziologisch als brauchbare Illegalität,[23] juristisch als Nachholung von im Normtext versäumter Kontextualisierung im Sinne des sogenannten Verhältnismäßigkeitsgrundsatzes,[24] staatstheoretisch und radikaldemokra-

---

sprachige Literatur Marks, Amber/Bowling, Benjamin/Keenan, Colman: »Automatic Justice? Technology, Crime, and Social Control«, in: Roger Brownsword/Eloise Scotford/Karen Yeung (Hg.), The Oxford Handbook of Law, Regulation, and Technology, Oxford: Oxford University Press 2017, S. 705-730, bes. S. 707-710, 714f.

23 Vgl. Luhmann, Niklas: Funktionen und Folgen formaler Organisation, Berlin: Duncker & Humblot 1999, S. 304-314.

24 Man kann in solchen Konstellationen davon sprechen, dass das Recht, bezogen und gemessen an seinem legitimen Ziel, eine Art von Overblocking betreibt bzw. vorschreibt. Vgl. dazu Rademacher, Timo: »Wenn neue Technologien altes Recht durchsetzen: Dürfen wir es unmöglich machen, rechtswidrig zu handeln?«, in: Juristenzeitung 74 (2019), S. 702-710, hier S. 707ff.; Becker, Maximilian: »Von der Freiheit, rechtswidrig handeln zu können«, in: Zeitschrift für Urheber- und Medienrecht 2019, S. 636-648, hier S. 637

tisch als ziviler Ungehorsam[25] oder – freilich eng verwandt[26] – philosophisch als Ausdruck menschlicher Vernunft.[27] Der kleinste gemeinsame Nenner dieser Ansätze ist, dass sie alle einen im weiten Sinne dialogischen Umgang mit dem Recht beschreiben und diesen positiv bewerten. Die Umsetzung des Rechts wird als Aushandlungsprozess mit den Umständen des Einzelfalls, der Gesellschaft und letztlich sogar mit sich selbst verstanden.[28] Das realisierte Recht soll damit sicher nicht zufällig sein, aber – in diesem positiven Verständnis – doch als kontingent in dem Sinne erkannt werden, dass aus der kritischen Konfrontation von Recht, Realität und Rechtsunterworfenem Rückschlüsse auf eine alternative Ausgestaltung des Rechts folgen – und damit seine potenzielle Weiterentwicklung.

Dogmatisch und positivistisch denkende Jurist*innen haben mit diesen Ansätzen allerdings ihre Probleme. Denn wenn Normen in demokratischen Verfahren geschaffen werden, ist dadurch auch die Freiheit der oder des Einzelnen gewährleistet.[29] Das gilt jedenfalls dann, wenn die demokratische Mehrheit nicht allein durch freie Wahlen zustande kommt, sondern sich die parlamentarisch-demokratische Mehrheit auch an Grundrechte und sonstiges Verfassungsrecht halten muss. Wenn das Recht derart verfahrensmäßig legitimiert ist, ist die Überlegung, der oder die Einzelne könne ein Recht darauf haben, dem Recht die Gefolgschaft zu verweigern, rechtsdogmatisch schwer erträglich.[30] Ein Recht auf Devianz oder genauer: ein Recht darauf, rechtswidrig handeln zu können, passt schlecht in unser rechtliches Denken. Stattdessen sind die Dialog- und Diskursräume zur Kritik und Veränderung des Rechts selbst rechtlich verfasst, nämlich in Form von Wahlen, gerichtlichen (Verfassungs-)Beschwerden oder Bürger begehren und -entscheiden.

---

bezeichnet die urheberrechtlichen Upload-Filter auch als Folge von »unpassendem Recht« (gemeint ist das Urheberrecht).

25 Siehe v.a. Habermas, Jürgen: »Recht und Gewalt – ein deutsches Trauma«, in: Merkur 38 (1984), S. 15-28, hier S. 16. Aus der juristischen Literatur M. Becker: Von der Freiheit, rechtswidrig handeln zu können (Fn. 24), S. 636.

26 Vgl. J. Habermas: Recht und Gewalt (Fn. 25), S. 23.

27 Vgl. Rostalski, Frauke: »Brave New World«, in: Goltdammer's Archiv 166 (2019), S. 481-488, hier S. 483 m. w. N.

28 Vgl. auch Poscher, Ralf: »Verwaltungsakt und Verwaltungsrecht in der Vollstreckung«, Verwaltungsarchiv 89 (1998), S. 111-136, hier S. 113: »Kampf um Rechtsbehauptungen kommunikativ absorbiert«, mit Verweis auf Luhmann.

29 Zu Freiheit als Verfahren bzw. durch Verfahren im Zusammenhang mit digitalen Technologien siehe B. Wagner: Was bedeutet »Freiheit«? (Fn. 1), S. 206 m. w. N.

30 Dreier, Ralf: Recht – Staat – Vernunft, Frankfurt a. M.: Suhrkamp 1991, S. 41.

Nur »[w]o Gerichte fehlen oder ihre Sprüche nicht vollziehbar sind, ist faktischer Widerstand als Ungehorsam die Rückzugsbastion der Freiheit«.[31] Ein ›Dialog‹ *contra legem* ist damit Unrecht.

Zwar ist ein solches Urteil zeitgebunden, nämlich an die wohlwollende Beobachtung des real existierenden deutschen demokratischen Grundrechtsstaats. Auch die angelegten Maßstäbe für dieses Urteil sind zeitgebunden und damit eben nicht zwangsläufig universell ›richtig‹. Jürgen Habermas illustriert diesen Punkt in einem Aufsatz von 1984 eindrücklich mit dem Verweis auf Kant und dessen Einschätzung, es sei richtig, Frauen und Tagelöhner vom Wahlrecht auszuschließen.[32] Aus der bundesrepublikanischen Geschichte gibt einem das Urteil des Bundesverfassungsgerichts zur Strafbarkeit homosexueller Handlungen nicht weniger zu denken: Das Gericht hielt die Strafbarkeit für verfassungskonform.[33]

Habermas leitet aus seiner Beobachtung ein Plädoyer für eine Anerkennung des zivilen Ungehorsams »als Bestandteil der politischen Kultur eines entwickelten demokratischen Gemeinwesens« ab. Der demokratische Staat müsse das Sanktionieren eines Regelbrechers unter Umständen mit »Zurückhaltung« üben. Die Gründe des Ungehorsams müssten dafür, dass der Delinquent diese Zurückhaltung verdient, »aus anerkannten verfassungslegitimierenden [sic!] Grundsätzen begründe[t]« werden können; der Delinquent sei dann ein »potentieller Hüter [der staatlichen] Legitimität«.[34] Doch dieser Ansatz gibt zu denken, wenn man berücksichtigt, dass auch die Querdenker-Bewegung von 2020/21 ihren ätzenden Ungehorsam gegen Versammlungsauflagen ganz unproblematisch verfassungsrechtlich verankern und damit als zivilen Ungehorsam verklären konnte – methodisch (!) nicht viel anders als die Friedensbewegung von 1983, auf die sich Habermas mit seinen Thesen bezogen hat.[35]

---

31 So Waechter, Kay: Sicherheit und Freiheit in der Rechtsphilosophie, Tübingen: Mohr Siebeck 2016, S. 30.

32 J. Habermas: Recht und Gewalt (Fn. 25), S. 24.

33 BVerfG Urteil v. 10.5.1957 – 1 BvR 550/52, E 6, S. 389 – Homosexuelle.

34 J. Habermas: Recht und Gewalt (Fn. 25), S. 25f.

35 Interessant ist, dass Habermas als verfassungsrechtliche Verankerung des damaligen zivilen Ungehorsams – es ging um den Kampf gegen die Umsetzung des NATO-Doppelbeschlusses – meint, nicht auf den in Art. 2 Abs. 2 GG verankerten Lebensschutz zurückgreifen zu können (da sich auch die Gegenseite hierauf berufen könne), sondern vor allem auf die Nicht-Reversibilität eines Atomkrieges und die damit verbundene

Aber unabhängig davon, wie man sich nun zu dem normativen Konzept von Habermas positionieren will, galt eines bislang mit Gewissheit: Zumindest eine *faktische* Freiheit zur Devianz gab es immer. Denn eine Rechtsnorm kennzeichnet ein bestimmtes Verhalten zunächst lediglich als wünschenswert, verbleibt also auf einer abstrakten, rein kommunikativen Ebene, ohne selbst etwas zur Realisierung dieses Wunsches beitragen zu können.[36] Der demgegenüber zurückhaltende Einsatz von staatlichem Zwang oder staatlicher Sanktion zur Durchsetzung staatlicher Ziele hat – in vordigitalen Zeiten – nicht nur etwas mit dem Menschenbild vernunftbegabter und deshalb regeltreuer Bürger*innen zu tun. Vielmehr ist die Zurückhaltung eine Frage fehlender Ressourcen (gewesen).[37] Unabhängig davon, ob es wünschenswert wäre, an jede Ecke einen Polizisten oder eine Polizistin zu stellen – es ist schlicht nicht möglich (gewesen).

Rechtsdurchsetzung hat(te) daher etwas subjektiv Zufälliges oder (untechnisch gesprochen) Stichprobenhaftes. Sie hängt beispielsweise vom Rechtsverfolgungswillen etwaiger Geschädigter ab oder davon, ob ein Regelbruch überhaupt bemerkt wurde. Daher wurde in der Vergangenheit eher Klage über Vollzugsdefizite geführt.[38] Bereits gegen Ende des 20. Jahrhunderts suchte man nach Möglichkeiten, Rechtsbefolgung jenseits von Norm und Befehl durch psychologisch informierten Mitteleinsatz, das sogenannte Nudging, zu verbessern. Es war beziehungsweise ist der Versuch, sich eine (vielleicht) vorhandene, mit Mitteln der Psychologie entdeckbare und unbewusste Berechenbarkeit des Menschen zunutze zu machen. Befriedigend im

---

Unzulänglichkeit der (einfachen) Mehrheitsregel für entsprechende Entscheidungen. Vgl. J. Habermas: Recht und Gewalt (Fn. 25), S. 27.

36 Wir folgen hier dem von Möllers, Christoph: Die Möglichkeit der Normen, Berlin: Suhrkamp 2018, S. 125ff., etablierten Normbegriff.

37 Vgl. R. Poscher: Verwaltungsakt und Verwaltungsrecht (Fn. 28), S. 117, formuliert unter Rückgriff auf Luhmann: »Alle Macht auszuüben, würde den Machthaber überanstrengen. Moderne Gesellschaften müssen sich [deshalb] so organisieren, daß die Machtmittel und Sanktionen, die ihren Machthabern zur Verfügung stehen, nur in verschwindend wenigen Fällen eingesetzt werden.«

38 Diskursprägend Lübbe-Wolff, Gertrude: Modernisierung des Umweltordnungsrechts, Bonn: Economica 1996, sowie die Beiträge in Renate Mayntz (Hg.), Implementation politischer Programme, Wiesbaden: VS Verlag für Sozialwissenschaften Bd. I, 1980, Bd. II, 1983.

Sinne von effektiv sind die Ergebnisse nur bedingt.[39] Es überrascht daher nicht, dass das Recht weiterhin zu einem nicht kleinen Teil aus Arrangements besteht, die mit der Unberechenbarkeit des Menschen (genauer: der Unberechenbarkeit des menschlichen Rechtsgehorsams) rechnen und deshalb Haftung und Sanktion für Regelbrüche vorsehen.

In der Gegenwart ändert sich dies jedoch. Moinis *Würfel* führt uns eine Welt vor, die – in Ansätzen – schon die unsere ist. Es gibt immer mehr ›intelligente‹ (Infra-)Strukturen, die Rechtsgehorsam nicht *ex post* sanktionieren, sondern *ex ante* psychisch oder physisch erzwingen. Wir unterscheiden hier *intelligent surveillance* einerseits und *impossibility structures* andererseits. Prototypisch für *intelligent surveillance* steht die sogenannte intelligente Videoüberwachung. Hierbei filmt die Kamera nicht mehr einfach nur ›dumm‹ alles, was in ihrem Erfassungsbereich geschieht. Sie soll dank KI-getriebener Technologie zur Bilderkennung und -auswertung vielmehr in der Lage sein, verbotenes oder gefährliches Verhalten zu erkennen und Alarm zu schlagen (sogenanntes *predictive policing*[40]). Idealerweise würden Delikte auf diese Weise sogar verhindert, jedenfalls aber wäre damit flächendeckende Sanktionierung und Haftbarmachung von Regelbrechenden möglich.

Während *intelligent surveillance* immerhin die Freiheit lässt, die vollstreckungs- beziehungsweise sanktionsrechtlichen Konsequenzen des eigenen Handelns zu tragen (sich zum Beispiel die Freiheit zu regelabweichendem Verhalten durch ein Bußgeld zu erkaufen), unterbinden *impossibility structures* das rechtswidrige Handeln selbst.[41] Der Mensch ist dadurch zwar

39 Dazu ausführlich O'Hara, Laurence: »Grundrechtsschutz vor psychisch vermittelter Steuerung – Beschränkte Autonomie und verhaltenswissenschaftliche Annahmen in der Grundrechtsdogmatik«, in: Archiv des öffentlichen Rechts 145 (2020), S. 133-187.

40 Das Konzept von *predictive policing* geht über die intelligente Videoüberwachung hinaus und erfasst je nach Wortgebrauch alle Big-Data- oder KI-getriebenen Analysemethoden zu Sicherheitszwecken. Gute Übersicht zum aktuellen Forschungsstand bei Sprenger, Johanna: »Verbrechensbekämpfung«, in: Martin Ebers/Christian Heinze/Tina Krügel/Björn Steinrötter (Hg.), Rechtshandbuch Künstliche Intelligenz und Robotik, München: C.H. Beck 2020, § 31, m. w. N. bes. in Fn. 135.

41 Grundlegend Rich, Michael: »Should We Make Crime Impossible?«, in: Harvard Journal of Law & Public Policy 36 (2013), S. 795-838, bes. S. 802-804 zur Definition. Zur Einführung in die deutsche Diskussion T. Rademacher: Wenn neue Technologien altes Recht durchsetzen: Dürfen wir es unmöglich machen, rechtswidrig zu handeln? (Fn. 24). In der deutschen Diskussion ist mitunter auch von »embedded law« die Rede, siehe M. Becker: Von der Freiheit, rechtswidrig handeln zu können (Fn. 24), S. 637.

nicht berechenbar(er), aber seine Unberechenbarkeit in Sachen Rechtsgehorsam wird neutralisiert. *Impossibility structures* in diesem Sinn sind etwa die Filtersysteme, die die Kommunikationsströme im Internet nicht (nur) überwachen, sondern immer häufiger auch direkt verhindern, dass rechtswidrige Kommunikation erfolgt. Wenngleich die EU sich noch nicht dazu durchringen kann, den Einsatz von *impossibility structures* zum Beispiel durch Plattform- und Suchmaschinenbetreiber verbindlich vorzuschreiben, gibt es doch immer mehr Rechtsakte und Vorschläge für neue Rechtsakte, die zum Einsatz ermuntern oder ihn zumindest ausdrücklich erlauben (Stichwort Upload-Filter).[42] *Impossibility structures* sind aber auch in der analogen Welt denkbar, wenn etwa intelligente Steuerungssysteme verhindern, dass sich Autos anders als im Rahmen des straßenverkehrsrechtlich Zulässigen nutzen lassen.[43]

Wenngleich diese Beispiele gegenwärtig noch punktuell erscheinen, sollte berücksichtigt werden, wie weit verbreitet digitale ›intelligente‹ Systeme in unserer Umwelt bereits sind und alsbald sein werden. Moinis *Der Würfel* ist – in diesem Sinne – kein Zukunftsroman, sondern ein Roman über unsere Gegenwart, in dem einige Entwicklungen weitergedacht werden, deren Anfänge wir schon heute konkret beobachten. Er wirft damit die auch juristisch drängende Frage auf, wie sehr wir künftig von Sensorik umgeben sein werden und sein wollen, die erkennen kann, ob wir rechtstreu oder rechtswidrig handeln, oder dies gar technisch verunmöglicht und sanktioniert.

---

42 Eine starke Ermunterung ist Art. 17 Abs. 4 der EU-Richtlinie 2019/790 über das Urheberrecht im digitalen Binnenmarkt. Vgl. auch Art. 6 über »Proaktive Maßnahmen« des Vorschlags der EU-Kommission für eine Verordnung zur Verhinderung der Verbreitung terroristischer Online-Inhalte, COM(2018) 640 final v. 12.9.2018. Eine ausdrückliche Erlaubnis von *impossibility structures* findet sich im neuen Vorschlag der EU-Kommission für einen *Digital Services Act* v. 15.12.2020, COM(2020) 825 final. Art. 6 des Vorschlags stellt klar, dass Diensteanbieter wie etwa Youtube, Facebook oder auch Amazon mit seinem von vielen Diensteanbietern genutzten Cloud-Dienst AWS weiterhin in den Genuss von Haftungsprivilegien kommen sollen (Art. 5 des Vorschlags), und zwar auch dann, wenn sie ihre Plattformen *freiwillig* nach rechtswidrigen Inhalten ihrer Nutzer*innen filtern. Eigentlich war das Haftungsprivileg für Diensteanbieter geschaffen worden, die Nutzer*innen lediglich einen Upload von Inhalten ermöglichen, ohne selbst Einfluss auf die Inhalte nehmen zu wollen (sogenannte Hosting-Dienste).

43 Der Hersteller Volvo hat entsprechende Systeme für seine künftigen Fahrzeuge bereits angekündigt. Siehe Maak, Niklas: »Sie sind alle auf 180«, Frankfurter Allgemeine Sonntagszeitung v. 10.3.2019, S. 38.

3 Ein ›Recht zum Rechtsverstoß‹ im digital optimierten Recht?

Wie verhalten sich Grundgesetz und bundesverfassungsgerichtliche Rechtsprechung zu einem möglichen digitalisierten Vollvollzug des Rechts? Wie steht das Gericht im Spannungsverhältnis von menschlicher Unberechenbarkeit und Autonomie (einschließlich der Freiheit zum Rechtsverstoß) und technologisch ermöglichter ›perfekter‹ Durchsetzung des demokratisch-rechtsstaatlich gesetzten Rechts?

Vorneweg: Ein Recht zum Rechtsverstoß oder präziser: ein Recht auf Gegen-Recht-verstoßen-*Können* hat das Bundesverfassungsgericht nie anerkannt. Es kann dies aus seiner institutionellen Eigenlogik heraus vielleicht auch nicht tun. Denn nach seinem Selbstverständnis als ›Optimierer‹ unseres Rechtssystems wird das Gericht immer versuchen, dafür zu sorgen, dass Bürger*innen einen legitimen Freiheitswunsch auch *rechtsförmlich* artikulieren können (»Freiheit durch Verfahren«). Und dennoch zeigt das Gericht, wenn es um Überwachung und Rechtsdurchsetzung geht, interessanterweise dieselbe ambivalent-abwägende Haltung, die in Moinis *Würfel* zum Ausdruck kommt.[44]

In einer seiner zentralen Entscheidungen zum Einsatz automatisierter Erkennungstechnologien, also nach hiesiger Diktion einem Fall von *intelligent surveillance*,[45] etablierte das Verfassungsgericht im Jahr 2018 eine *Vermutung zugunsten der Rechtschaffenheit* von Bürger*innen.[46] Konkret ging es in dem Verfahren um automatisierte Kennzeichenkontrollen, mit denen Fahrzeuge gefunden werden sollen, die im Fahndungsregister verzeichnet sind.

---

44 Wichtig ist an dieser Stelle der Hinweis, dass hier keine verfassungsrechtlich ›saubere‹ Gesamteinordnung dazu geliefert werden kann, ob, wo, wie und von wem neue Technologien eingesetzt werden dürfen, um Rechtsregeln einem Vollvollzug anzunähern. Dazu sind die möglichen Technologien intelligenter Überwachung zu vielfältig. Dazu Rademacher, Timo/Perkowski, Lennart: »Staatliche Überwachung, neue Technologien und die Grundrechte«, in: Juristische Schulung 60 (2020), S. 713-720.

45 BVerfG Beschluss v. 18.12.2018 – 1 BvR 142/15, E 150, S. 244 – Kennzeichenkontrollen 2.

46 Siehe ebd., Rn. 51, wo das Gericht zusätzlich darauf hinweist, dass staatliche Überwachung Einschüchterungseffekte auslösen kann, sodass Bürger*innen eventuell sogar auf legales Handeln verzichten. Daher: »Zur Freiheitlichkeit des Gemeinwesens gehört es, dass sich die Bürger grundsätzlich fortbewegen können, ohne dabei beliebig staatlich registriert zu werden, hinsichtlich ihrer Rechtschaffenheit Rechenschaft ablegen zu müssen und dem Gefühl eines ständigen Überwachtwerdens ausgesetzt zu sein […].«

Die vom Gericht etablierte Rechtschaffenheitsvermutung besagte hier sinngemäß, dass der Staat von seinen Bürger*innen nicht verlangen darf, ständig nachzuweisen, dass sie (beziehungsweise ihr Auto) *nicht* amtlich zur Fahndung ausgeschrieben sind – unabhängig davon, dass die Abfrage gar nicht zu spüren wäre, denn sie erfolgt ja automatisiert im Vorbeifahren. Diese Vermutung dürfe der datenverarbeitende (also: der überwachende) Staat nur durchbrechen, wenn es dafür einen Anlass gibt.[47] Der Staat muss also zum Beispiel den Verdacht haben, dass gesuchte Personen beziehungsweise Fahrzeuge in einer bestimmten Gegend aufzufinden sein werden (oder allgemeiner, jenseits des konkreten Beispiels: dass etwas Gefährliches passieren könnte oder etwas Strafbares passiert ist), etwa durch einen Hinweis aus der Bevölkerung oder eine Streife gehende Polizistin. Das Zufällige, das in einer solchen Anlassbindung verborgen liegt, wird vom Gericht konserviert. So schafft es einen mehr oder weniger großen Freiheitsraum für abweichendes Verhalten und verweist den Staat auf reaktive Arrangements zum Umgang mit der Unberechenbarkeit der Bürger*innen im Rechtsgehorsam.

Aber doch nicht ganz: Denn ausdrücklich sollen auch anlassunabhängige Kontrollen möglich bleiben.[48] Wenn

> polizeiliche Kontrollen an ein gefährliches oder risikobehaftetes Tun beziehungsweise an die Beherrschung besonderer Gefahrenquellen anknüpfen, kann schon darin ein dem Verhältnismäßigkeitsgrundsatz genügender Grund liegen. Die Rechtfertigung für Kontrollen kann dort bereits an der besonderen Verantwortung der Betroffenen gegenüber der Allgemeinheit anknüpfen und bedarf deshalb eines darüberhinausgehenden Anlasses grundsätzlich nicht.[49]

47 BVerfG Beschl. v. 18.12.2018 – 1 BvR 142/15, E 150, S. 244 Rn. 93 – Kennzeichenkontrollen 2. Jüngst bestätigt von BVerfG Beschl. v. 10.11.2020 – 1 BvR 3214/15, Rn. 102, 107ff. – Antiterrordateigesetz II, und BVerfG Beschl. v. 27.5.2020 – 1 BvR 1873/13 = NJW 2020, 2699 Rn. 145-150 – Bestandsdatenauskunft II.

48 Es ist dann auch von ›Verdachtsgewinnungsverfahren‹ die Rede. Grundlegend hierzu Bull, Hans Peter: »Polizeiliche und nachrichtendienstliche Befugnisse zur Verdachtsgewinnung«, in: Lerke Osterloh/Karsten Schmidt/Hermann Weber (Hg.), Festschrift Peter Selmer, Berlin: Duncker & Humblot 2004, S. 29-50.

49 BVerfG Beschl. v. 18.12.2018 – 1 BvR 142/15, E 150, S. 244 Rn. 94 – Kennzeichenkontrollen 2: »Für automatisierte Kennzeichenkontrollen kommt das etwa in Betracht, wenn mit ihnen Gefahren bekämpft werden, die sich gerade aus dem Betrieb der Kraftfahrzeuge ergeben, etwa die Durchsetzung der Versicherungspflicht durch Kontrollen zum Auffinden unversicherter Fahrzeuge.«

Zudem seien auch »stichprobenhaft[50] durchgeführte Straßenverkehrskontrollen oder anlasslose Kontrollen in weiten Teilen etwa des Umwelt- und Wirtschaftsverwaltungsrechts« weiterhin erlaubt (wobei hier in der Entscheidung unklar bleibt, ob diese auch automatisiert erfolgen dürfen oder nicht).[51] Etwas abgesetzt davon heißt es dann noch, dass Kontrollen, um verhältnismäßig zu sein, nicht »flächendeckend« eingeführt werden dürfen.[52]

Was bedeutet dies für die Frage nach Berechnung und Freiheit in der digitalen Welt? Bei aller Zurückhaltung im Hinblick auf Verallgemeinerungen verfassungsgerichtlicher Rechtsprechung kann man folgende These aufstellen:

In einem ersten Schritt konserviert das Bundesverfassungsgericht mit seiner ›Anlassdogmatik‹ die reaktive Art des staatlichen Rechtsvollzugs – unter Rückgriff auf eine allgemeine Rechtschaffenheitsvermutung. Es bleiben damit Freiräume für die autonome Entscheidung des Menschen (etwa für abweichendes Verhalten) und damit für die (subjektive) Zufälligkeit des Rechtsgehorsams. Im nächsten Schritt verdünnt das Gericht die Anlässe aber deutlich, indem schon gefährliches oder gefahrgeneigtes Verhalten von Bürger*innen (etwa Autofahren) einen ausreichenden Anlass für ›anlasslose‹ automatisierte Kontrollen geben kann. Dies aber wird unter den Vorbehalt gestellt,[53] dass solche Kontrollen nicht flächendeckend sein dürfen; das Zufällig-Stichprobenhafte mit seinen devianzsichernden Effekten bleibt also *ein bisschen* erhalten.

---

50 Dazu, dass Stichprobenkontrollen trotz ihrer Zufälligkeit nicht willkürlich im rechtsstaatlichen Sinne sind, BVerfG Beschl. v. 28.6.1994 – 1 BvL 14/88, E 91, S. 118 (124) – Bezirksrevisor: Stichproben seien »nicht, wie es scheinen mag, von vornherein mit Willkür gleichzusetzen. Soweit es, wie hier, nicht um die Zuteilung von Leistungen, sondern um die Kontrolle der Rechtmäßigkeit einer Leistung geht, kann es sogar dem Gleichbehandlungsgebot in besonderer Weise Rechnung tragen, da das Kontrollrisiko gleichmäßig verteilt wird.«

51 BVerfG Beschl. v. 18.12.2018 – 1 BvR 142/15, E 150, S. 244 Rn. 94 – Kennzeichenkontrollen 2.

52 Ebd., Rn. 100.

53 Wobei in der zitierten Entscheidung die Bezüge an dieser Stelle zugegeben unklar sind, da die Ausführungen zu »anlasslosen Kontrollen« in Rn. 94 erfolgen, die zum Verbot einer »flächendeckenden« Überwachung indes in Rn. 100, sodass hier große Restunsicherheiten verbleiben.

4 Ein austariertes Verhältnis von Berechnung und Zufallselementen für individuelle und gesellschaftliche Freiheit

Die von uns analysierten Beispiele aus der zeitgenössischen Literatur illustrieren, dass die digitale Erfassung des Menschen in mancher Hinsicht durchaus wünschenswert sein kann: Zahlreiche Figuren in Moinis Roman schätzen die Optimierung, die ihnen der Würfel-Algorithmus in verschiedenen Lebensbereichen bietet, etwa bei der Partnervermittlung oder der Verbrechensbekämpfung. Die Beispiele zeigen aber auch, wo Berechenbarkeit als Norm an Grenzen stößt: Die Literatur veranschaulicht mit ihren fiktionalen Zukunftsexperimenten, welche positive Rolle Formen von Zufall, Serendipität oder ein Bewusstsein für Kontingenz im Leben spielen können: als Grundlage für das Entdecken oder Erleben von etwas Neuem, als Beobachtung von etwas ursprünglich nicht Gesuchtem, das sich als überraschend nützlich oder angenehm erweist, oder als Voraussetzung für ein Denken in fiktionalen Welten, in denen variierende Strukturen oder Szenarien erprobt werden können. Zufall, Serendipität oder Kontingenz schaffen damit wichtige Gegengewichte zu einer berechneten Welt und vermeintlich berechenbaren Menschen.

Dies lässt sich auf das Recht als Anschauungsfeld übertragen: Der Verstoß Einzelner gegen demokratisch gesetzte Rechtsnormen ermöglicht der Gesellschaft insgesamt einen Einblick in alternative Welten. Oft wird diese Erfahrung von Devianz gesamtgesellschaftlich unerwünscht sein, denn die meisten Rechtsnormen erweisen sich als gut und vernünftig für das Gemeinwohl. Aber das gilt nicht für alle Normen, und das positive Urteil über unsere Normen gilt nicht für immer. Hier kann das (aus Sicht der Gesellschaft) Zufällige, das in der einzelnen menschlich-unberechneten Abweichungshandlung liegt, im Idealfall zu einer Form von Serendipität werden, das heißt Lernerfahrungen ermöglichen und Reflexionsprozesse auslösen. Die damit potenziell verbundene Einsicht in die Kontingenz des Rechtssystems kann den Blick schärfen für Varianten der Normgebung, die aktuell nicht verwirklicht, aber möglich (und vielleicht wünschenswert) sind.

Aus rechtsphilosophischer und (wohl) sogar aus verfassungsrechtlicher Perspektive ist es angesichts des immer wirkmächtigeren digitalisierten Rechtsvollzugs beziehungsweise immer wirksamerer digitalisierter Überwachung sinnvoll, bewusst Möglichkeiten zum Rechtsverstoß im Rechtssystem selbst vorzusehen, beispielsweise durch Elemente des Zufalls im Rechtsvollzug (nur eine zufällig ausgewählte Anzahl an Normverletzungen wird geahndet oder Ähnliches). Was *prima facie* wenig rechtsstaatlich scheint,

entpuppt sich bei genauem Hinsehen als Strategie der Flexibilisierung und Dialogisierung des Rechts: eine Leistung, die früher rein faktisch durch die Unmöglichkeit eines technisch optimierten Vollvollzugs des Rechts erbracht wurde, die heute und vor allem zukünftig aber als bewusste architektonische Leistung in das Rechtssystem wird eingeschrieben werden müssen. Das auf diese Weise vermittelte ›Recht zum Rechtsverstoß‹ ist demnach kein einklagbares Recht, aber eine wichtige Denkfigur, die den Wert des Auch-anders-sein-Könnens des Rechts illustriert und dabei hilft, Freiheit(sräume) auszuloten.

In seinem Buch über *Die Möglichkeit der Normen* fordert Christoph Möllers bereits einen Ort des Zufalls in der Rechtsordnung:

> Wenn man unterstellt, dass die technologische Entwicklung nicht per se aufzuhalten ist, müssen die Leistungen normativer Ordnungen [z.B. Ermöglichung von Devianz im Recht] in sie integriert werden. Dazu könnte es gehören, die Vorgaben […] durch Zufallsarrangements anzureichern.[54]

Mit seiner flexiblen ›Anlassdogmatik‹ – dem dreistufigen Konzept aus (1) grundsätzlich gebotenem Anlass, (2) ausnahmsweise anlasslosen Kontrollen, die aber (3) nicht flächendeckend sein dürfen – hat das Bundesverfassungsgericht eine Stellschraube für solche Arrangements geschaffen.[55]

Es erlaubt damit dem rechtsdurchsetzenden Staat, die Unberechenbarkeit der Bürger*innen in Sachen Rechtsbefolgung zurückzudrängen, ohne dadurch den Weg für einen digitalen Vollvollzug freizugeben, der *jede* Freiheit zur Normabweichung und damit jede Form von Serendipität verdrängt.

Vor diesem Hintergrund können nun die eigentlich schwierigen – und zugleich spannenden – Fragen gestellt werden: Wenn nicht überall, *wo genau* wollen wir als technisch optimierte Wesen in einer berechneten Welt le-

---

54 C. Möllers: Die Möglichkeit der Normen (Fn. 36), S. 478. Eigentlich hat der Zufall in der Rechtswissenschaft keinen guten Leumund, er gilt als zu lösendes Problem (z.B. Haftung für zufällige Schäden, vgl. beispielhaft §§ 446, 848 BGB). Nur unter eher engen Voraussetzungen kommt Zufall nach herrschender Meinung als rechtsstaatlich akzeptabler Steuerungsmechanismus für staatliches Handeln infrage.

55 Dies gilt trotz der Unsicherheit, ob das in der zitierten Entscheidung des BVerfG aufgebaute Urteil so verallgemeinerungsfähig ist. Zusätzliche Fragen, die hier nicht vertieft werden können, wirft das im Grundgesetz in Art. 5 Abs. 1 S. 3 vorgesehene Zensurverbot auf, das im Rahmen der Kommunikationsregulierung im Internet durch Upload-Filter und sonstige Technologien des Moderierens von Inhalten besonders zu berücksichtigen ist.

ben? Wo soll, darf oder muss Raum für die fehlende Perfektion gelassen werden?[56] Die Fragen reichen weit über literarische Imaginationsräume und den Rechtsvollzug hinaus. Sie sind genuin philosophische Fragen, die diejenigen, die sie stellen, zwingen, sich grundlegend zu den Bedingungen des Menschseins zu positionieren. Das von uns abgesteckte Feld in Literatur und Recht bietet einen Ausgangspunkt, um Hoffnung und Unbehagen im Hinblick auf neue Technologien verallgemeinernd zu diskutieren. Wir plädieren dabei für ein austariertes Verhältnis von Berechnung und Zufallselementen als Element individueller und gesellschaftlicher Freiheit.

56 Hier ist abschließend auf eine jüngere Entscheidung des Gerichtshofs der Europäischen Union (EuGH) zu verweisen, der zum »Schutz der nationalen Sicherheit [und zur] Bekämpfung schwerer Kriminalität« die in der EU eigentlich unzulässige anlasslose »Vorratsdatenspeicherung« im speziellen Fall von IP-Adressen mit der Begründung zugelassen hat (EuGH Urteil v. 6.10.2020 – verb. Rs. C-511/18, C-512/18 und C-520/18 (La Quadrature du Net), Rn. 156), dass »im Fall einer im Internet begangenen Straftat die IP-Adresse der einzige Anhaltspunkt sein kann, der es ermöglicht, die Identität der Person zu ermitteln, der diese Adresse zugewiesen war, als die Tat begangen wurde« (ebd., Rn. 154). Kurz gesagt: Wenn und weil bestimmte Delikte – namentlich nennt der EuGH Kinderpornografie (ebd.) – ohne eine Vorratsdatenspeicherung im Internet strukturell nicht verfolgbar wären, ist die Speicherung *aller* IP-Adressen mit den Unionsgrundrechten vereinbar.

2.1.4 Privatheit
Zur Zukunft des Datenschutzes

Nils Leopold

I Privatheit in Gefahr

Wie sehr Privatheit und Selbstbestimmung gefährdet sind, insbesondere was staatliches Handeln angeht, zeigte zuletzt die durch die *Snowden-Enthüllungen* bekannt gewordene, weltumspannende geheimdienstliche Massenüberwachung. Denn der Präventionsstaat als spezielle Form des Überwachungsstaates zielt auf die effiziente Überwachung des Verhaltens der Bürger*innen mit digitalen Mitteln.

Was das Handeln privater Akteure angeht gewinnt seit Jahren der Konflikt um Datenökonomie und Privatheit an Schärfe. Der moderne Datenkapitalismus hat persönliche Daten zum flüssigen Gold erklärt. Wie schief oder falsch auch immer diese Formel sein mag,[1] die Betonung liegt stets auf dem Grundsatz: »Die Daten müssen fließen.« Der Skandal um Facebook und seine millionenfache Weitergabe von Kundendaten an das mit Wahlmanipulationen durch sogenanntes Microtargeting befasste Unternehmen Cambridge Analytica war ein Weckruf. Im Mittelpunkt der Auseinandersetzung steht die gewachsene Datenmacht großer Unternehmen. Ihre datengestützten digitalen Geschäftsmodelle verschieben die gesellschaftlich akzeptierten Grenzen grundlegend: Insbesondere Big Data und künstliche Intelligenz (KI) erlauben eine bislang nicht dagewesene feingranulare Auswertung und Überwachung der Datenspuren ganzer Bevölkerungen. Sie schaffen ein spezifisches Prognosewissen zur Manipulation von Menschen zu meist kommerziellen Zwecken.

1 Zutreffender dürfte es sich bei Daten in vielen Kontexten um gemeinwohlrelevante Grundlagen für das Wissen der Gesellschaft insgesamt handeln. Dementsprechend bedürfte es eher der Verständigung über weitere staatliche Interventionen zur Sicherung solcher gemeinwohlbezogener Verwertungen (Stichwort: Open Data).

Die Bürger*innen haben es weitgehend nicht mehr selbst in der Hand, durch ihr eigenes Verhalten einer Erfassung und digitalen Bewertung zu entgehen, selbst wenn sie bestimmte Angebote und Plattformen nicht nutzen.

Zugleich verändern der soziale und technische Wandel die Ideen und Leitbilder von Privatheit. Die geradezu klassisch zu nennende Vorstellung von Privatheit als einer Art individueller Kontrolle, also der Möglichkeit, selbst entscheiden zu können, wer wann Zugang zu den eigenen Angelegenheiten hat, scheint überholt. Müssen wir daher das Ende der Privatheit konstatieren?

Die These dieses Beitrages lautet: Nein – denn in der liberalen Demokratie muss sich nicht der Mensch in digitale Geschäftsmodelle und staatliche Effizienzkonzepte einfügen, sondern vielmehr muss es weiterhin darum gehen, den Einsatz digitaler Technik menschengerecht zu gestalten. Das Private ist politisch – das gilt auch, wenn es um seine Formung durch die Digitalisierung geht.

Wenn etwa zukünftig anhand algorithmenbasierter Auswertungen des Verhaltens in sozialen Netzwerken Kredite vergeben und Arbeitsstellen besetzt werden, wenn dabei selbst Personen, die sich nie auf entsprechenden Plattformen bewegt haben, diesen maschinenbasierten Prognosen unterworfen werden oder wenn Videoüberwachung in öffentlichen Räumen mit biometrischer Gesichtserkennung aufgerüstet wird, dann stehen grundlegende Machtverteilungsfragen der Gesellschaft auf dem Spiel. Auch die Auseinandersetzungen um die Corona-Warn-App oder um die Einführung von digitalen Impfpässen belegen, wie sehr gesellschaftliche Konflikte um neue Technologien von Fragen nach den Folgen für die Privatheit der Einzelnen und der Gesellschaft insgesamt geprägt sind. Man kann fast sagen: Wertegeleitete Diskurse rund um die Digitalisierung sind aktuell vor allem Privatheitsdiskurse.

Funktionen von Privatheit

Bei all diesen Konflikten geht es um Privatheit als Sicherung der individuellen Zugänglichkeitsgrenzen von Menschen. Es geht um den Erhalt von persönlichen Freiräumen. Die Funktionen der Privatheit sind dabei vielfältig. Privatheit wird etwa als Bedingung von Identität und Individualität, physischer oder emotionaler Entspannung beschrieben, als Bedingung der Möglichkeit von Kreativität und des Lernens, der Verhaltensvielfalt, von vertraulichen Nähebeziehungen, der Ausbildung und Ausfüllung einer Pluralität von Rollen

oder der individuellen Autonomie. Damit trägt sie auch zu einer pluralistischen Gesellschaft bei.[2]

Datenschutz als Schutzkonzept der Privatheit

Privatheit bildet einen entscheidenden Wert in der Digitalisierung, gerade weil digitale Verfahren und Instrumente die Grenzen persönlicher Freiräume grundlegend verschieben. Sie steht daher mit Recht im Mittelpunkt der politischen Debatte darum, wie Datenmacht einzuhegen ist. Daneben steht die Selbstbestimmung als Paradigma liberaler Rechtsordnungen, die ihre Verankerung unter anderem im Würdegebot des Grundgesetzes findet. Als Grundrecht auf Datenschutz der Grundrechte-Charta der EU sowie als Menschenrecht auf Privatheit haben die Konzepte von Privatheit und Selbstbestimmung längst weltweite normative Verbreitung gefunden.

Privatheit und Selbstbestimmung[3] gelten deshalb als Bollwerk zum Schutz von Freiheit und Autonomie, weil sie nicht bloß eine moralische Idee oder partikulare Ethik der Vernunft repräsentieren, sondern als bindendes Recht entfaltet sind. Vor allem das Datenschutzrecht enthält wichtige Steuerungselemente zum Schutz vor Überwachungsstaat und Überwachungskapitalismus.

Doch muss der Datenschutz auf mehreren Ebenen entschlossen weiterentwickelt werden, um angesichts der enormen gesellschaftlichen Herausforderung durch die Digitalisierung seiner Funktion weiterhin gerecht zu werden. Dabei werden Konzepte von Privatheit und Selbstbestimmung weit über den Datenschutz hinaus zu einer Ausdifferenzierung der Instrumente und gesellschaftlichen Antworten zum Schutz der Rechte der Bürger*innen führen müssen. Ansatzpunkte für die nötigen Weiterentwicklungen liefert auch die Kritik an Privatheit und Selbstbestimmung, deren genauere Analyse daher lohnt.

II Kritik an der Privatheit

Die Auseinandersetzungen um Privatheit und Selbstbestimmung in der Digitalisierung erfolgen in Wellenbewegungen. Eher selten schlägt das Pendel

2 Vgl. Albers, Marion: Grundrechtsschutz der Privatheit, in: DVBL 2010, S. 1062 m.w.N.

3 Siehe auch den Beitrag von Christiane Woopen und Sebastian Müller in diesem Band.

dabei stärker zugunsten der Privatheit aus. Zuletzt allerdings konnte dies beobachtet werden, als in einem europäischen Kraftakt die Datenschutz-Grundverordnung (DSGVO) verabschiedet wurde. Vorherrschend scheint aber ein Grundsound der Vergeblichkeit. Die sozialwissenschaftliche Kritik behauptet unter anderem, die Konzepte seien der Komplexität der Herausforderung nicht (mehr) gewachsen, seien ohne Rückhalt im konkreten Handeln der Bevölkerung, die freiwillig auch noch die fragwürdigsten digitalen Angebote in Anspruch nehme (Privacy Paradox). Daher kommen die Konzepte stets zu spät oder seien sogar gleich denklogisch ausgeschlossen.

Systemtheorie und Big Data

Zum Teil wird vertreten, Privatheit und Selbstbestimmung seien am Ende, weil die Digitalisierung letztlich eine evolutionäre, quasi zwingenden Gesetzmäßigkeiten folgende Entwicklung darstelle. Die dabei innerhalb von Systemlogiken handelnden Wirtschaftsunternehmen oder staatlichen Stellen seien in ihrem Verhalten letztlich nicht determinierbar. Das Funktionieren digitaler Technik sichere vielmehr seine Akzeptanz. Privatheit und Selbstbestimmung werden verkürzend als Konzepte individueller Kontrolle dargestellt. Das Besondere digitaler Technik im Allgemeinen als auch von Big Data im Besonderen liege darin, dass sie Informationen bei Dritten erzeugten, die sich also der Kontrolle der Einzelnen entziehen.[4] Insbesondere das Konzept der Einwilligung (unter anderem als Cookie-Banner bekannt) laufe vor dem Hintergrund von Big Data leer, weil es letztlich nur eine kurzfristige Handlungshemmung in einer ansonsten überwiegend im Unbewussten ablaufenden Digitalnutzung setze.

Der Kritik ist darin zuzustimmen, dass sie einige der mit den überindividuellen Auswirkungen von Big Data verbundenen konzeptionellen Fragen für Selbstbestimmung und zunehmend fragwürdige Instrumente wie die Einwilligung aufgreift. Eine umfängliche Debatte im Datenschutz setzt sich seit langem mit der Frage auseinander, welche zusätzlichen Elemente die Relevanz dieses Instruments erhalten können. Nicht überzeugend ist die Suggestion

4 »Die Digitaltechnik mit ihren detektivischen Funktionen ist ein Mittler, der mich dazu bringt, etwas zu tun, was ich nicht selbst kontrollieren kann«, vgl.: Nassehi, Armin: Muster. Theorie der digitalen Gesellschaft, Bundeszentrale für politische Bildung, 2020, S. 315.

einer Alternativlosigkeit in der Gestaltung digitaler Anwendungen. Stets bestehen Handlungsoptionen, und der weitere gesellschaftliche Handlungsrahmen wird durch Politik und Recht mitbestimmt. Überholt ist jedoch das konzeptionelle Verständnis von Privatheit als individueller Kontrolle. Vielmehr wird Privatheit etwa im Datenschutz seit langem durch ein wesentlich breiteres präventives Konzept aus einer Vielzahl von Elementen geschützt, mit denen auf die die Informationen verarbeitende Organisation abgezielt wird (interne Datenschutzvorgaben, Rechtmäßigkeitskontrolle, Privacy by Design-Vorgaben usw.). Individuelle Kontrolle, etwa in Gestalt der Einwilligung, ist lediglich ein steuerndes Element, und unterliegt selbst weiteren zum Schutz der Betroffenen eingezogenen Beschränkungen.

Der Vorwurf der Fehlkonstruktion

Ein Kritikansatz betont konzeptionelle Mängel des Datenschutzrechts. Unterstellt wird ein allgemeines Verbot unterschiedslos allen personenbezogenen Datenverarbeitungen, egal ob es sich um Facebook oder den Bäcker an der Ecke handele. Stattdessen bedürfe es des Grundsatzes des freien Flusses von Daten, nur in besonderen Fällen müsse gesetzlich geregelt werden. Mit dem sogenannten »Verbotsvorbehalt« werde eine risikobezogene Unterscheidung von höchst unterschiedlichen digitalen Anwendungen unmöglich gemacht.

Diese Kritik überbetont einen letztlich rechtskonstruktiven Aspekt. In der Praxis bestehen für kleine und mittlere Unternehmen alle rechtlichen Freiheiten, die benötigten Daten zu verarbeiten. Richtig ist allerdings, dass viele kleine Unternehmen bedeutend geringere Risiken für die Privatheit von Kund*innen oder Beschäftigten darstellen. Erleichterungen von den zahlreichen Anforderungen der Datenschutzgesetze erscheinen daher ausbaufähig.

Datenschutz als Innovationsbremse und Bürokratieklotz

In diesem Gewand kommt politisch motivierte Kritik des Datenschutzes typischerweise daher. Zumeist fehlen Argumente, die den Vorwurf untermauern. Auch wird er häufig herangezogen, um von anderweitigen Missständen im Bereich unternehmerischer oder staatlicher Digitalisierungsvorhaben abzulenken. Der Datenschutz wird somit als Sündenbock genutzt. Oft scheint diese Kritik auch der parteipolitischen Profilierung zu dienen, weil sie als Ausweis der eigenen Fortschritts- und Wirtschaftsfreundlichkeit verstanden sein will.

Diese Kritik erschwert die Weiterentwicklung des Datenschutzes ungemein. Sie verstärkt bestehende Widerstände in Organisationen und erschwert sachbezogene Auseinandersetzungen. Die Unterstellung einer allgemeinen Innovationshemmung ist abwegig. Ob und in welchem Umfang etwa ein digitales Geschäftsmodell als innovativ bezeichnet werden kann, entscheidet sich auch nach seinen Gemeinwohlwirkungen. Letztlich stellen Datenschutzüberlegungen auch Faktoren der Akzeptanz von digitalen Anwendungen dar. Nachweisbare Datenschutzvorkehrungen schaffen Vertrauen bei Kund*innen und Bürger*innen.

Die Wahrnehmung von Privatheit wird auch durch Bewertungen des digitalen Wandels in seiner Gesamtheit beeinflusst. So wird in der Debatte um Künstliche Intelligenz fundamentaler Zweifel am menschlichen Selbstverständnis freier Selbstbestimmung laut. Die Vorstellung von Menschen als individuelle autonome Entscheidungsträger sei aufgrund der Überlegenheit KI-gestützter, durchdigitalisierter Umgebungen nicht mehr aufrecht zu erhalten.[5] Richtig ist vielmehr, dass Konzeptionen von Privatheit und Selbstbestimmung schon heute ein differenziertes Verständnis menschlicher Autonomie zugrunde legen. Ob und in welchem Umfang ein Schutz gewährleistet werden kann, bleibt letztlich eine Frage der politischen Verständigung.

Die allermeisten Klagegesänge haben der Privatheit letztlich nichts anhaben können. Im Gegenteil zeigt sich: Privatheit ist mehr denn je tragende Säule der Digitalisierung, weil sie ein diverses, sich ständig wandelndes Konzept und Denkmuster ist: Als privat kann bezeichnet – und muss geschützt – werden, was jeweils die Funktionen von Privatheit erfüllt.[6]

Zudem ist sie im Recht – den Grundrechten des Grundgesetzes ebenso wie dem europäischen Recht und den internationalen Menschenrechtsregimen – tief verankert. Daran kommt auch die sozialwissenschaftliche und politisch motivierte Kritik nicht vorbei. Allerdings verweisen einige der hier angeführten Kritikbeispiele auf Modernisierungsbedarf insbesondere beim Datenschutzrecht.

5 Vgl. u.a. Harari, Yuval, Harari: Homo Deus, München: C.H. Beck 2018.
6 Vgl. Albers, a.a.O., S. 1063.

III Datenschutz: Plötzlich im Mittelpunkt

Der Datenschutz hat weltweit Konjunktur. Nach neuen Datenschutzgesetzen in Ländern wie Japan, Brasilien und Thailand ist am 1. Januar 2020 sogar in Kalifornien, am Ursprungsort des Überwachungskapitalismus, der California Consumer Privacy Act (CCPA) in Kraft getreten. Er orientiert sich in vielem an deutschen und europäischen Datenschutzregelungen für die Wirtschaft und öffentliche Institutionen.[7] Insbesondere die Datenschutz-Grundverordnung (DSGVO) der EU gilt als globaler Goldstandard der Gesetzgebung.[8]

Allerdings sollte man die bloße Schaffung von Gesetzen nicht überbewerten. Schließlich entscheidet über deren tatsächliche Bedeutung und Wirkung erst der gesellschaftliche und kulturelle Zusammenhang, in dem sie zur Anwendung kommen. So boten etwa das ausgefeilte Bundesdatenschutzgesetz über Jahrzehnte einen eher geringen Schutz der Rechte der Bürger*innen, weil es kaum durchgesetzt wurde. Private Akteure jedenfalls ignorierten über Jahre dessen Vorgaben größtenteils und betrachteten es als bloßen Papiertiger.

Die 2018 in Kraft getretene Datenschutz-Grundverordnung (DSGVO) hat diese Lage wesentlich verändert. Die EU beendete damit ihre gut 20 Jahre andauernde eigene Laissez-faire-Haltung in Sachen Digitalisierung und Privatheit. Denn die effektive Umsetzung stellt einen der Schwerpunkte des Gesetzes dar.

Möglich war das politisch wohl nur aufgrund einiger besonderer Umstände. In der EU war über Jahre der Eindruck gewachsen, man habe vor allem den großen US-Unternehmen der Digitalwirtschaft wirtschaftlich nichts entgegenzusetzen. Aufwändige Kartellverfahren gegen Google oder Microsoft zogen sich lange hin, selbst Strafen in Milliardenhöhe schienen keine Wirkung zu haben. Angebote und Plattformen dieser Unternehmen dominieren nach wie vor die verschiedenen Märkte in einer Weise, die zu massiven Abhängigkeiten europäischer Unternehmen führt. Echten Handlungsdruck erzeugten schließlich die Bedrohungen für so etablierte europäische Wirtschaftszweige

7 Er ist zwar nicht auf EU-Bürger anwendbar, deren Daten im Silicon Valley verarbeitet werden. Seine Existenz hat allerdings Auswirkungen auf die lange geführte US-Debatte um die Schaffung einer möglichen bundesstaatlichen Regelung. Zum Teil geht der CCPA sogar darüber hinaus.

8 Vgl. Bradford, Anu: The Brussels Effect. How the European Union Rules the World, Oxford: Oxford University Press 2020.

wie das Automobilgeschäft. Vor diesem Hintergrund waren womöglich wettbewerbsförderliche Korrekturen von Geschäftsmodellen zumindest in Teilen auch über die Datenschutzgesetzgebung erreichbar und daher auch für europäische Wirtschaftskreise akzeptabel. Und die großen US-Digitalkonzerne konnten so immerhin auf mehr Rechtssicherheit und ein *level playing field* (gleiche Wettbewerbsbedingungen) in Europa setzen.

Stets spielt dabei auch das Ziel der Datensouveränität eine gewisse Rolle. Es fasst im Wesentlichen die Bereitschaft Europas zusammen, eine gegenüber den dominanten Digitalmächten USA und China eigenständige Datenpolitik zu verfolgen, um die heimische Wirtschaft vor Abhängigkeiten zu schützen.

Doch auch und insbesondere der bundesdeutsche und europäische Datenschutzdiskurs haben die DSGVO ermöglicht. Der Unmut über das Geschäftsgebaren von Unternehmen wie Facebook, Google und Co. und deren offenkundiger Unwille zu mehr Transparenz und Mitbestimmung über die kommerzielle Verwertung der kundenbeziehbaren Informationen und Daten war und ist groß. Mitten in die Umsetzungsphase des Gesetzes fielen im Sommer 2013 dann die Veröffentlichungen des Whistleblowers Edward Snowden. Sie gaben der DSGVO Rückenwind. Schwere Irritationen löste die mit den Snowden-Leaks verursachte Erkenntnis aus, wie sehr Europa in ein weltumspannendes Netzwerk von Massendatenabgriffen westlicher Geheimdienste verstrickt ist. Das totalitäre Potenzial der modernen Datenverarbeitung wurde sichtbar. Zumindest lag es nicht fern, Privatheit als eine vor dem Untergang zu bewahrende kulturelle Leistung moderner demokratischer Gesellschaften wahrzunehmen. Immerhin hatte der Geheimdienstskandal damit seinen Anteil daran, dass der schillernde Begriff der digitalen Souveränität seinen Eingang in die Datendebatten fand.[9]

Heute steht die EU mit der DSGVO im Wettbewerb mit den streng marktliberal ausgerichteten, datenschutzarmen USA und dem autoritären, auf Überwachung der Gesamtbevölkerung abzielenden China als Leuchtturm grundrechtlicher und rechtsstaatlicher Bürgerorientierung da.

Die DSGVO kommt in den EU-Mitgliedstaaten unmittelbar zur Anwendung, was die Möglichkeiten, ihre Vorgaben zu umgehen, entscheidend verringert. Massive Sanktionsandrohungen und gerichtliche Klagen von Betroffenen verschafften dem Datenschutz erstmalig die volle Aufmerksamkeit auch in den Chefetagen. Der Anwendungsbereich wurde auf alle

9 Siehe hierzu auch den Beitrag von Julia Pohle und Thorsten Thiel in diesem Band.

Unternehmen ausgeweitet, die mit ihren Produkten und Dienstleistungen den europäischen Markt erreichen (Marktortprinzip). Das zwang sogar die sogenannten GAFA plus M[10], sich mit der DSGVO auseinanderzusetzen. Erst kürzlich erklärte der Europäische Gerichtshof dann in der spektakulären Schrems-II-Entscheidung auf Grundlage der DSGVO das EU-Abkommen mit den USA über Datenübermittlungen in die USA für unwirksam. Damit wurden auf einen Schlag sämtliche Datenflüsse in die USA von Unternehmen mit Kunden in Europa rechtlich unsicher. Denn das Urteil lässt offen, in welchem Umfang bestehende rechtliche Instrumente diesen Datenflüssen weiter als Grundlage dienen können. Das Urteil war eine Reaktion auf den umfassenden Zugriff von US-Geheimdiensten auf die Daten der Digitalunternehmen, und auf den nicht mit Europa vergleichbaren Schutzstandard für Daten in den USA. Zwar bleibt damit die Rechtsunsicherheit der vielen betroffenen Unternehmen hoch und eine tragfähige Rechtsgrundlage für die Datenflüsse fehlt weiterhin. Doch der Datenschutz ist zu einer rechtlichen Größe gewachsen, mit der gerechnet werden muss.

Auf den zweiten Blick sieht es für den Datenschutz kurz- bis mittelfristig weniger rosig aus. Zumindest die EU-Kommission und die Datenschutzaufsichtsbehörden stehen unter Druck, viele Bestimmungen der DSGVO erst noch tatsächlich umzusetzen. Es hakt unter anderem bei der Abstimmung zwischen den Aufsichtsbehörden, ausgerechnet die Quasi-Monopolisten wie Facebook und Co. konnten bislang nicht belangt werden. Ungemach droht dem Datenschutz auch und gerade aus der Politik. Dort steigt der Druck, endlich Erfolge bei der Digitalisierung der Verwaltung, dem sogenannten E-Government, vorzuweisen. Der Datenschutz wird oft als störend wahrgenommen, übergangen oder als Sündenbock für gescheiterte Digitalprojekte missbraucht. Die immer wieder aufflammende Debatte um den Datenschutz als vorgebliches Hindernis bei der Corona-Bekämpfung steht stellvertretend für diesen Umgang. Die etablierte EU-Wirtschaft schließlich sieht sich durch die Digital-Konkurrenz aus China und den USA bedroht und fordert deshalb massive Unterstützung beim Aufbau datengetriebener Märkte. Die Politik gibt diesem Druck zunehmend nach, zugleich sträubt sie sich dagegen, nach

10 Google, Amazon, Facebook, Apple und Microsoft

der Verabschiedung der DSGVO noch eine weitere rote Linie zum Schutz der Bürger*innenrechte zu ziehen.[11]

Auch die Corona-Pandemie spitzt viele liegen gebliebene oder verdrängte Probleme der Digitalisierung weiter zu. Der Druck zur sofortigen Digitalisierung, etwa im Bereich der Schulen, erzwingt pragmatische Entscheidungen und legt gnadenlos die Überforderung der zuständigen Behörden offen. Diese sind beispielsweise weder rechtlich noch faktisch in der Lage, Videokonferenzsoftware auf Datenschutzkonformität zu prüfen und Empfehlungen auszusprechen, ohne mit dem Risiko längerer Gerichtsverfahren gegen ihre Bewertungen rechnen zu müssen. Derweil sind fast die einzigen Profiteure der Pandemie die Quasi-Monopolisten der Digitalwirtschaft, deren Einfluss auch in der EU beständig zunimmt und die weiterhin als Quasi-Gesetzgeber Standards in ihrem Einflussbereich setzen. Hier bleibt der Gesetzgeber gefordert, im Rahmen der Plattformregulierung seinen grundrechtlichen Schutzpflichten nachzukommen und gegebenenfalls bis hin zu Entflechtungen der betreffenden Konzerne die Grundrechte der Bürger*innen durchzusetzen.

Was schützt der Datenschutz?

Was genau aber schützt der Datenschutz? Die Antwort weist den Weg, wie der Datenschutz weiterzuentwickeln ist.

Lange Jahre dümpelte der Datenschutz als Steckenpferd früher Informatiker*innen und Nischenjurist*innen in einem eher akademischen Abseits. Vieles änderte sich mit dem Volkszählungsurteil von 1983. Vorausgegangen waren breite Proteste in der Bevölkerung gegen Art und Umfang dieser Datenerhebung. Das Bundesverfassungsgericht schuf aus unterschiedlichen anerkannten Strängen des Grundrechts auf Achtung der freien Entfaltung der Persönlichkeit ein auf die Datenwelt zugeschnittenes, eher weit angelegtes Recht auf informationelle Selbstbestimmung.[12]

Vor dem Urteil galten Inhalte und Daten allerdings nur dann als schützenswert, wenn sie der *Privatsphäre* entstammten, also die Privatheit ihres Entstehungskontextes teilten.[13] Digitalisierung aber verselbstständigt gera-

11 Insoweit beispielhaft erscheinen die Verzögerungen um die sogenannte E-Privacy-Verordnung, die ursprünglich mit der DSGVO verabschiedet werden sollte und Regelungen zum Schutz der Onlinekommunikation vorsieht.

12 Siehe hierzu auch den Beitrag von Ulf Buermeyer und Malte Spitz in diesem Band.

13 Vgl. dazu die maßgebliche Untersuchung von Albers, Marion: Informationelle Selbstbestimmung, Baden-Baden: Nomos 2001.

de Informationen gegenüber ihrem Entstehungszusammenhang. Wer etwa seine private Kommunikation über das auf Vernetzung und Werbung ausgelegte Unternehmen Facebook führt, bewegt sich angesichts der entstehenden und nicht steuerbaren zusätzlichen Datenerfassungen nicht mehr in einem als privat zu bezeichnenden Raum. Kontextverlust ist Kennzeichen und insoweit Ziel der Datenverarbeitung, als gerade eine multifunktionale Verwendung von Daten angestrebt wird. Besonders deutlich wird das im heutigen Paradigma der Kombination aus Big Data und Techniken der KI, mit denen beliebige Korrelationen von Datenbeständen für statistische Prognosen ermöglicht werden. Am prominentesten wird die breite Nutzung von Gesundheitsdaten diskutiert. Der Datenschutz bietet hier ein weit angelegtes Schutzkonzept mit verschiedenen Schutzelementen, wie der Zweckbindung von Datenverarbeitungen, der Notwendigkeit von Rechtsgrundlagen, von Transparenz, Beteiligungsrechten und effektiver Aufsicht. Das Bundesverfassungsgericht bestätigte mit dem Volkszählungsurteil dieses Konzept im Wesentlichen innerhalb des Rechts auf informationelle Selbstbestimmung, das damit weit über technischen Datenschutz hinausreicht.

Der Umgang des Staates mit persönlichen Informationen und Daten wurde danach vom Bundesverfassungsgericht zielgenauer bearbeitet: Spezielle weitere Rechte wie das Recht am eigenen Wort, am eigenen Bild, das allgemeine Persönlichkeitsrecht oder auch das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (das sogenannte IT-Grundrecht) wurden geschaffen. Mit dieser Auffächerung setzte das Bundesverfassungsgericht eine Dimension des Volkszählungsurteils um, wonach erst der konkrete Verwendungskontext von Daten über den Schutzbedarf entscheidet.

It's the infomation, stupid

Im Volkszählungsurteil schlummert eine weitere Grundentscheidung. Anders als die bis dahin bestehenden Datenschutzgesetze, die sich eng auf die Verarbeitung personenbezogener Daten konzentrieren, wurde das Recht auf informationelle Selbstbestimmung eben gerade nicht allein als Recht am eigenen Datum, sondern gleich eine ganze Dimension höher angelegt.[14] Statt eines eigentumsanalogen Verständnisses, wonach Daten natürlichen Personen

14 So zutreffend Forgó, Rn. 33, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, München: C.H. Beck, 3. Auflage 2019.

praktisch *gehören*, wurden übergreifend *Selbstbestimmungsrechte* für diejenigen geschaffen, die von Datenverarbeitungsprozessen betroffen sind. Die Bürger*innen bestimmen zum Teil darüber mit, ob und in welchem Umfang die sie betreffenden Informationen und Daten verarbeitet werden dürfen. Dementsprechend steht heute die Einwilligung als Rechtsgrundlage für Verarbeitungen im Mittelpunkt, aber auch etwa Auskunftsrechte, Widerspruchs- und Löschungsrechte.

Auf Grundlage dieses Urteils zeigte sich in der Rechtswissenschaft[15] schon bald: Eigentlich geht es nicht um Datenschutzrecht, sondern um ein Recht des Umgangs mit personenbezogenen Informationen und Daten.[16] Man kommt ohne die Unterscheidung von Informationen und Daten nicht mehr aus: Informationen sind die eigentliche Leitkategorie, nicht Daten. Daten sind die auf einem Datenträger sehr selektiv festgehaltenen Zeichen, die als Informationsgrundlagen dienen. Als bloße Zeichen weisen sie für sich allein auch keinen Personenbezug auf.

Informationen hingegen betreffen den Sinn, der aus Beobachtungen, Mitteilungen oder Daten erst erzeugt werden kann und muss. Informationsinhalte knüpfen also an Daten an, doch sie setzen auch eine aktive Interpretationsleistung des sinnhaften Verstehens der empfangenden Stelle oder Institution voraus. Damit rücken die Behörden oder Unternehmen und deren Prozesse in den Vordergrund. Deren interne Prozesse bilden einen Wissens- und Interpretationskontext, der auch ihr Handeln bestimmt. Deutlich wird: Wer den Umgang mit diesen personenbeziehbaren Daten effektiv schützen will, muss auf dieser empfangenden und verarbeitenden Seite durch präventive Vorgaben regulieren. Letztlich wird damit erst klar, wo die Risiken liegen, und wie weitgehend die Vorgaben des Rechts sein müssen, um die Betroffenen wirksam zu schützen. Der Schutz vor Staat und Wirtschaft hat inzwischen vergleichbaren Umfang, auch wenn er juristisch anders hergeleitet wird. Die Risiken für die Privatheit mögen im Einzelnen anders gelagert sein, erscheinen aber im Bereich der Wirtschaft heute vielfach tiefgreifender. Zudem behalten sich staatliche Stellen auch hier den Zugriff vor.

15 Grundlegend: Albers, Marion: Informationelle Selbstbestimmung, Baden-Baden: Nomos 2005.

16 Mit dem Telekommunikationsgeheimnis in Artikel 10 des Grundgesetzes gibt es eine spezifische Schutzausprägung von Kommunikationen und allen dabei anfallenden Daten.

Die neuen (und alten) Herausforderungen der Digitalisierung

Der Datenschutz musste sich in Reaktion auf neue Entwicklungen der IT-Industrie beständig fortentwickeln, um den durch die informationelle Selbstbestimmung gebotenen Schutzstandard zu gewährleisten. Bedeutende Weiterentwicklungen lagen in Konzepten von Zertifizierungen und Audits, dem Privacy by Design, dem Selbstdatenschutz oder der Transparenz von Technik.[17] Den Aufsichtsbehörden wird viel Konkretisierungsarbeit bei der Auslegung von Gesetzen überlassen. Doch für einzelne Entwicklungen wird dieser bestehende allgemeine Rahmen kaum mehr genügen.

Bereits während der Verhandlungen zur DSGVO wurde die vielgestaltige Nutzbarkeit von Big Data in Verbindung mit KI als offenkundig grundlegende Veränderung in Wirtschaft und Verwaltung erkannt. Dabei geht es um technische Systeme, die so konzipiert sind, dass sie Probleme eigenständig bearbeiten und sich selbst auf veränderliche Bedingungen einstellen können. Systeme künstlicher Intelligenz basieren auf der Analyse von Massen von Daten (Big Data), die zum ständigen Trainieren der Algorithmen gebraucht werden. Noch geht es um die auf bestimmte Ziele beschränkte, schwache KI und um überwiegend unterstützende Aufgaben. Doch zukünftig werden mit der sogenannten starken KI Systeme entstehen, die in der Lage sind, die Vorgaben der Programmierung zu verlassen und eigenständige kognitive Fähigkeiten aufzubauen. Sie sind mehr als je zuvor bei digitaler Technologie eine Black Box. Sie sind insbesondere mit der Auswertung großer Datenmengen (Big Data) befasst, um Prognosen zu erstellen und komplexe Prozesse zu steuern. Als ein Beispiel gilt das selbstfahrende Auto. Sensorgestützte Umwelten der Datenerfassung, die wiederum digitale Zwillinge analoger Umgebungen zu erstellen suchen, bilden die Grundlage. Deren Daten werden den sogenannten Big-Data-Reservoirs (z.B. in Gestalt von Cloud-Datenspeichern) zur Verfügung gestellt, die als Datenpools für das Trainieren der Algorithmen dienen. Es handelt sich um eine übergreifende, alle Wirtschafts- und Gesellschaftsbereiche erfassende IT-Entwicklung: Von der Krebsbekämpfung über Predictive Policing (vorhersagende Polizeiarbeit) bis zum autonomen Fahren soll KI die technische Grundlage für Innovationen und neue Geschäftsmodelle bilden

17 Zu den vielfältigen Ambivalenzen dieser Ansätze vgl. z.B.: Richter, Philipp: Big Data, Statistik und die Datenschutz-Grundverordnung, in: Datenschutz und Datensicherheit 2016, S. 91.

und Entscheidungsprozesse steuern. Die beschriebenen Herausforderungen lassen sich unter anderem durch die folgenden Ansätze angehen.

(1) Anonymisierung und Personenbezug

Gerade bei Big-Data-Analysen ist vorab unklar, wofür Daten verarbeitet werden. Zusätzlich ist es für Aufsichtsbehörden kaum möglich, die Transparenz der Funktionsweise und Nachvollziehbarkeit (Revisibilität) zu sichern. Und Anwender*innen versuchen durch vollständige Anonymisierung den Anwendungsbereich des Datenschutzes gänzlich zu meiden. Doch gelingt eine vollständige Anonymisierung im heutigen Umfeld der Datenverarbeitung faktisch kaum noch oder nicht dauerhaft zuverlässig. Dynamische Veränderungen der Datensätze und auch wachsendes Zusatzwissen wie etwa durch Open-Data-Datenbanken erlauben die De-Anonymisierung.

Dieser Befund stellt daher die bislang auch vom Gesetzgeber vehement vorgenommene Trennung personenbezogener und nicht-personenbezogener Daten infrage. Wenn heute scheinbar anonyme Datenbestände durch die erwartbare Art und Weise ihrer Verarbeitung zu irgendeinem Zeitpunkt doch wieder personenbeziehbar werden, liegt es nahe, auch die bisherige völlige Befreiung nicht-personenbezogener Daten vom rechtlichen Regime des Datenschutzes anzuzweifeln. Damit gerät auch der Glauben an die schützenden Wirkungen der Anonymisierung, an den sich auch der Gesetzgeber klammert, ins Wanken.

(2) Daten als kommerzielle Güter und Innovationsressource

Die neuen Technologien entwickeln sich im internationalen Wettbewerb der Datenökonomien.[18] Aus ökonomischer Sicht werden personenbezogene Daten längst als kommerzielle Güter bewertet und auch gehandelt. Beispielhaft stehen hierfür die gigantischen Werttaxierungen der großen IT-Unternehmen sowie die in der Praxis von Unternehmenskäufen entscheidende Due-Diligence-Prüfung (sorgfältige Prüfung) auch der personenbezogenen Datenbestände zur Werterhebung und Kaufpreisbildung. Politisch erfahren derzeit Datenstrategien und KI-Entwicklungen allerhöchste Priorität und Förderung. Im Kern geht es darum, Datennutzung, Datentausch und Datenhandel zu ermöglichen und zu fördern, um die für die digitale und insbesondere die KI-Wirtschaft erforderlichen massenhaften Datenbestände zu erschließen. Neben der Öffnung von (zunächst) nicht-

18 Lesenswert: Datenökonomie, APuZ, 60. Jahrgang, 2019.

personenbezogenen Daten sollen dabei stets auch personenbezogene Datenbestände mobilisiert und besser handelbar werden. Beispielsweise werden vermehrt sogenannte Datentreuhänder und datenaltruistische Organisationen in Stellung gebracht.[19] Unabhängig von diesen gesetzgeberischen Anstrengungen besteht ein weltweit organisierter, sehr weitgehender grauer Handel mit personenbezogenen Daten.

(3) Einwilligungsfragen und kollektive Wirkungen durch Datenverarbeitung
Das bestehende Datenschutzregime bleibt individualistisch ausgerichtet. Der Schutz der oder des Einzelnen steht im Mittelpunkt. Konsequenterweise steht im privaten Sektor die individuelle Einwilligung zur Datenverarbeitung im Mittelpunkt. Diese ist im Kontext des Internets und komplexer Datenverarbeitungen schon lange als problembehaftet erkannt, wenn nicht dysfunktional geworden. Die Allgemeinen Geschäftsbedingungen der Anbieter sind unlesbar, überfordern und fallen damit als Informationsquelle für die Betroffenen aus.[20] Die allermeisten Menschen klicken sich ritualisiert durch. Das beste Beispiel bieten die mit Inkrafttreten der DSGVO noch penetranteren sogenannten Cookie-Banner. Hier blockiert die Werbeindustrie weiterhin nutzerfreundliche technische Lösungen etwa durch sogenannte Do-not track-Browser-Voreinstellungen.

IV Die Weiterentwicklung des Datenschutzes

Recht bietet stets hochselektive, notwendig unvollkommene Antworten auf komplexe gesellschaftliche Problemlagen. Aber es ist ein wichtiger Teil einer Immunantwort rechtsstaatlich gefasster Gesellschaften auf die Folgen des digitalen Wandels.

Der Datenschutz und das bestehende Datenschutzrecht werden in den kommenden Jahren im Wesentlichen fortbestehen. Dafür hat schon die umfassende Aufnahme des Konzepts in die DSGVO gesorgt. Um den Erfolg der DSGVO zu bewahren, bedarf es in den kommenden Jahren großer Anstrengungen der EU-Kommission, der Aufsichtsbehörden der Mitgliedstaaten, des

19 Vgl. etwa den Entwurf des Data Governance Act vom 25.11.2020, COM (2020) 767 final. Mit dem sog. Data Act wird für Herbst 2021 gerechnet.

20 Fallen die Begleittexte zu schlicht aus, bergen sie allerdings das Risiko des Überlesens wichtiger Konsequenzen, ebenfalls ein Dilemma.

Europäischen Datenschutzausschusses als ihr Koordinierungsgremium und der Regierungen der EU-Mitgliedstaaten. Der Nachweis der Vollziehbarkeit dieses Rechts steht im Mittelpunkt. Wo irgend möglich, muss die Aufsicht effizienter konstruiert und auf die wirklich wesentlichen Aufgaben der Rechtsdurchsetzung gegenüber besonders risikoreichen Verfahren und Anwendungen ausgerichtet werden.

Doch daneben zeichnen sich notwendige gesetzliche und konzeptionelle Weiterentwicklungen ab.

Zum einen gilt dies für die DSGVO selbst. Viele ihrer Bestimmungen sind notwendig abstrakt und unpräzise. Oft wird die Konkretisierung der Bestimmungen insoweit durch den Europäischen Datenschutzausschuss der Aufsichtsbehörden und die Gerichte erfolgen müssen. Doch teilweise wird das nicht ausreichen. Ein Beispiel bietet die Regelung von automatisierten Entscheidungen beziehungsweise des Profilings. Die entsprechende Norm des Artikels 22 DSGVO regelt ausgerechnet die vielfältigen Risiken, die mit Profilbildungen einhergehen, äußerst unzureichend. Für zahlreiche andere Bestimmungen erscheinen Präzisierungen der Normen im Sinne der Rechte der Verbraucher*innen diskussionswürdig.[21]

Von grundlegenderer Bedeutung ist die durchgängige bessere Differenzierung von Datenverarbeitungen nach ihren tatsächlichen Risiken. Während wegen des Grundsatzes der Technikneutralität bestimmte Formen der Datenverarbeitung wie Big Data, Cloud Computing oder KI in ihren Funktionen nicht gezielt geregelt werden, gelten viele der Grundsätze des Datenschutzes in praktisch gleichem Umfang auch für kleine Unternehmen, die im Schwerpunkt gar nicht mit der Verarbeitung von Daten befasst sind. Hier muss letztlich, auch im Sinne der Fokussierung und der Akzeptanz des Datenschutzes, zukünftig besser abgeschichtet werden.

Besonders hervorzuheben sind notwendige Verbesserungen zum Schutz von unbeteiligten Dritten. Big-Data-Analysen und selbstlernende algorithmenbasierte Entscheidungsverfahren liefern umfassende statistische Prognosegrundlagen. So werden auch Personen und Personengruppen bewertet und womöglich diskriminierend schlechter gestellt, die selbst gar nicht notwendigerweise durch ihre Daten an der Herstellung der Bewertungsgrundlagen mitgewirkt haben. Ehepartner*innen und Familienangehörige etwa erhalten aufgrund ihrer Nähe zur betroffenen Person

21 Umfangreiche Vorschläge für mögliche Änderungen finden sich bei Roßnagel/Geminn: Datenschutz-Grundverordnung verbessern, Baden-Baden: Nomos 2020.

vergleichbare Kreditbewertungen. Ähnliches geschieht beim Geoscoring, bei dem alle Bewohner*innen einer Straße oder eines Stadtviertels aufgrund der statistisch errechneten Dichte von Kreditrisiken einsortiert werden. Bei der Verarbeitung genetischer Daten einer Person sind automatisch alle näher Verwandten mit betroffen. Diese womöglich auch gänzlich anonymen Verfahren bewirken eine kollektive Vergemeinschaftung bestimmter Merkmalsträger[22] und können das Handeln Betroffener weitreichend bestimmen, wenn sie sich entsprechend anpassen, um bestimmten Mustern statistischer Normalität zu entsprechen. Die damit verbundenen Fragen weisen über das Datenschutzrecht teilweise deutlich hinaus und adäquate Schutzvorkehrungen müssen gefunden werden. Ein grundlegendes, bislang nicht gelöstes Problem stellt schließlich auch die Reproduktion von Diskriminierungen in den Algorithmen dar. So kam es vor, dass biometrische Gesichtserkennung Menschen mit dunkler Hautfarbe überhaupt nicht erkannte.[23]

Grundsätzlich bietet der Datenschutz zwar ein überaus breites Anwendungsfeld mit je nach Kontext seines Einsatzes ganz unterschiedlichen Schutzgegenständen. So können beispielsweise Maßnahmen zum Schutz vor Diskriminierungen bereits im Rahmen von bestehenden gesetzlichen Vorgaben für soziale Netzwerke zur Anwendung kommen. Sogenannte Dark Patterns von Plattformangeboten, also Designs von Oberflächen mit dem Ziel, zu bestimmten Handlungen zu verleiten, können die Freiwilligkeit von Einwilligungen berühren und verdienen nähere Beachtung. Gerade für den Bereich von Big Data und KI bedarf es aber der Weiterentwicklung und problemgerechten Erweiterung der Normen. Eine nach Risiken der Anwendungen abgestufte Regelung, wie etwa von der Datenethikkommission der Bundesregierung vorgeschlagen, sichert eine differenzierte gesetzliche Bewertung.

Auf einer grundlegenden konzeptionellen Ebene wird der Datenschutz nicht um die Klärung einiger Grundlagen herumkommen: Die für seine Anwendbarkeit maßgebliche Grenze des Personenbezuges wirkt einerseits zu eng, andererseits zu unspezifisch. So basiert Big Data häufig auf *mixed data sets*, es werden also personenbezogene und nicht-personenbezogene Daten miteinander vermengt. Wie oben beschrieben, werden so vormals nicht-personenbezogene Daten personenbeziehbar und müssen daher – je nach ge-

22 Vgl. zum Ganzen Roßnagel, a.a.O, S. 162ff.

23 Siehe hierzu auch die Beiträge von Eric Hilgendorf, von Lorena Jaume-Palasí und von Francesca Schmidt und Nicole Shephard in diesem Band.

planter Verarbeitung – womöglich schon vor einem feststellbaren Personenbezug gewissen Schutzregelungen unterworfen werden.

Zentrale Herausforderungen für den künftigen Datenschutz zeichnen sich ebenso in einzelnen Regelungsfeldern ab, etwa die im Gesundheitsdatenschutz augenfällige überkomplexe Regelungsvielfalt, die Reform der Datenschutzaufsicht mit dem Ziel größerer Einheitlichkeit und Augenhöhe gegenüber großen Unternehmen sowie die effektivere Durchsetzung des Datenschutzes bei der Abstimmung der Behörden im Mehrebenensystem der EU.

Das Gesetzgebungverfahren zur DSGVO selbst hat die Idee von bereichsspezifischen Datenschutzregelungen aufgegriffen. So sollte neben der Datenschutz-Grundverordnung eine E-Privacy-Verordnung der EU unter anderem für einen ausgeprägten Schutz der besonders gefährdeten Online-Kommunikation sorgen. Dies erscheint angesichts der Schutzvorgaben des Grundgesetzes etwa für das Telekommunikationsgeheimnis auch dringend geboten.

Den Mitgliedstaaten werden in der DSGVO zudem eigene gesetzliche Regelungen nahegelegt, etwa für den Bereich des Beschäftigtendatenschutzes oder zum Ausgleich von Pressefreiheit und Datenschutz. In beiden Bereichen gibt es vielfältige offene und komplexe Regelungsfragen, deren Lösung auf gesetzlicher Ebene für alle Seiten mehr Rechtssicherheit bieten könnte.

(1) Verbraucher(-daten-)schutzrecht

Die nun seit über zwanzig Jahren diskutierte Kommerzialisierung personenbezogener Daten und das stetig wachsende Feld des Verbraucherdatenschutzrechts legen eine aktive gesetzgeberische Weiterentwicklung nahe. Einen Anfang hat die EU mit der Digitale-Güter- und Dienstleistungen-Richtlinie[24] gemacht. Auch der Datenschutzdiskurs darf sich dieser Diskussion nicht verschließen. Zu sehr sind Daten in ihrem kommerziellen Wert längst Gegenstand und Ziel der Geschäftsmodelle der Wirtschaft.

Verbessert werden muss die Stärkung der Stellung der Verbraucher*innen im Verhältnis zu übermächtigen Anbietern. Verbraucher*innen verdienen Unterstützung etwa durch gezielte Qualitätsprüfungen von riskanten Verfahren wie etwa KI-Anwendungen durch unabhängige Prüfstellen. Verbraucherschutzverbände könnten mit eigenständigen Beschwerderechten ausgestattet werden. Und Verfahren der treuhänderischen Wahrnehmung

24 Vgl. https ://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX :32019L0770

von Datenschutzrechten durch spezialisierte Anbieter verdienen zur Entlastung der Verbraucher*innen eine nähere Prüfung. Im Umgang mit Big Data, aber auch zur Unterstützung der Bürger*innen bei der Nutzung der vielen privaten digitalen Angebote können zukünftig sogenannte PIM-Software (Product Information Management) und Datentreuhandangebote womöglich entscheidend zum Schutz der Bürger*innen beitragen.

Der Überforderung der Verbraucher*innen mit der Art und Weise, wie Transparenzpflichten wahrgenommen und Entscheidungsverfahren ausgestaltet werden, muss mit weiteren Vorgaben vorgebeugt werden. Das Ziel der Verständlichkeit und der *Verdaubarkeit* von Informationen kann mit abgestuften Verfahren, den sogenannten *layered notices*, verbessert werden. Auch für Lösungen durch bildhafte Darstellungen liegen längst zahlreiche Vorschläge auf dem Tisch.

Naheliegend wären etwa gezielt den IT-Bereich aufgreifende zivilrechtliche Regelungen zur Kontrolle von Allgemeinen Geschäftsbedingungen (AGB). Die den Verbraucher*innen aufgezwungenen, skandalös intransparenten AGB der Internetunternehmen bieten hier genug Anhaltspunkte. Vorgeschlagen werden etwa inhaltliche Restriktionen des zulässig zu Vereinbarenden und Zertifizierungspflichten für besonders bedeutsame AGB.[25]

(2) Informationelle Selbstbestimmung für das digitale Zeitalter verankern

Gerade die jüngsten Reformvorschläge der EU zur Plattformregulierung zeigen eine gesteigerte Bereitschaft, auch Allgemeininteressen und weitere gesetzgeberische Ziele auf die Digitalwirtschaft auszudehnen. Dazu zählt etwa der Schutz vor Monopolbildung. Im Kern basiert das sich erweiternde Eingriffs-Instrumentarium der Kartellbehörden allerdings auf dem besonderen Schutzbedarf der von Plattformen monopolisierend und zweckwidrig verarbeiteten personenbezogenen Daten. Deutlich wird, dass daten- und informationsbezogene Regelungskomponenten in bislang davon unberührte Rechtsmaterien integriert werden.

Auch die Regelungen zur Bekämpfung von Hassbotschaften, Hassrede und Verhetzungen könnten in diesem Zusammenhang genannt werden, soweit diese Pflichten zur Herausgabe und Übermittlung personenbezogener Daten von Kund*innen an Sicherheitsbehörden betreffen, aber auch die hoch

25 So etwa Hoffmann-Riem, Wolfgang: Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, in: Archiv des öffentlichen Rechts 2017, S. 39.

problematische Filterung der persönlichen, zur Veröffentlichung bestimmten Inhalte von Kund*innen. Deutlich wird jedenfalls, dass der Datenschutz hier nur noch einen beschränkten Teil der informationellen Konflikte bearbeitet, zunehmend von weiteren Schutzzielen begleitet wird und Einbettung in übergreifendere Informationszusammenhänge erfährt.

(3) Rote Linien gegen ausufernde Datenerfassung

Viele Elemente des Datenschutzes zielen auf wohlabgewogene Anwendungen im Einzelfall und lassen den Betroffenen Handlungsspielräume im Sinne ihrer Selbstbestimmung. Damit wird einer vielfältigen Lebenswirklichkeit Rechnung getragen. Doch es muss auch klare und eindeutige rote Linien geben. Wo gravierende und multiple Risiken nicht nur für einzelne Betroffene und deren Rechte, sondern auch für die Kommunikation und die Privatheit der Gesellschaft insgesamt drohen, braucht es klare, absolute Grenzen. Hierzu zählen beispielsweise die unterschiedslos alle Bürger*innen betreffende anlasslose Vorratsdatenspeicherung von Kommunikationsverkehrsdaten, die biometrische Gesichtserkennung in öffentlichen Räumen sowie das umfassende Verhaltenstracking von sozialen Netzwerken zur Erstellung von Persönlichkeitsprofilen oder die verdeckte gezielte Beeinflussung von politischen Wahlen im Wege des sog. Microtargeting. Diese Beispiele belegen je für sich die enorme Dimension der Bedrohung für die Grundrechte, die die Digitalisierung angenommen hat.

Anpassung und Durchsetzung von Privatheit als Daueraufgabe

Die Zukunft der Privatheit hängt wesentlich vom politischen Willen ab. Letztlich zählt sie zwar dank der vielfältigen grundrechtlichen Verankerung zum Recht, dass notfalls dem Staat auch Schutzpflichten zu dessen Erhalt auferlegt. Deutlich sollte aber geworden sein, dass die Durchsetzung des bestehenden Rechts als auch dessen notwendige Weiterentwicklung eine anspruchsvolle Daueraufgabe darstellen. Angesichts der raschen Veränderungen durch die Digitalisierung muss das Datenschutzrecht selbst vielfältige und auch innovative Wege einschlagen, um weiter mithalten zu können. Abgesänge kommen, das zeigen gerade die intensiven Auseinandersetzungen um Privatheit in der jüngsten Zeit, jedenfalls zu früh. Die Selbstbehauptung menschlicher Freiheit und Privatheit in der sich beschleunigenden Digitalisierung erscheint vielmehr lebendiger denn je.

2.1.5 Würde

Gemeinwohlorientierte Plattformen als Grundlage sozialer Freiheit

Philipp Staab und Dominik Piétron

Viel ist in den vergangenen Jahren über die Zukunft der Arbeit im Zeichen ihrer Digitalisierung geschrieben worden. Die Debatte hatte zunächst zwei Schwerpunkte: Während auf der einen Seite die wirtschaftlichen Potenziale zeitgenössischer Kommunikationstechnologien betont wurden, fürchtete man auf der anderen Seite, dass gerade effizienzsteigernde Effekte der Digitalisierung zu Verwerfungen auf dem Arbeitsmarkt und letzten Endes zu »technologischer Arbeitslosigkeit« führen würden.[1] Doch diese Diskussion thematisiert im Grunde nur die gleichen Prognosen aus unterschiedlichen normativen Richtungen.[2] Sie ist zudem stark geprägt von »industrialistischen«[3] Erwartungen: Unternehmen gewinnen in einer solchen Perspektive Wettbewerbsvorteile, indem sie dank immer effizienterer Produktionsbedingungen vor der jeweiligen Konkurrenz liegen. Der Ort dieses Wettlaufs ist der Shopfloor (Produktionshalle) des produzierenden Sektors. Nur wer hier vorne liegt, kann im globalen Wettlauf dauerhaft punkten, denn wie Paul Krugman es formulierte: »Productivity isn't everything, but in the long run,

1 Wie Keynes es in seinem in der Debatte wieder zitierten Aufsatz zu den wirtschaftlichen Möglichkeiten unserer Enkelkinder erläutert hatte: Keynes, John Maynard: »Economic Possibilities for our Grandchildren«, in: John Maynard Keynes (Hg.), Essays in Persuasion, New York: W.W.Norton & Co. 1963, S. 358-373.

2 Da wirtschaftliches Wachstum sich am Ende aus Effizienzgewinnen speist, die in aller Regel durch betriebliche Rationalisierung erreicht werden, und da dies üblicherweise auch den Faktor Arbeit betrifft, sind Wachstumsgewinne und Druck auf Arbeit nur verschiedene Arten, den gleichen Zusammenhang zu thematisieren.

3 Baethge, Martin: »Abschied Vom Industrialismus. Konturen einer neuen gesellschaftlichen Ordnung der Arbeit«, in: SOFI-Mitteilungen 28 (2000), S. 87-102.

it is almost everything.«[4] Die deutsche Industrie 4.0-Strategie, die in diesem Jahr ihr zehnjähriges Jubiläum feiert, war der prononcierteste Ausweis dieser Sicht auf den technologischen Wandel in der Gegenwart.

Die Architekten der wirklich erfolgreichen Geschäftsmodelle der Digitalisierung zielten bisher freilich weniger auf Innovationen im Bereich der *Produktion*. In der wirtschaftlichen Praxis von Unternehmen wie Google, Amazon oder Uber geht es vielmehr um das Besetzen entscheidender Stellen für die *Distribution* von Gütern und Dienstleistungen.[5] Für die soziotechnische Organisationsform dieses Prozesses hat sich der Begriff digitale Plattform etabliert. Plattformen sind digitale Infrastrukturen, die verschiedene Akteure miteinander verbinden und es ihnen ermöglichen, als Marktteilnehmer*innen miteinander zu interagieren (zweiseitige Märkte). Dabei sind gerade Dienstleistungsplattformen in den vergangenen Jahren vielfach wegen ausbeuterischer Arbeitsbedingungen in die Kritik geraten – man denke nur an Proteste gegen die Arbeitsbedingungen von Uber-Fahrer*innen oder von Zusteller*innen der Essenslieferplattformen.

Der gesellschaftliche Konflikt in diesem Kontext fußt auf der Angst, dass sich die *Plattformisierung* der Wirtschaft und Arbeit über die bisherigen Grenzen hinaus verbreiten werde und damit soziale Standards oder gleich die soziale Marktwirtschaft gefährde. Unter dem Strich basiert der größte Teil der Kritik an der Plattformökonomie auf dem Vorwurf, sie sei Treiber eines Unterbietungswettbewerbs im Bereich von Einkommen und Arbeitsbedingungen und stelle historisch errungene Anrechte infrage.[6] So sind sogenannte Gigworker auf Dienstleistungsplattformen wie TakeAway oder Helpling, aber auch Online-Händler*innen auf Plattformen wie Amazon fest in die Organisation der Plattform eingebunden und von dieser abhängig, ohne dass die Plattformbetreiber ihre Verantwortung als Arbeitgeber wahrnehmen. Gigworker und Online-Händler*innen sind meist soloselbstständig und prekär beschäftigt. Sie müssen für ihre Arbeitsmittel selbst aufkommen, erhalten kein Urlaubsgeld oder Sozialversicherungsbeiträge und können dennoch nicht einfach auf andere Plattformen wechseln, da die Plattformbetreiber die

4 Krugman, Paul R.: The Age of Diminished Expectations. U.S. Economic Policy in the 1990s, Cambridge, Massachusetts: MIT Press, 1994.

5 Staab, Philipp: Falsche Versprechen. Wachstum im Digitalen Kapitalismus, Hamburg: Hamburger Edition 2016.

6 Nachtwey, Oliver/Staab, Philipp: »Die Avantgarde des Digitalen Kapitalismus«, in: Mittelweg 36 (6) (2015), S. 59-84.

Daten der Arbeiter*innen nicht freigeben. Einem Großteil der Plattformarbeiter*innen bleibt damit würdevolle Arbeit verwehrt. Gegenüber traditionellen Formen der Erwerbsarbeit fehlt ihnen der Status als abhängig Beschäftigte und die damit verbundenen Rechte.

Folglich stellt sich die Frage, ob digitale Plattformen überhaupt dem Gemeinwohl dienlich sind oder notwendigerweise als Ausbeutungsstrukturen funktionieren. Auch wenn der Lohndruck auf Plattformen sicherlich zu deren schneller Verbreitung beigetragen hat, kann nicht geleugnet werden, dass sie für Konsument*innen offensichtlich mit gewissen Wohlfahrtsgewinnen verbunden sind. Weil die anfallenden Daten ein effizientes Matching von Plattformteilnehmer*innen erlauben, ermöglicht die Vernetzung verschiedener Marktteilnehmer*innen einen reibungsloseren Austausch als klassische Märkte, was zum Vorteil aller Beteiligten wirken kann (niedrigere Transaktionskosten). Darauf aufbauend liegt es nahe, nicht die Plattformtechnologie selber für unwürdige Arbeitsbedingungen verantwortlich zu machen, sondern die sozialen Verhältnisse, in die sie eingelassen ist.

Vor diesem Hintergrund wollen wir im vorliegenden Beitrag untersuchen, wie die Arbeitsbedingungen auf Plattformen verbessert werden können. Dazu werden wir das Modell einer gemeinwohlorientierten Plattformorganisation skizzieren, also eines, das die Wohlfahrtsgewinne von Plattformen kollektiv sichert und Machtmissbrauch durch Plattformbetreiber verhindert. Hierfür werden wir zunächst (1) in groben Zügen das Modell der digitalen Plattform erläutern. Anschließend (2) werden wir aufbauend auf Axel Honneths Theorie gesellschaftlicher Freiheit die soziale Institution digitaler Plattformen normativ rekonstruieren und kritisieren, bevor wir schließlich (3) drei Grundprinzipien gemeinwohlorientierter Plattformen ausbuchstabieren – Öffentlichkeit, Mitbestimmung und Datensouveränität.

1 Plattformen als proprietäre Märkte

Wie bereits angedeutet lassen sich Plattformen als digitale Infrastrukturen beschreiben, die die Interaktion einer oder mehrerer Parteien ermöglichen. Shoshana Zuboff hat mit dem populär gewordenen Konzept des »Überwachungskapitalismus« versucht zu zeigen, dass jenseits dieser Basisdefinition vor allem Sekundärverwertungen der von Plattformen extrahierten Daten

eine entscheidende Bedeutung zukommt.[7] Daten sind demzufolge zunächst einmal das Nebenprodukt digitaler Kommunikation. Wann immer wir uns im digitalen Raum austauschen, hinterlassen wir Spuren, die einigen Unternehmen als eigene Profitquelle dienen. Die Leitfirmen dieser Entwicklung sind bekanntlich die Giganten der Online-Werbung, Google und Facebook.

Auch viele andere Autor*innen argumentieren auf Basis dieser Prämisse, die im Grunde die Selbstbeschreibung der genannten Unternehmen erst übernimmt, um sie dann zu kritisieren. Zuboff hat den Ansatz allerdings zu einer besonders umfassenden These über die Veränderung des Kapitalismus erweitert. Sie beschreibt, wie das eigentliche Ausschussprodukt (Nutzer*innen-)Daten im Laufe der 2000er Jahre – zunächst von Google und Facebook – als neuer, profitabler Rohstoff des kommerziellen Internets entdeckt wurde. Anstatt personenbezogene Daten wie ein normales Produkt zu behandeln und es beispielsweise in Portionen oder über Nutzerlizenzen zu verkaufen, habe man den eigenen Wert personenbezogener Daten erkannt und damit begonnen, sie zu aggregieren. Auf Basis der so entstehenden Informationsmacht ließen sich detaillierte Profile einzelner Personen erstellen und über den Verkauf zielgruppenspezifischer Werbung zu Geld machen. Das gesamte kommerzielle Internet lässt sich Zuboff zufolge als gewaltiger Überwachungsapparat verstehen. In den letzten Jahren hätten immer mehr Unternehmen ihre Wertschöpfung auf Überwachungsprofite ausgerichtet, weshalb von einem schnellen Vormarsch des Überwachungskapitalismus auszugehen sei. Bei der von Zuboff beschriebenen Praxis digitaler Plattformen geht es um den Aufstieg einer wirtschaftlichen Logik, die nicht auf das ressourceneffiziente Herstellen von Dingen gerichtet ist, wie es beispielsweise die deutsche Industrie 4.0-Strategie leitet, sondern auf die Vermessung, Beeinflussung und letztlich Steuerung unseres Verhaltens.

Eine nüchterne Betrachtung dieser Beschreibung wirft freilich die Frage auf, in welches größere wirtschaftliche Projekt diese Datenökonomie eingelassen ist. Eine Volkswirtschaft kann schließlich nicht nur aus Onlinewerbung bestehen. Hier kommt die *Theorie proprietärer Märkte*[8] ins Spiel. Demnach sind die Plattformunternehmen des kommerziellen Internets als Märkte in Privatbesitz zu verstehen. Sie sind nicht Marktakteure, die um letzte Promille

7 Zuboff, Shoshana: The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power, New York: PublicAffairs 2019.

8 Staab, Philipp: Digitaler Kapitalismus. Markt als Eigentum, Berlin: Suhrkamp 2019.

an Effizienzgewinnen einer tradierten Wirtschaftsform konkurrieren. Vielmehr haben sie sich vielerorts als Handelsmonopole für bestimmte Güter und Dienstleistungen etabliert, etwa Plattformen für Taxifahrten (Uber), Musik- und Videostreaming (Spotify), Fernbusfahrten (Flixbus), Hotellerie (Booking) oder Essenslieferungen (Lieferando). Die Leitunternehmen des kommerziellen Internets agieren, so die zugespitzte These, nicht wirklich auf Märkten, deren Preisbildungsmechanismen sie beispielsweise verzerren könnten. *Sie sind diese Märkte*. Die Marktfunktion selbst wird von ihnen privatisiert und in den Dienst einzelner Kapitalinteressen gestellt, indem etwa von denjenigen, die Güter oder Arbeitskraft auf den Plattformen anbieten, auf unterschiedliche Weisen Gebühren für die Marktteilnahme eingezogen werden.

Die Theorie proprietärer Märkte beschreibt nicht nur eine angebotsseitige Datenerfassung im Sinne Zuboffs, die auf das Verhalten potenzieller Käufer*innen ausgerichtet ist. Sie zielt vielmehr auch auf die nachfrageseitigen Effekte der plattformbasierten Wirtschaftskoordination, die eine weitreichende Restrukturierung ehemals vorgelagerter Wertschöpfung und damit von *Arbeit im weiteren Plattformkontext* zur Folge hat: Je stärker Online-Plattformen Absatzmärkte durch Skalen- und Netzwerkeffekte monopolisieren und eine Gatekeeper-Position zwischen Verkäufer*innen und ihren Kund*innen einnehmen können, desto eher können sie externen Unternehmen die Marktzugangsbedingungen diktieren, deren Arbeitsleistung in ihre eigene Wertschöpfungskette integrieren und vielfach die spezifischen Formen und Bedingungen der Arbeit festlegen.

Diese Logik lässt sich auch auf die umfassenden *soziotechnischen Ökosysteme*[9] der Leitunternehmen des digitalen Kapitalismus, Alphabet (Google), Apple, Facebook und Amazon, übertragen, die vielfältige digitale Dienste miteinander verknüpfen. Sie setzen sich aus je bereichsspezifischen Plattformen zusammen – wobei auch die digitale Infrastruktur, Hardware, wie Computer, Smartphones, Smart TVs und Wearables, als digitale Vermittlungsplattformen funktionieren –, über die Arbeitsleistungen externer Marktteilnehmer*innen, etwa Apps oder Filme, besteuert beziehungsweise mit hohen Provisionen von durchschnittlich 30 Prozent belegt werden. Die soziotechnischen Ökosysteme sind darauf ausgerichtet, sämtliche Bedürfnisse ihrer Nutzer*innen aus einer Hand zu befriedigen, und werden für eine wachsende Zahl von Unternehmen zum unumgänglichen Gatekeeper für den Zugang

9 Dolata, Ulrich: »Volatile Monopole. Konzentration, Konkurrenz und Innovationsstrategien der Internetkonzerne«, in: Berliner Journal für Soziologie 24(4) (2015), S. 505-529.

zu ihren Kund*innen. Diese Machtposition gleicht einer Goldgrube, weil auf immer kompetitiveren Verbrauchermärkten nur diejenigen etwas verkaufen können, die Wahrnehmung für ihre Produkte erzeugen. In dieser Aufmerksamkeitsökonomie monopolisieren die Digitalkonzerne den Zugang zu den Konsument*innen und können so wachsende Teile des geschaffenen Mehrwerts abschöpfen.[10]

Vier Formen der Kontrolle durch Plattformanbieter

Die Macht der Marktbesitzer materialisiert sich dabei in vier analytisch unterscheidbaren Formen der Kontrolle: Zunächst üben Plattformunternehmen durch (1) Überwachung eine Informationskontrolle aus,[11] das heißt anhand datenbasierter Verhaltenserfassung von Konsument*innen und Produzierenden sowie der darauf aufbauenden Sortierung und Kuratierung von Information für die jeweils andere Marktseite. Diese datenbasierte Intermediärsmacht ermöglicht drei weitere Formen der Kontrolle – von (2) Zugängen, von (3) Preisen und von (4) Leistungen. So entscheiden Plattformunternehmen, welche Anbieter*innen (2) auf den von ihnen betriebenen Märkten teilnehmen dürfen (Zugangskontrolle). Auf der Konsument*innenseite können sie zudem kontrollieren, wer welche Angebote zu welchen (3) Preisen zu sehen bekommt. Dies eröffnet nicht nur ein eigenes Geschäftsfeld, die algorithmische Preissetzung, sondern es ermöglicht den Plattformen zugleich eine lukrative Strategie der Preiskontrolle, die – anders als in der Monopoltheorie erwartet – bisher vornehmlich zugunsten, nicht zulasten der Konsument*innen eingesetzt wird: Durch ihre Macht über die Angebotsseite können die Marktbesitzer die Konkurrenz zwischen den Marktteilnehmer*innen im Dienste der eigenen Profite optimieren. So haben die Plattformbetreiber beispielsweise die Möglichkeit, das Angebot strategisch zu erweitern, um die Preise für Konsument*innen zu senken (und damit die Umsätze zu steigern).

Die (4) Leistungskontrolle zielt schließlich direkt auf die in ihrem Kontext erbrachten Arbeitsleistungen. Der Arbeitsprozess jener Anbieter*innen, die über Plattformen Zugang zum Markt finden, wird vielfach bis ins Detail mitstrukturiert. Dies gilt in ähnlicher Weise für ganz unterschiedliche Gruppen: Unabhängige Softwareproduzent*innen, die ihre Produkte über Googles

10 Siehe hierzu auch den Beitrag von Christian Stöcker.

11 Vgl. S. Zuboff: The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power.

oder Apples Appstores vertreiben wollen, müssen sich bei der Form der Leistungserbringung an klar definierte und einseitig festgelegte Regeln und Vergütungen halten. Gleiches gilt für Dritthändler*innen auf E-Commerce-Plattformen wie Amazon, denen im Dienste einheitlicher Services kaum Spielraum bei der Spezifizierung der Leistungserbringung zugestanden wird (etwa bezüglich der Zeit und Stückzahl, in der Produkte an Amazons Warenlager zu liefern sind). Am deutlichsten wird die Leistungssteuerung durch marktgleiche Plattformen freilich im Kontext von Arbeitskraftplattformen: Mit den App-basierten Instrumenten des algorithmischen Managements, die zur Administration, Steuerung und Kontrolle der dort Arbeitenden genutzt werden, akquirieren Plattformen Leistungsdaten der Dienstleister*innen und nutzen diese, um die jeweiligen Kontroll- und Steuerungsstrategien kontinuierlich zu verfeinern. So kann die Taxi-Plattform Uber beispielsweise nur solchen Fahrer*innen Aufträge zuweisen, deren Profile sie als besonders zuverlässig ausweisen, und Fahrer*innen, die öfter Zuweisungen abgelehnt haben oder anderweitig negativ aufgefallen sind, Aufträge versagen. Auf diese Weise wird über den Zugang zu Aufträgen und damit zu Arbeit ein regelkonformes Verhalten der Plattformarbeiter*innen eingefordert.

Verwoben mit der Kontrolle von Plattformarbeiter*innen sind auch spezifische plattformeigene Instrumente der Preiskontrolle: Ubers »Blitz Pricing«-Modell beispielsweise verspricht höhere Entlohnung für Fahrer*innen, die sich zu einem bestimmten Zeitpunkt in besonders nachgefragte Gebiete bewegen. Folgen viele Fahrer*innen diesem Anreiz, entsteht ein Überangebot an Arbeitskraft am betreffenden Ort, das es möglich macht, die Preise pro Fahrt und damit den Lohn der Fahrer*innen sogleich wieder zu senken. Auch (scheinbar) widerständiges Handeln, das sich diesen Strategien zu entziehen versucht, wird von den Instrumenten des algorithmischen Managements weitgehend erfasst und folglich bewertbar und kontrollierbar gemacht.

Unter dem Strich stellen proprietäre Märkte ein neues Modell der Arbeitsorganisation dar, das Vorteile für Konsument*innen auf Basis einer verstärkten Ausbeutung von Arbeitenden ins Werk setzt – zum einen durch das Abschöpfen von Profiten durch die Besteuerung von Marktzugängen, zum anderen durch die Intensivierung von Ausbeutung durch Instrumente des algorithmischen Managements.

2 Normative Rekonstruktion der Plattformökonomie: Das Recht der sozialen Freiheit

Wie lässt sich nun eine konkrete Kritik dieser neuen unternehmerischen Praxis der Plattformen formulieren, die über Spontanevidenzen wie der Ablehnung ausbeuterischer Geschäftsmodelle hinausgeht? Was wären ihre Kernaussagen und wie lässt sich diese kritische Reflektion konstruktiv wenden? Wir werden im Folgenden aufbauend auf Axel Honneths Theorie der Rechte[12] eine Antwort auf diese Fragen erarbeiten. Honneth folgend hat die Kritik einer historisch *konkreten* Gesellschaft ihren Ausgangspunkt in den jeweils dominanten normativen Orientierungen zu nehmen, das heißt in den zentralen Wertvorstellungen, die sich in die maßgeblichen Institutionen der jeweiligen Gesellschaftsformation eingeschrieben haben.

Doch welcher Maßstab kann zur Kritik normativer Ordnungen digitaler Plattformen angelegt werden? Für Honneth besteht kein Zweifel, dass unter »all den ethischen Werten, die in der modernen Gesellschaft zur Herrschaft gelangt sind und seither um Vormachtstellung konkurrieren, […] nur ein einziger dazu angetan [war], deren institutionelle Ordnung auch tatsächlich nachhaltig zu prägen: die Freiheit im Sinne der Autonomie des Einzelnen«[13]. Der Begriff der Freiheit kennt freilich unterschiedliche Spezifizierungen, die »sich im moralischen Diskurs der Moderne, jenen erbittert geführten Konflikten um die Bedeutung von Freiheit, […] herausgebildet haben«[14]. So sieht Honneth, im Gegensatz zum eindimensionalen Freiheitsverständnis des Liberalismus, wie es beispielsweise in der Gerechtigkeitstheorie von John Rawls zum Ausdruck kommt, individuelle Freiheit nur dann verwirklicht, wenn sie in drei Sphären der modernen Gesellschaft – Recht, Moral und den sozialen Institutionen – umgesetzt ist. Dementsprechend unterteilt er drei Formen von Freiheit: (1) negative, (2) reflexive und (3) soziale Freiheit.

(1) »Negative Freiheit« sei zunächst schlicht als »Fehlen von Widerstand«[15] zu verstehen, also als Möglichkeit, den eigenen Willen nach persönlichem Gutdünken durchzusetzen. Sie bildet den Fluchtpunkt der berühmten Theori-

12 Honneth, Axel: Das Recht der Freiheit. Grundriss einer demokratischen Sittlichkeit, Berlin: Suhrkamp 2011.
13 Ebd., S. 35.
14 Ebd., S. 42.
15 Ebd., S. 44.

en des Gesellschaftsvertrages, etwa von Hobbes,[16] die die staatliche Gewährleistung von Sicherheit als Bedingung für autonomes Handeln konzipieren, das sich nur durch diese ohne Gefahr für Leib und Leben (also Widerstand) durch andere Individuen entfalten kann.

(2) Nicht thematisiert wird bei einem solchen Freiheitsbegriff die Fähigkeit der Subjekte, sich im Rahmen »reflexiver Freiheit« selbst eigene Zwecke zu setzen. Dieser zweite, moderne Begriff der Freiheit in der Tradition Kants ermögliche erst den Begriff der Selbstbestimmung, der als Voraussetzung der negativen Freiheit betrachtet werden kann. Nur wenn Individuen in der Lage sind, die Ziele, die sie verfolgen, im Prinzip selbst und frei zu wählen, können sie frei von Heteronomie sein.

(3) Die »soziale Freiheit« bezieht sich schließlich auf die Lebenswirklichkeit der Menschen in sozialen Institutionen (etwa der Ehe, in Freundschaftsbeziehungen, am Arbeitsplatz oder in freiwilligen Assoziationen), Organisationen und gesellschaftlichen Infrastrukturen, die ihre individuellen Handlungen ermöglichen und einschränken. Im Unterschied zur negativen und reflexiven Freiheit, die im Diskurs der Moderne in letzter Instanz nur abstrakte, absolute Werte und auf das Individuum bezogene Kategorien thematisieren, adressiert die soziale Freiheit damit die konkreten sozialen Vollzugsbedingungen von Freiheit. Dabei werden Institutionen als kollektive Handlungspraktiken verstanden, die nur dann freiheitlich sein können, wenn sie Individuen die Möglichkeit geben, sich gegenseitig in ihrer Andersheit anzuerkennen und einander in der Realisierung ihrer Freiheit zu unterstützen. Hier werden also die historisch konkreten Verwirklichungschancen von Freiheit zum Thema. Soziale Freiheit bildet folglich den Lackmustest einer gerechten Gesellschaft: Die Frage ist nicht mehr, worauf sich das Individuum gründet, sondern ob es in einer Zeit lebt, die halten kann, was sie verspricht, weil ihre zentralen Institutionen die Entfaltung von Freiheit ermöglichen. »Es ist eine solche institutionelle Erweiterung des Freiheitsbegriffs,« so Honneth, »die dem dritten *sozialen* Begriff der Freiheit als Richtschnur dient; nach dieser Vorstellung lässt sich die Idee der reflexiven Freiheit nicht entfalten, ohne dabei die institutionellen Formen einzubeziehen, die ihren Vollzug ermöglichen.«[17]

16 Hobbes, Thomas: Leviathan. Or the Matter, Forme, and Power of a Commonwealth Ecclesiasticall and Civill, New Haven, Connecticut: Yale University Press 2010 [1651].

17 A. Honneth: Das Recht der Freiheit. Grundriss einer demokratischen Sittlichkeit, S. 80.

Soziale Freiheit in der plattformvermittelten Realität

Die Anwendung eines solchen sozialen Verständnisses von Freiheit auf das Phänomen digitaler Plattformen ist naheliegend, da sie als Infrastrukturen der digitalen Gesellschaft den soziotechnischen Rahmen bilden, innerhalb dessen sich menschliches Zusammenleben derzeit neu formiert. Im Zuge der normativen Rekonstruktion dieses Prozesses ist jedoch zunächst die Frage zu beantworten, inwiefern Plattformen als digitale Märkte überhaupt zur Verwirklichung sozialer Freiheit beitragen *können*. Schließlich dominiert bis heute ein modernes Marktverständnis, das die Moralität von Märkten grundsätzlich bestreitet und sie in der Tradition Adam Smiths auf die Durchsetzung negativer Freiheiten reduziert.

Doch die Annahme der Amoralität von Märkten ist gleich in zweifacher Hinsicht ein Trugschluss: Einerseits zeigen wirtschaftssoziologische Ansätze, dass es gerade die normativen Grundlagen kollektiver ökonomischer Praktiken sind, die das Funktionieren des Marktes, das heißt die routinierten Interaktionen der Marktteilnehmer*innen, überhaupt erst ermöglichen.[18] Andererseits übersehen die Verfechter*innen des vermeintlich amoralischen beziehungsweise wertfreien Marktes, dass dieser nicht nur vom Konkurrenzprinzip, sondern ebenso von Inseln der Kooperation durchdrungen ist. So ist die unternehmerische Organisation von Arbeit ein konstitutives Element von Märkten und zugleich einer der bedeutendsten Einflussfaktoren auf die (Nicht-)Verwirklichung sozialer Freiheit. Wenngleich diese nach Auffassung Honneths in der Marktsphäre besonders schwach ausgeprägt ist, machen doch gerade das zwischenmenschliche Verhältnis von Kolleg*innen oder hierarchiearme Genossenschaftsmodelle deutlich, dass auch im Markt soziale Freiheit möglich ist. Honneth zufolge reicht es nicht aus, die Sphäre des Marktes lediglich von außen rechtlich einzubetten. Es sei vielmehr notwendig, das moralische Anliegen gegenseitiger Anerkennung in die ökonomischen Handlungslogiken selbst einzuschreiben, damit Individuen als Marktteilnehmer*innen »durch die reziproke Anerkennung ihrer Abhängigkeit voneinander zur Erfüllung ihrer Zwecke gelangen [können]«[19]. So leitet Honneth aus der grundlegenden Möglichkeit sozialer Freiheit im Markt die

18 Vgl. Beckert, Jens: »Die soziale Ordnung von Märkten«, in: Jens Beckert/Rainer Diaz-Bone/Heiner Ganßmann (Hg.), Märkte als soziale Strukturen, Frankfurt a.M.: Campus 2007, S. 43-62.

19 A. Honneth: Das Recht der Freiheit. Grundriss einer demokratischen Sittlichkeit, S. 88.

moralische Pflicht ab, »dass die für den Markt konstitutive Erlaubnis zu rein individuellen Nutzenorientierungen die normative Bedingung erfüllen können muss, von den Beteiligten als geeignetes Mittel zur komplementären Verwirklichung ihrer je eigenen Zwecke verstanden werden zu können«[20].

Mit Blick auf die Kontrollformen digitaler Plattformen drängt sich nun systematisch der Eindruck auf, dass die Expansion proprietärer Märkte die Vollzugsbedingung für soziale Freiheit weiter einschränkt. Gerade das »ihre ganze Legitimität ausmachende Versprechen, durch Tauschprozesse zu einer komplementären Ergänzung individueller Handlungsabsichten beizutragen«[21], stellen Märkte in ihrer proprietär vermachteten Form grundsätzlich infrage. So erscheinen Plattformen als eine disruptive Technologie, die zunächst mittels Informations- und Zugangskontrolle die direkte Kooperation zwischen Marktteilnehmer*innen unterbricht und anschließend unter hierarchisch vorgegebenen Bedingungen neu ermöglicht. Nehmen wir das Beispiel der Dienstleistungsplattformen wie Uber (Fahrdienstleister), Helpling (haushaltsnahe Dienstleistungen) oder TakeAway (Essenslieferung): Sie schaffen neue Erwerbsoptionen für Menschen, die – beispielsweise aufgrund eines fehlenden Aufenthaltstitels, mangels formalisierter Qualifikationsnachweise oder zerstückelter Arbeitszeiten aufgrund von weiteren (Arbeits-)Verpflichtungen – auf Offline-Arbeitsmärkten benachteiligt werden. Dieser vermeintlich teilhabefördernde Charakter der Plattformen wird jedoch hinfällig, sobald die Arbeitsbedingungen in den Blick genommen werden. Die Bezahlung ist häufig so niedrig, dass abzüglich der Kosten für Arbeitsmaterialien und Versicherungen der Mindestlohn nicht eingehalten wird. Dies ist möglich, weil Plattformarbeiter*innen rechtlich gesehen meist als Soloselbstständige behandelt werden, die im Vergleich zu abhängig Beschäftigten mehrere entscheidende Nachteile haben: Die seit dem 19. Jahrhundert erkämpften Arbeitsrechte und insbesondere das Recht auf Koalitionsfreiheit, Kollektivverhandlungen und betriebliche Mitbestimmung gelten für sie nicht. Als »Kontingenzarbeitskräfte«[22] haben solche Plattformarbeiter*innen folglich keine ausreichende Verhandlungsmacht, um ihre Interessen gegenüber dem Plattformbetreiber geltend zu machen. Vielmehr kann ihre formale Soloselbstständigkeit sogar als rechtlicher Vorwand missbraucht werden, um einen Zusammenschluss der Arbeiter*innen mit Verweis auf das Verbot von Kartell-

20 Ebd., S. 348.
21 Ebd.
22 O. Nachtwey/P. Staab: Die Avantgarde Des Digitalen Kapitalismus.

absprachen zu verhindern. Mit dem Soziologen Albert O. Hirschmann gesprochen bleibt den Plattformarbeiter*innen im Falle eines zu hohen Leidensdrucks keine »Voice«-Strategie, sie können sich nicht wehren, und selbst eine »Exit«-Strategie, der Wechsel auf andere Plattformen, ist aufgrund der stark konzentrierten Plattform-Märkte und der umfangreichen Anbieter-Lock-in-Effekte oft keine reale Handlungsoption. So bleibt als letzte Möglichkeit nur »Loyalty« gegenüber dem Plattformunternehmen, das heißt eine bedingungslose Unterwerfung unter Verzicht auf wesentliche Grundfreiheiten.[23]

Zudem institutionalisiert das Modell proprietärer Märkte einseitige Verfügungsrechte bei den Marktbesitzern auf Kosten der Marktteilnehmer*innen. Durch das einseitige Setzen der Regeln, die eine Marktpartizipation erlauben (Zugangs-, Preis- und Leistungskontrolle), können Plattformen hohe Provisionen von den Marktanbietern verlangen und große Teile des erwirtschafteten Mehrwerts abschöpfen. Das Beispiel Amazon zeigt, wie Plattformen mit zunehmendem Marktanteil die Abgaben der Marktteilnehmer*innen sukzessive erhöhen können. Auch kleine und mittlere Unternehmen werden auf diese Weise zu »Usern« degradiert und einem Zwang zur Konformität unterworfen. Der Zugang zur Plattform erfordert meist eine widerspruchslose Unterordnung unter eine intransparente algorithmische Plattform-Architektur, die den Handlungsspielraum der Unternehmen standardisiert und die Durchführung von Arbeitsschritten nur in einer – nämlich der vorgeschriebenen – Weise zulässt. Im Vergleich zu Offline-Märkten ist die soziale Freiheit hier deutlich reduziert, weil die Normen des Wettbewerbs nicht mehr aus einer kollektiven Praxis erwachsen, sondern von den Plattformbetreibern im eigenen Interesse hierarchisch in die Softwarelogik des digitalen Marktes eingeschrieben werden. Diese Privatisierung der Gestaltung essenzieller ökonomischer Institutionen blockiert individuelle Partizipation an der Regelsetzung – im Bereich der Arbeit etwa in Form verbürgter Mitbestimmungsrechte. Folglich stehen proprietäre Plattformen in ihrer aktuellen, gewinnorientierten Form der Institutionalisierung von sozialer Freiheit in der Sphäre des Marktes entgegen.

23 Hirschman, Albert O.: Exit, Voice and Loyalty. Responses to Decline in Firms, Organizations, and States, Cambridge, Massachusetts: Harvard University Press 1970.

3 Eine gemeinwohlorientierte Plattformökonomie

Wie könnte nun ein Modell digitaler Plattformen aussehen, das im Sinne einer gerechten Gesellschaft Marktformen institutionalisiert, die sozialer Freiheit Vorschub leisten? Im Folgenden schlagen wir drei Governance-Prinzipien für eine gemeinwohlorientierte Plattformökonomie mit würdevollen Arbeitsbedingungen vor: Öffentlichkeit, Mitbestimmung und Datensouveränität.

3.1 Öffentlichkeit

Damit Menschen überhaupt frei urteilen und handeln können, müssen sie in der Lage sein, die sie umgebenden Strukturen und die darin eingeschriebenen Logiken zu erkennen. Dabei ist der Zugang zu Informationen entscheidend. Gerade Plattformarbeiter*innen benötigen zur Durchsetzung ihrer Rechte ausreichend Wissen über die Funktionsweise der Plattform-Softwareumgebung, um daran Kritik üben und notfalls Widerstand gegen diskriminierende oder ausbeuterische Praktiken leisten zu können. Die in der Plattformökonomie etablierte Wissensasymmetrie – Plattformkonzerne wissen alles über Arbeiter*innen, während Arbeiter*innen kaum etwas über die Plattformkonzerne wissen – muss durchbrochen werden. Das Prinzip der Öffentlichkeit wird auf diese Weise zu einem Grundbaustein gemeinwohlorientierter Plattformentwicklung, das verhindert, dass Plattformen gegenüber den Bürger*innen und Arbeiter*innen eine intransparente Fremdherrschaft herausbilden. In diesem Sinne empfehlen sich drei Wege zu mehr Plattform-Öffentlichkeit:

(1) Algorithmische Transparenz: Ein wichtiger Schutzmechanismus gegen Fehlverhalten sind strenge Transparenzanforderungen an die Plattformbetreiber. So sollten Plattformunternehmen dazu verpflichtet werden, die Funktionsweise und Kriterien der Bewertungs- und Sortieralgorithmen nachvollziehbar darzulegen und die dabei verwendeten personenbezogenen Daten anzugeben. Auf diese Weise können unabhängige Kontrollinstitutionen und Wissenschaftler*innen potenzielle Gefahren, wie algorithmische Diskriminierung, frühzeitig erkennen und Nutzer*innen bei der Ausübung ihres Grundrechts auf informationelle Selbstbestimmung unterstützen. Insbesondere intelligente Algorithmen, die nicht nur Regeln befolgen, sondern sich weiterentwickeln und neue Regeln schaffen, sollten in einer Datenbank öffentlich zugänglich sein, sodass

die formalisierten Parameter und deren Gewichtung für die automatisierte Entscheidungsfindung verständlich werden. Vor allem im Kontext des Arbeitsschutzes erfordert die Ausübung der informationellen Selbstbestimmung darüber hinaus ein Recht auf individuelle Anpassung der entscheidenden Algorithmen-Parameter, damit Plattformarbeiter*innen die Kontrolle über die Erfassung und Verarbeitung ihrer Daten behalten.

(2) Open Source: Eine weitere Maßnahme für Öffentlichkeit in der Plattformökonomie ist das Publikmachen des Softwarecodes der Plattformen unter einer Open-Source-Lizenz, wie es die Free- und die Open-Source-Bewegung seit Beginn des Software-Zeitalters einfordern. Auf diese Weise kann der Code auch von externen Expert*innen eingesehen und kontrolliert werden, um die Gewährleistung von Privatsphäre, Sicherheit, Arbeits-, Verbraucherschutz- und Wettbewerbsrecht zu kontrollieren. Während Privatunternehmen ihre Software meist als geistiges Eigentum betrachten, könnten beispielsweise öffentliche Akteure mit gutem Beispiel vorangehen und die Entwicklung von Open-Source-Plattformen unterstützen, indem sie ihre eigene Software unter einer offenen Lizenz veröffentlichen und die von ihnen beauftragten Dienstleister ebenfalls dazu veranlassen. Darüber hinaus wäre eine Pflicht zur Offenlegung des Plattform-Codes bei unabhängigen Zertifizierungsstellen im Rahmen von Plattform-Audits denkbar, um auch dann sichere und würdevolle Arbeitsbedingungen auf Plattformen zu garantieren, wenn Plattformbetreiber ihren Code aus Wettbewerbsgründen nicht frei verfügbar machen wollen.

(3) Interoperabilität: Eine besonders weitreichende Forderung ist die Pflicht für Plattformbetreiber, ihre Datenschnittstellen zu öffnen. Dazu stellt der Plattformbetreiber ein Application Programming Interface (API) bereit, mit dem Plattformnutzer*innen über externe Dienste auf die Daten der Plattform zugreifen und sich mit anderen Plattformnutzer*innen austauschen können. Dazu muss ein gemeinsamer Kommunikationsstandard entwickelt und implementiert werden, der das problemlose Zusammenwirken, das heißt Interoperabilität zwischen Plattformen und Zugangsdiensten, sicherstellt.[24] Im Mobilfunkbereich ist es beispielsweise selbstverständliche Praxis, dass ein Telekom-Kunde mit einer Vodafone-Kundin kommunizieren kann. Während die Plattformen in diesem System nach

24 Vgl. Piétron, Dominik: »Digitale Souveränität durch Interoperabilität. Zur Möglichkeit dezentraler sozialer Netzwerke in der Plattformökonomie«, in: WISO Direkt 24 (2019).

wie vor Dreh- und Angelpunkt der Datenflüsse sind, erhalten Plattformnutzer*innen die Möglichkeit, den Zugang zur Plattform selbst zu gestalten. Dabei könnten sie eigene Software-Architekturen entwickeln, die ihre Interessen widerspiegeln und beispielsweise keine Datenerfassung zu Überwachungszwecken erlauben. Eine solche Regelung ergibt nur Sinn, wenn Plattformen gleichzeitig zur Neutralität verpflichtet werden und Nutzer*innen anderer Zugangsdienste nicht benachteiligen dürfen. Zudem müssen für diesen Zweck branchenbezogene Standardisierungsprozesse unter Einbezug aller Stakeholder organisiert werden, die sich auf ein gemeinsames Kommunikationsprotokoll für die essenziellen Datenflüsse einigen.

3.2 Mitbestimmung

So wie die Macht der Industriekapitalisten über die Arbeiterschaft in ihrem Eigentum an Produktionsmitteln gründete, so basiert die Macht der Plattformunternehmen über die Händler*innen und Dienstleister*innen auf dem Eigentum an Distributionsmitteln, das heißt dem Zugang zu den Konsument*innen. Um sich wirksam gegen Missbrauch durch übermächtige Unternehmen zu schützen, müssen Arbeiter*innen damals wie heute auf einer abgesicherten rechtlichen Basis kollektiv ihre Interessen geltend machen können. Idealerweise passiert dies in einem deliberativen Prozess, in dem alle Beteiligten angehört werden, um so ein maximales Maß an Freiheit für alle zu ermöglichen.

Doch selbst die Minimalvoraussetzung für einen solchen Prozess – die Anerkennung von Plattformnutzer*innen als berechtigte Stakeholder – ist in der Plattformökonomie nicht gegeben. Deshalb müssen zunächst die in den Kämpfen der Arbeiterbewegung errungenen Grundrechte auf Koalitionsfreiheit, Kollektivverhandlungen und betriebliche Mitbestimmung ins digitale Zeitalter übertragen werden. Nur wenn Plattformarbeiter*innen auf diese Weise eine kollektive Verhandlungsmacht entwickeln und über die Rahmenbedingungen ihrer Arbeitserbringung mitentscheiden können, kann soziale Freiheit im Sinne Honneths überhaupt verwirklicht werden. Das trifft auch auf die Gruppe der Konsument*innen auf Plattformen zu, die in ihren alltäglichen Handlungen von essenziellen Plattformunternehmen mit Infrastruktur-Charakter abhängig geworden sind. Das Prinzip der demokratischen Teilhabe beziehungsweise der Mitbestimmung an der Ausgestaltung von Plattformen wird damit zu einem zweiten entscheidenden Kriterium für

gemeinwohlorientierte Plattformentwicklung. Um dies zu erreichen, bieten sich wiederum drei Optionen an:

(1) Rechte von Plattformarbeiter*innen stärken: Zunächst sollte das geltende Verbot von Schein-Selbstständigkeit in der Plattformwirtschaft besser durchgesetzt werden. Viele Plattformarbeiter*innen werden zu Unrecht als Soloselbstständige behandelt, obwohl sie den Großteil ihres Einkommens über eine Plattform verdienen und dieser gegenüber weisungsgebunden sind.[25] Regulatoren sind damit aufgerufen, die weitreichende Abhängigkeit von Plattformarbeiter*innen anzuerkennen und Plattformbetreiber in die Pflicht zu nehmen. Letztere sollen ihrer sozialen Verantwortung nachkommen und sich – wie alle anderen Arbeitgeber – paritätisch an der sozialen Absicherung der Arbeiter*innen beteiligen. Zudem bedarf es einer neuen rechtlichen Grundlage für Plattformarbeiter*innen, damit diese auch als Soloselbstständige ihre Grundrechte auf Koalitionsfreiheit und Kollektivverhandlungen wahrnehmen können.
(2) Institutionelle Beteiligungsverfahren: Gerade digitale Plattformen erlauben eine Fülle von digitalen Werkzeugen, die in den letzten Jahren speziell zu dem Zweck entwickelt wurden, partizipative Governance im großen Maßstab zu ermöglichen. Digitale Werkzeuge könnten die Kosten der Teilhabe an Entscheidungsfindungsprozessen erheblich senken, indem sie beispielsweise asynchrone Abstimmungen und Diskussionen von zu Hause aus erlauben. Auf Basis dieser Werkzeuge sollten Plattformbetreiber dazu verpflichtet werden, grundlegende Mitspracherechte für Arbeiter*innen und Nutzer*innen zu institutionalisieren. Dazu bedarf es Mechanismen zur kollektiven Bewertung und Überwachung der Plattformen, über die Plattformarbeiter*innen an wesentlichen Entscheidungen der Plattformentwicklung beteiligt werden und Beschwerden einreichen können. Darüber hinaus sind leicht zugängliche Streitbeilegungsmechanismen mit unabhängigen Schiedsgerichten nötig, die Datenzugang beantragen und Rechtsmittel einlegen können.
(3) Genossenschaften: Das vergleichsweise günstige Errichten eines Online-Vertriebskanals für eine Gruppe von Händler*innen oder

25 Vgl. Schneider-Dörr, Andreja: Erwerbsarbeit in der Plattformökonomie. Eine kritische Einordnung von Umfang, Schutzbedürftigkeit und arbeitsrechtlichen Herausforderungen, Working Paper Forschungsförderung, No. 116, Düsseldorf: Hans-Böckler-Stiftung 2019.

Dienstleister*innen hat weltweit zur Verbreitung von Plattform-Genossenschaften[26] geführt, die sich vollständig im Besitz ihrer Mitarbeiter*innen befinden.[27] Als Mitglieder einer Genossenschaft haben Arbeiter*innen größere Kontrolle über ihre Arbeitsbedingungen und sind stärker an den erarbeiteten Gewinnen beteiligt. Entscheidungen werden kollektiv getroffen, wobei jedes Genossenschaftsmitglied über eine Stimme verfügt. Regierungen können Plattform-Genossenschaften fördern, indem sie die rechtlichen Einstiegshürden für Genossenschaften im digitalen Raum senken, Gründungsberatungen speziell für Kooperativen anbieten und gezielt Open-Source-Software fördern, die das Aufsetzen von digitalen Vertriebskanälen in verschiedenen Branchen ermöglicht. Auf diese Weise erhalten Plattformarbeiter*innen eine realistische Chance, alternative Plattformmodelle zu etablieren und insbesondere lokale Netzwerkeffekte auszunutzen.

3.3 Datensouveränität

Die Macht von Plattformen basiert unter anderem auf der massenhaften Aneignung personenbezogener Daten, aus denen Vorhersagen über das Verhalten ihrer Arbeiter*innen und Nutzer*innen abgeleitet werden. Auf diese Weise können große Menschengruppen manipuliert und dieser Einfluss an Dritte verkauft werden. Das zugrunde liegende datenschutztechnische Laissez-Faire-Modell verletzt nicht nur das Recht auf informationelle Selbstbestimmung und damit die Würde von Plattformarbeiter*innen, es schränkt auch die Autonomie der Individuen ein, persönliche Entscheidungen entlang der eigenen Wertmaßstäbe zu treffen. Wenn Plattformbetreiber exklusiven Zugriff auf die Daten ihrer Arbeiter*innen haben, lässt sich diese Informationsmacht zudem in eine ökonomische Macht umwandeln, mit der die Leistungsanforderungen und Umsatzbeteiligungen erhöht oder besonders profitable Produkte identifiziert werden können.

Dagegen lässt sich das Prinzip der Datensouveränität in Stellung bringen, das auf dem Recht auf informationelle Selbstbestimmung aufbaut und

26 Vgl. Scholz, Trebor: Platform Cooperativism. Challenging the Corporate Sharing Economy, Rosa-Luxemburg-Stiftung (Hg.), New York 2016.

27 Vgl. Pentzien, Jonas: The Politics of Platform Cooperativism. Political and Legislative Drivers and Obstacles for Platform Co-ops in the U.S.A., Germany, and France, ICDE Report 05: ICDE 2020.

neue Institutionen zu deren Durchsetzung einfordert. Datensouveränität ergänzt das individualistische Datenschutzrecht, indem es den kollektiven beziehungsweise relationalen Charakter personenbezogener Daten anerkennt, die immer auch Rückschlüsse auf bestimmte Gruppen zulassen.[28] Zur Entscheidung über die Verwendung von personenbezogenen Daten in der Plattformökonomie sind also demokratische Verfahren notwendig, die den unkontrollierten Datenzugriff seitens der Privatwirtschaft ebenso wie staatlicher Institutionen einschränken. Ohne ein transparentes System von *Checks and Balances* kann die umfassende Quantifizierung der Gesellschaft schnell in eine technokratische Fremdsteuerung umkippen, in der bürgerliche Freiheitsrechte flächendeckend außer Kraft gesetzt sind.

Um dem entgegenzuwirken, hat sich in den letzten Jahren insbesondere das Konzept der sogenannten Datengenossenschaften beziehungsweise Datentreuhänder[29] herauskristallisiert, die im Auftrag ihrer Mitglieder sämtliche Daten sicher speichern und nur für klar definierte Zwecke zur Verfügung stellen. Datengenossenschaften fungieren als unabhängige Datenverwalter, die die Kontrolle über die Erhebung, Auswertung und Nutzung personenbezogener Daten kollektivieren. Dabei wird nach dem Prinzip der Gewaltenteilung eine funktionale Trennung zwischen Datenverwaltung und Datennutzung vorgenommen und auf diese Weise ein verlässliches demokratisches Fundament für datenbasierte Geschäftsmodelle geschaffen. So können Datengenossenschaften einen lebendigen partizipativ-demokratischen Willensbildungsprozess etablieren, der um die zentrale Frage im digitalen Kapitalismus kreist: Welche gesellschaftlichen Daten sollen von wem gesammelt und für welche Zwecke genutzt werden?

Konkret könnte dies wie folgt aussehen: Die Datengenossenschaft wird als eigene Rechtspersönlichkeit in Form eines Vereins oder einer Genossenschaft für eine bestimmte Plattform oder eine Gruppe von Plattformen gegründet.

---

28 Immer wenn eine Person Daten über sich preisgibt, können daraus Rückschlüsse auf Menschen mit ähnlichen sozioökonomischen Merkmalen oder Vorlieben gezogen werden, die sich gegen eine entsprechende Einordnung jedoch nicht wehren können.

29 Europäische Kommission: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz) 2020/0340 (COD), Brüssel: Europäische Kommission 2020, S. 35ff.; Delacroix, Sylvie/Lawrence; Neil D.: »Bottom-up Data Trusts. Disturbing the ›One Size Fits All‹ Approach to Data Governance«, in: International Data Privacy Law 9(4) (2019), S. 236-252; Singh, Parminder Jeet/Vipra, Jai: »Economic Rights Over Data. A Framework for Community Data Ownership«, in: Development 62(1-4) (2019), S. 53-57.

Die Nutzer*innen dieser Plattformen erteilen der Datengenossenschaft eine treuhänderische Vollmacht, ihre personenbezogenen Daten unter klar definierten Bedingungen für ausgewählte Zwecke zur Verfügung zu stellen. In regelmäßigen Sitzungen können alle Mitglieder demokratisch über die Leitlinien zur Datennutzung und einzelne Nutzungsanfragen abstimmen. Wollen öffentliche Akteure, NGOs, Wissenschaft, Presse oder Unternehmen die Daten verwenden, stellen sie einen Antrag, über den die Datengenossenschaft auf Grundlage der beschlossenen Leitlinien entscheidet.

Insbesondere öffentliche Plattformen,[30] die von kommunalen oder staatlichen Stellen betrieben werden, könnten das Modell der Datengenossenschaften schon heute konkret werden lassen, indem sie die Vertretung von individuellen Datenrechten durch unabhängige Datenverwalter anerkennen und die technische Infrastruktur für Datengenossenschaften bereitstellen. Technisch gesehen könnten personenbezogene Nutzerdaten in diesem Fall auf den Servern der Plattformbetreiber verbleiben und über eine Datenschnittstelle ausgewählten Dritten zur Verfügung gestellt werden. Die Datenanalyse beziehungsweise das Training von Algorithmen könnte dabei auch über ein Remote-Access-Modell durch die Datengenossenschaften selbst erfolgen, sodass die Rohdaten geschützt bleiben.

Aktuell sind Datengenossenschaften ein Nischenphänomen, das nur vereinzelt und ohne reale Verhandlungsmacht gegenüber Plattformbetreibern getestet wird, wenngleich auf europäischer Ebene erste rechtliche Schritte in diese Richtung gegangen werden. Dabei sollten auch die rechtlichen Unsicherheiten bei der Übertragung individueller Datenschutzrechte auf Datengenossenschaften dringend behoben werden, um das Prinzip der Datensouveränität als soziales Freiheitsrecht zu verankern. Datengenossenschaften könnten auf diese Weise insbesondere auch für Plattformarbeiter*innen ein institutionelles Gerüst zur kollektiven Verwaltung ihrer Daten bereitstellen, das vor Datenmissbrauch, algorithmischer Diskriminierung und Verstößen gegen die Privatsphäre von Gigworkern und Online-Händler*innen schützt und ein würdevolles Arbeiten auf Plattformen ermöglicht.

30 Vgl. Piétron, Dominik: »Öffentliche Plattformen und Datengenossenschaften. Zur Vergesellschaftung digitaler Infrastrukturen«, in: Timo Daum /Sabine Nuss (Hg.): Die unsichtbare Hand des Plans, Berlin: Dietz Verlag 2021 (i.E.).

4 Fazit: Technologieentwicklung als freiheitliche Praxis

In der Plattformökonomie gilt es heute, die Idee der Freiheit und Würde mit neuem Inhalt zu füllen. Dazu braucht es eine erweiterte Perspektive auf zentrale digitale Intermediäre, in der wir uns nicht darauf beschränken als Konsument*innen Großkonzerne zu kritisieren. Es müssen vielmehr neue Wege gefunden werden, auf denen wir als mündige Bürger*innen im digitalen Zeitalter die Kontrolle über unsere Leben zurückerlangen und vom bloßen Widerstand zur partizipativen Umgestaltung der digitalen Gesellschaft übergehen können.

Das Recht auf soziale Freiheit, wie es Honneth formuliert, kann dabei als Leitlinie herangezogen werden, um die Plattformökonomie normativ zu rekonstruieren. Dabei rücken die Arbeitsbedingungen der betroffenen Plattformarbeiter*innen in den Fokus, deren alltägliche Handlungsspielräume durch die Architektur der Plattformen besonders stark eingeschränkt werden. Einseitig gesetzte Zugangs-, Preis- und Leistungskontrollen sowie weitreichenden Verfügungsrechte der Betreiber der Plattformen erfordern eine bedingungslose Unterwerfung, die die wesentlichen Grundfreiheiten und die Würde der betroffenen Arbeiter*innen untergräbt. Mitbestimmung und Partizipation an der Regelsetzung von Plattformen werden damit zu konkreten Ansatzpunkten für die Verankerung sozialer Freiheit in digitalen Interaktionsräumen.

Der gesellschaftliche Druck für würdevolles Arbeiten in der Plattformökonomie und für einen sicheren und souveränen Umgang mit Digitaltechnik nimmt zu. Gewerkschaften, Datenschutzorganisationen und die digitale Zivilgesellschaft arbeiten an vielversprechenden Alternativen zum traditionell hierarchischen Plattform-Modell proprietärer Märkte. Die hier skizzierten drei Prinzipien gemeinwohlorientierter Plattformen sind insofern als institutionelle Grundlage für ein Erstarken kollektiver Macht zu verstehen, mit der sich Menschen die Plattformen, die sie tagtäglich zur Bewältigung ihres Alltags nutzen, zu eigen machen und sie an ihren individuellen Interessen ausrichten können. Es geht damit nicht nur um ein Primat des Rechts im Kontext neuer kapitalistischer Organisationsformen, sondern um eine Praxis der Freiheit, die allen offen stehen muss.

2.2 Gerechtigkeit und Gleichheit

2.2.1 Gerechtigkeit

Künstliche Intelligenz und Diskriminierung – Eine Archäologie

Lorena Jaume-Palasí

Künstliche Intelligenz (KI) ist eine Technologie, die für komplexe algorithmische Systeme steht. Als Begriff ist sie der akademischen Nische und der Belletristik entwichen und breitet sich im Alltag aus. Smartphones, Impfforschung, Programme für Personalmanagement, soziale Medien, Polizei und Banken verwenden einfache, aber mittlerweile auch komplexere algorithmische Systeme, die wir als KI bezeichnen. Diese Systeme automatisieren Prozesse. Die Prozesse sollen durch die Automatisierung versachlicht werden. Jedoch wird nahezu täglich in den Medien von Fehlern in algorithmischen Systemen berichtet. Vielfach ist von diskriminierenden Effekten die Rede.

Nicht selten heißt es in der öffentlichen Diskussion, dass die Effekte dieser Technologien dringend zu regulieren seien. In politischen Kreisen wird seit 2018 die Entwicklung von ethischen Kodizes und Gesetzesentwürfen gefordert. Denn europäische Gesetze werden als eine Art Gegenmittel zu Algorithmen gesehen. Dabei haben rechtliche und algorithmische Systeme im kontinentaleuropäischen Denken durchaus gemeinsame Ursprünge und Züge. Sie stellen keine Gegensätze dar. Sie formulieren vielmehr in unterschiedlicher Sprache eine bestimmte kulturelle Vorstellung des Systematisierens der Welt – und können somit gleichermaßen auch Diskriminierung erzeugen. Das Denken in Kategorien wie *gutes Recht* und *böse Algorithmen* ist daher bei der Suche nach angemessenen Lösungen nur selten hilfreich. Die europäische Rechtskultur wird ohne ein inneres Umdenken die Diskriminierungseffekte von algorithmischen Systemen nicht einhegen können.

Mit diesem Beitrag treten wir einen Schritt zurück und blicken kritisch auf die Leitgedanken und Theorien, die die heutige Wissenschaft und das Recht prägten, und fragen, welche Effekte sie in Bezug auf Diskriminierun-

gen haben. Anschließend wird beschrieben, wie diese Effekte sich in algorithmischem und in rechtlichem Denken widerspiegeln.

Diskriminierung passiert nicht einfach, sie wird konstruiert

Algorithmische Systeme müssen diskriminieren. Es ist ihre Aufgabe. Sie automatisieren Prozesse. Dafür werden mathematische Standards und Regeln benutzt. Daraus entstehen Kategorien, Korrelationen und somit auch mathematisch eingehegte Schubladen, die komplexe Sachverhalte in Prozessschritte unterteilen und so vereinfachen. Dieses Vorgehen ist einem mechanischen Denken inhärent. Damit ist nicht das Denken von Maschinen gemeint, sondern das menschliche Denken, das kulturgeschichtlich in Europa im Sinne einer mechanischen Methodik und Normativität trainiert ist und auch Eingang in unsere Rechtsordnung gefunden hat. Dies gilt insbesondere für Antidiskriminierungsgesetze. Will man die Diskriminierung durch algorithmische Entscheidungssysteme verstehen und durchbrechen, muss man sich die Frage stellen, inwieweit dies im Grundgerüst einer europäischen Rechtssystematik überhaupt möglich ist, die ebenfalls vom mechanischen Denken geprägt ist. Mit anderen Worten: Inwieweit sind Recht und algorithmische Systeme gleichermaßen in ihren Voreinstellungen gefangen?

Rationalität ist die Basis, auf der ein Großteil der westlichen Wissenschaft und Philosophie (sowie der sozialen und institutionellen Praktiken) fußt: von Naturwissenschaften über die Sozialwissenschaften bis hin zu den Kunst- und Geisteswissenschaften, einschließlich dem relativ jungen Gebiet der Technik- und Computerwissenschaften.

Das Verständnis von Rationalität im Mainstream der Philosophie der Neuzeit ist der Kern des mechanischen Denkens. Zwar gibt die aktuelle Debatte über künstliche Intelligenz (KI) der Silicon-Valley-Mentalität (oder auch der *Kalifornischen Schule*) die Schuld für Verzerrungen (Bias) und in der Folge für Diskriminierung. Grund sei ein Weltbild, das soziale Sachverhalte durch einen technischen Solutionismus, nach dem es für jedes (soziale) Problem eine technische Lösung geben muss, in ihrer Komplexität reduziert.[1] Doch ein genauerer Blick auf die europäische Philosophie beweist eine andere Herkunft dieses Weltbildes. Vielmehr muss die europäische

1 Vgl. Morozov, Evgeny: To Save Everything, Click Here – The Folly of Technological Solutionism, New York: PublicAffairs 2013.

Neuzeit mit dem kartesischen Rationalismus und dem mit ihm initiierten jahrhundertelangen Projekt des Delegierens der Rationalität an Maschinen[2] als Wiege des technischen Solutionismus angesehen werden. Tatsächlich ist das europäische rechtliche und politische Denken in der Logik des Mechanischen gefangen. Dieses methodologische Denken stellt eine relevante Herausforderung für normative Ansätze im Allgemeinen dar, insbesondere aber, wenn Diskriminierung in der KI überwunden werden soll.

Um Diskriminierung in algorithmischen Systemen zu verstehen, ist also nicht nur eine Analyse der Softwareprodukte notwendig, sondern auch der sozialen Ideologien und normativen Vorgaben der Gesellschaft, die solche Systeme einsetzt. Ethik und Recht geben Leitplanken bei der Nutzung von Technologien. Sie produzieren sowohl Bewertungsmaßstäbe und Einschränkungen, an denen die Verwendung von Technologien gemessen wird, als auch gesellschaftliche und wirtschaftliche Erwartungshaltungen und Verhaltensanreize.

Von den Ursprüngen des mechanischen Denkens

Das 17. Jahrhundert bricht mit der Philosophie des Mittelalters, das auf die Qualitäten in der Natur gerichtet war. Fortan prägte Mathematik die Programmatik der Philosophie. Erkenntnistheoretische und naturwissenschaftliche Theorien waren bestimmt von einer mathematischen Rationalisierung, die wiederum Grundlage für darauf aufbauende politische Theorien und Ethiken wurde.

Die Natur wurde zunehmend und allumfassend aus dem Blickwinkel der Mathematik betrachtet. Qualitäten wurden homogenisiert und quantifiziert.[3] Die Natur wurde als Zusammenwirken von kleinen Teilchen erklärt. Form, Größe und Bewegung wurden zu maßgebenden Kriterien, um die Natur zu beschreiben. So wurden Farben nicht mehr über Qualitäten dargestellt, sondern beispielsweise von René Descartes durch die verschiedenen Rotationsgeschwindigkeiten von Lichtteilchen.

2 Vgl. E Smith, Justin: Irrationality: A History of the Dark Side of Reason, Princeton: Princeton University Press 2019.

3 Vgl. J. Dijksterhuis, Eduard: Die Mechanisierung des Weltbildes, Berlin/Heidelberg: Springer-Verlag, 1956. Insbesondere S. 556f.

René Descartes[4] will das Wissen von veränderlichen und fehlbaren menschlichen Intuitionen und Emotionen befreien, stattdessen soll die Suche nach Erkenntnis von einer »objektiven« Vernunft geleitet sein. Es geht ihm darum, Strukturen unter den veränderlichen und schwankenden Phänomenen der Natur aufzudecken. Und diese Strukturen sollen zu den Fundamenten der Erkenntnis führen. Alles, was angezweifelt werden kann, wird ausgeschlossen. Folglich sind Diskussionen und das Verständnis von Begriffen wie Wissen und Ethik tendenziell abstrakt, befreit von Kontext, von Geschlecht oder Herkunft. »Wissen ist nach dieser Weltsicht im idealen, rationalen, statischen, in sich geschlossenen und autarken Subjekt verwurzelt, das als körperloser und desinteressierter Beobachter ›rein kognitiv‹ die Außenwelt aus der Ferne betrachtet.«[5]

Durch die Vereinigung der Mathematik mit der Maschinenlehre, insbesondere durch Galileo Galilei im 16. Jahrhundert, bedeutete die Mathematisierung der Natur zugleich die Mechanisierung der Natur. Experimente, Beobachtung, quantitative Messung und Analyse des Beobachteten basierten auf Mathematik. Galilei forderte, dass diese Methodik Vorrang gegenüber den bisherigen philosophischen Erkenntnismethoden habe, um die Natur und das, was der Mensch erfahren kann, zu erklären.

Francis Bacon systematisiert wissenschaftstheoretisch diese Sicht auf die Natur und überträgt diese Methode in seinen Schriften *Novum Organon* (1620) und *Nova Atlantis* (1624) auf die Wissenschaft im Allgemeinen. Dabei strukturiert Francis Bacon Wissen in eine deutlich patriarchale Richtung, wie Horkheimer und Adorno bemerken:

> »Die glückliche Ehe zwischen dem menschlichen Verstand und der Natur der Dinge, die er [Bacon, Anm. d. Verf.] im Sinne hat, ist patriarchal: der Verstand, der den Aberglauben besiegt, soll über die entzauberte Natur gebieten. Das Wissen, das Macht ist, kennt keine Schranken, weder in der Versklavung der Kreatur noch in der Willfährigkeit gegen die Herren der Welt.«[6]

4 Descartes, René: The Philosophical Writings of Descartes, Vol. 2, Cambridge: Cambridge University Press 1984.

5 Eigene Übersetzung. Birhane, Abeba: Algorithmic injustice: a relational ethics approach, Patterns, Volume 2, Issue 2, 2021. https://www.sciencedirect.com/science/article/pii/S2666389921000155.

6 Horkheimer, Max; Adorno, Theodor W.: Dialektik der Aufklärung. Philosophische Fragmente 1947, Frankfurt a.M.: Firscher, 1988, S. 10.

Sara Ahmed geht weiter. Für Ahmed prägen die Geschichte der Wissenschaft und der Philosophie nicht nur das Denken, sondern darüber hinaus das Physische eines Individuums. Demnach erben alle Körper Geschichte, und das Erbe des *Kartesianismus* (Philosophie von Descartes) beruht auf einer weißen, heterosexuellen Ontologie. Der Körper und die Welt des westlichen heterosexuellen weißen Mannes maskiert sich als unsichtbarer Hintergrund, der als »normal«, »Standard« oder »universelle« Position angesehen wird. Alles, was davon abweicht, kann als »Ausreißer« bezeichnet werden.[7]

Descartes Betrachtung der Welt als Maschine beeinflusst nicht nur seine Analyse der Welt und des Menschlichen, sondern auch seine philosophischen Methoden. Probleme werden in kleine Schritte unterteilt, um untersucht zu werden. Analysen werden induktiv vom Konkreten zum Abstrakten entwickelt und die Rekursion, die Überprüfung der Vollständigkeit der Analyse, wird zu einer Art Feedback-Loop.[8] Demnach ist der Mensch die Krone einer Schöpfung voller Automaten. Diese Automaten werden nicht als künstliche Maschinen mit einem Innenleben voller Rädchen gesehen, sondern als reduktiv erklärbare Automaten. Als Systeme, die vollständig durch ihre Einzelteile bestimmt werden. Dabei soll jede Ursache eine Wirkung haben. Diese Wirkung kann selbst Ursache für eine weitere Wirkung sein, doch mehrfache Wirkungen und Rückwirkungen werden im Reduktionismus nicht betrachtet. Mit dieser Methode sollen nicht nur Naturphänomene beschrieben, sondern es soll auch verdeutlicht werden, wie sich der Mensch die Natur aneignen kann. Weiterhin soll sie als wissenschaftliche Methode dafür gelten, die Natur – mitunter auch die menschliche – zu beherrschen und zu überwinden.

Gottfried Wilhelm Leibniz geht hier ein Stück weiter. Mit der Schaffung der mechanischen Rechenmaschine unternahm er einen ersten Schritt hin zu dem, was Justin E. H. Smith als ein Jahrhundertprojekt der »Auslagerung der Rationalität« an Maschinen bezeichnen würde.[9] Die Maschine und das maschinelle Denken sollen im Sinne Bacons die Einschränkungen überwinden, die den Menschen durch seine Natur, seine Kultur und seinen falschen Sprachgebrauch an Erkenntnissen hindern.[10] Die Natur wird so zum Material, das mechanisch manipulierbar und durch künstliche Maschinen nach-

7 Ahmed, Sara: »A phenomenology of whiteness«, In: Feminist Theory, 8 (2007), S. 149-168.

8 Vgl. Descartes, René : Discours de la méthode, (II. 7-10).

9 Vgl. Smith, Justin E.: Irrationality, Princeton, NJ: Princeton University Press 2019.

10 Vgl. Gloy, Karen: Die Geschichte des wissenschaftlichen Denkens, Köln: KOMET 1995, S. 179ff.

geahmt, ersetzt oder überwunden werden kann – im Gegensatz zu anderen Ansätzen, wie etwa in der chinesischen Philosophie, die Harmonie mit der Natur sucht.

Diese Theorien prägten nicht nur die naturwissenschaftliche Forschung, sondern auch die politische und Rechtsphilosophie methodisch und inhaltlich. So entwirft Thomas Hobbes mit dem Leviathan ein künstliches Wesen:

> »Die Natur (die Kunstfertigkeit, vermittelst welcher Gott die Welt erschaffen hat und regiert), wird durch die Kunstfertigkeit des Menschen, wie in vielen anderen Dingen, so auch hierin nachgeahmt, daß sie ein künstliches Tier erschaffen kann. Denn da ja das Leben nur eine Bewegung von Gliedern ist, deren Beginn in irgendeinem Hauptteil liegt, warum können wir dann nicht sagen, daß alle Automaten (Maschinen, die sich durch Federn und Räder bewegen, wie es eine Uhr tut) ein künstliches Leben haben? Denn was ist das Herz anderes als eine Feder, was sind die Nerven anderes als lauter Stränge und die Gelenke anderes als lauter Räder, die dem ganzen Körper Bewegung verleihen, wie es vom Konstrukteur beabsichtigt wurde? Die Kunstfertigkeit geht noch weiter, indem sie jenes vernunftbegabte und höchst vortreffliche Werk der Natur, den Menschen, nachahmt. Denn durch Kunstfertigkeit wird jener große Leviathan, Gemeinwesen oder Staat genannt (lateinisch civitas), erschaffen, der nur ein künstlicher Mensch ist.«[11]

Darin sind »Billigkeit und Gesetze künstliche Vernunft und künstlicher Wille«[12]. Sprich, Gesetze und Gerichtsbarkeit sollen als die künstliche Formulierung des Volkswillens gesehen werden. Sie sind die *Algorithmen*, mit denen der künstliche Leviathan in Gang gesetzt und beherrscht wird. Das mechanistische Denken als wissenschaftliche Herangehensweise prägte relevante Vertragstheorien in der Geschichte der Verfassung und der politischen Theorie. Mal inhaltlich, als Ideal menschlicher Entwicklung. Wie etwa John Lockes oder Tocquevilles Bestreben[13] zur Emanzipation von der Natur und des Naturzustandes, in der die menschlichen Triebe problematisiert werden. Diesen Naturzustand gilt es zu überwinden und zivilisatorisch durch das Politische

11 Hobbes, Thomas: Leviathan, Hamburg: Felix Meiner 1996, 1. Teil, Einleitung.

12 Ebd.

13 Locke, John: Zwei Abhandlungen über die Regierung, Frankfurt a.M.: Suhrkamp 1977 (13. Nachdruck 2008). Und Alexis de Tocqueville: Democracy in America. Harvey Mansfield and Delba Winthrop, trans., ed.; Chicago: University of Chicago Press 2000.

als das Künstliche ins Geordnete zu rücken. Mal als Beschreibung des anthropologischen Menschenbildes, das klassischerweise als Begründung und Legitimation von Vertragstheorien zwischen den Bürger*innen und dem Staat dient. Wie beispielsweise in Adam Smiths mechanistischen Beschreibungen der menschlichen Triebe. Und auch methodologisch werden mechanistische Ansätze verfolgt, wie Max Webers bürokratische Verwaltung, die sich durch ihre Orientierung am Rationalen, an der Leistungsfähigkeit durch Arbeitsteilung und Berechenbarkeit auszeichnet.

Als Gegenstück zum mechanischen Denken von Descartes – und um die Entmenschlichung der Rationalität durch ihre Externalisierung auf Maschinen zu vermeiden – fanden der europäische Idealismus und die Romantik die Metapher des Organismus. Der Organismus war ein sich selbst regulierendes System, im dialektischen Austausch mit seinem Ökosystem. Die Kybernetik vereinte diese beiden Denkformen. Wie Hans Jonas in seinem Buch *Das Prinzip Leben*[14] anmerkte, wandelte sich die traditionelle dualistische Theoriebildung in eine Form des organischen Prozessdenkens, die auf der Mechanik (Input, Output, Feedback) beruht. Das organische Denken war nicht mehr das Gegenstück zum mechanistischen Denken, sondern eine Weiterentwicklung dessen.

Mechanisches Denken leitet unsere Gesellschaftspolitik

Die Praktiken hinter der Strukturierung von Gesellschaften, das Systematisieren nach dem Baukastenprinzip, das Zerlegen von Prozessen in einzelne Schritte, das Kategorisieren[15] nach objektiven Regeln der Rationalität – dies alles bildet wie oben aufgeführt den Kern des mechanischen Denkens. Dabei führt die Privilegierung der Vernunft als ultimatives Kriterium »zu einem distanzierten Akt«[16]. Die rationale Weltsicht strebt nach »Gewissheit, Stabilität und Ordnung, und so bilden Isolation, Trennung und klare Binaritäten die Grundlagen«[17]. Die *Binaritäten* des Rationalen stehen der Ambivalenz, der

14 Jonas, Hans: Das Prinzip Leben. Ansätze zu einer philosophischen Biologie, Frankfurt a.M.: Suhrkamp 1997.

15 Zur Frage der Bedeutung von nichtkategorisierten Räumen des Zufalls siehe den Beitrag von Timo Rademacher und Erik Schilling in diesem Band.

16 Birhane Abeba: 2021.

17 Prigogine, Ilay; Stengers, Isabelle: Order Out of Chaos: Man's New Dialogue with Nature, New York City: Verso Books 1984.

Ideologie, den Emotionen, moralischen Werturteilen und all dem, was dazwischen liegt, gegenüber.

Das mechanische Denken ist somit keineswegs nur Systematisierung der wissenschaftlichen Ordnung. Strukturieren und Kategorisieren sind zutiefst politische Akte. Kategorien kumulieren und strukturieren Informationen über die Mitglieder einer Gesellschaft. Beispielsweise kann eine Frau kategorisiert werden als Muslima, Dame, Tante oder Tochter.[18] Und jede Kategorie beinhaltet einen anderen Satz von Kategorien, der Aktivitäten, Prädikate oder Rechte und Pflichten beschreibt, die von einem Zugehörigen dieser Kategorie erwartet werden. Kategorien sind andererseits eine Einschränkung und ziehen Grenzen. Eine Kategorie ist statisch und setzt Verallgemeinerbarkeit voraus. Sie muss für mehr als für einen individuellen Fall verwendbar sein, sonst hat sie keine Bedeutung. Sie kann bestenfalls verschiedene Dimensionen eines Sachverhalts künstlich zerlegen und nacheinander reihen (Muslima, Dame, Tante, Tochter). Dadurch vereinfacht sie die Komplexität eines Sachverhalts allerdings zwangsläufig. Nuancen können in Kategorien und Prozentsätzen nicht abgebildet werden. Fragen der Intersektionalität bei Diskriminierungen können durch Kategorien nicht abgebildet werden (siehe unten). Die Ambivalenzen in und zwischen den verschiedenen Dimensionen werden verdunkelt, und damit all das, was außerhalb der Kategorisierung bleibt. Das hat eine unmittelbare politische Konsequenz für das soziale Gewebe einer Gesellschaft. Systematisierungen mittels Kategorien, die menschliche und gesellschaftliche Sachverhalte in ihrem Wesen abbilden und einen universellen Charakter beanspruchen, können nicht alle Menschen und gesellschaftlichen Sachverhalte in Kategorien abbilden. Das lassen die oben beschriebenen methodologischen Einschränkungen nicht zu. Somit werden die unkategorisierten Menschen und Sachverhalte in politischen Verfahren nicht berücksichtigt. Eine inklusive Gesellschaft auf Basis dieser Methodologie zu bilden ist grundsätzlich eine Herausforderung, wenn nicht gar eine Unmöglichkeit.

18 Vgl. Sacks, Harvey.: Lectures on Conversation, Vol. 1 and 2, ed. Gail Jefferson, Oxford: Blackwell 1992. S. 40ff.

Recht als Wenn-Dann-Maschine

Auch Recht folgt einer mechanistischen Verfahrensweise. Sachverhalte werden in eine Wenn-Dann-Struktur eingeordnet. Das *Wenn* beschäftigt sich mit dem Tatbestand, das *Dann* mit den Konsequenzen. Tatbestände bestehen in der Regel aus mehreren Tatbestandsmerkmalen. Ähnlich wie bei der Automatisierung von menschlichen Prozessen wird der Sachverhalt an sich in mehreren Schritten strukturiert und kategorisiert. Durch Subsumtion, das heißt die Unterordnung eines Sachverhalts unter den Tatbestand einer Rechtsnorm, werden Tatbestandsmerkmale sortiert. Diese Art der Systematisierung führt zwar zu Rechtssicherheit und Berechenbarkeit, doch sie ist nicht unproblematisch. Ein konkreter Sachverhalt kann nur in die vorgegebene Kategorie im Gesetz eingeordnet und innerhalb dieser ausgelegt werden. Durch diese Systematik kommt es darauf an, welche Art von Kategorie verwendet wird und inwiefern diese sozialen Interaktionen und Konflikte systematisch abbildet, ohne sie durch kategoriale Reduktion zu verzerren.

Warum kategorienbasierte Antidiskriminierungsgesetze nur bedingt helfen

Diese Zusammenhänge werden relevant bei der Betrachtung von algorithmischen Systemen. Denn diese Systeme führen bestimmte mechanistische Vorstellungen fort, wie die Möglichkeit, Rationalitäten auszulagern und zu optimieren. So werden Softwareprodukte angepriesen, die nicht nur in der Lage sind, menschliche diskriminierende Sprache beziehungsweise Verhaltensweisen zu identifizieren. Sie sollen zugleich menschliche Entscheidungen ersetzen, indem sie beispielsweise ›frei von Verzerrung, objektiv den idealen Bewerbenden vorselektieren‹. Als wären Softwareprodukte abtrennbar von den Menschen, die diese Produkte entwickeln (Datenwissenschaftler*innen, Informatiker*innen, Designer*innen etc.) und deren Annahmen, Subjektivitäten und Vorurteilen. Die sozialen Systeme, in die sie eingebettet sind, zeichnen sich selbst durch ein normativ mechanistisches Denken aus, das Diskriminierung nicht als strukturelles Phänomen, sondern primär als individuellen Schaden betrachtet, basierend auf rechtlich aufgelisteten Kategorien (Geschlecht, Religion, Alter etc.), die unterschiedliche Schutzgrade beschreiben (siehe unten). Nicht aufgelistete Kategorien (wie Körperform, eine der laut

Forschung häufigsten Diskriminierungserfahrungen in der Arbeitswelt)[19] genießen wiederum kaum bis gar keinen Schutz. Folglich entwickeln Unternehmen und Institutionen anhand dieser rechtlichen Kategorien technische Mechanismen und Rechenvorschriften, um mögliche Diskriminierungsmuster hinsichtlich der rechtlich vorgegebenen Kategorien zu identifizieren und ihnen zu begegnen. Nicht rechtlich relevante Kategorien bleiben hingegen undokumentiert. Methodologisch kann so die in der Sozialforschung beschriebene intersektionale Dimension der Diskriminierung nicht erforscht werden.

Diskriminierung als Phänomen weist unterschiedliche Formen und Intensitäten auf. Es ist gekoppelt an die sozio-ökonomische Machtposition eines Menschen (Bildungskapital, Körperform, Alter, familiärer Status etc.) und lässt sich schwer in Kategorien dahingehend auseinandernehmen, mit denen die Intensität einer rechtlich relevanten Form von Diskriminierung begründet wird. Ob eine schwarze Rollstuhlfahrerin aufgrund ihrer Hautfarbe, ihres Rollstuhles oder, weil sie als weiblich gelesen wurde, diskriminiert wird, lässt sich schwer trennen und in einer Kategorienskala abbilden.

Das bedeutet nicht nur, dass die algorithmischen und mathematischen Vorstellungen von Verzerrungen und entsprechenden mathematischen Gegenmaßnahmen von mechanistischem Denken geprägt sind. Sondern auch, dass durch das normative Denken in der kontinentaleuropäischen Rechtskultur Diskriminierung selbst einer mechanistischen Vorstellung unterliegt. Die Verzerrung, die in Maschinen zu finden ist, wird nicht nur durch die mathematische Methodologie, in der sie entsteht, sondern auch durch den normativen, rechtlichen Kontext der Diskriminierung mechanisch hergestellt, verstärkt und sogar legitimiert.

Insbesondere bei der Abbildung von intersektionaler Diskriminierung[20] wird es darauf ankommen, inwiefern diese Kategorien menschliche Merkmale auflisten, die möglicherweise zu illegitimer Ungleichbehandlung führen. Oder ob sie vielmehr den Fokus auf eine Systematisierung der Diskriminierungsprozesse und -dynamiken legen. Diese zwei Schwerpunkte führen zu jeweils anderen Ergebnissen und Anreizen. Das mechanistische Denken ist

19 Vgl. Tyrrell, J., Jones et al.: »Height, body mass index, and socioeconomic status: mendelian randomisation study in UK Biobank«, in: BMJ (Clinical research ed.) 2016, S. 352.

20 Siehe hierzu auch den Beitrag von Francesca Schmidt und Nicole Shephard in diesem Band.

eine Form von Systematisierung, wobei der Schwerpunkt dieser Systematisierung auf anderen Merkmalen, insbesondere der römischen Rechtskultur, beruht.

Ein weiteres Merkmal der neuzeitlichen, kontinentaleuropäischen Philosophie und der römischen Rechtskultur ist das Streben nach Antworten über das Sein und Wesen der Dinge, der Menschen und der Natur – im Gegensatz zu anderen Philosophien mit einem relationalen Ansatz, wie die afrikanische Philosophie des Ubuntu (»I am because you are.«). Mit Fragen nach dem Wesen wird nach universellen Antworten gesucht, die Anspruch auf globale Gültigkeit erheben.

Diese Essentialisierung legt den Fokus auf die Kategorisierung des Seins. Prozesse werden in eine zweite Instanz verlagert, um das Sein zu definieren. Input-Kategorien und Outputs werden überdacht und Feedback produziert, um die Kategorien in einem organischen Prozess neu anzupassen. Der mechanistische Prozess um die Reflexion zwischen Input und Output ersetzt die Beobachtung der tatsächlichen Interaktion (siehe oben die Ausführungen zu Kybernetik).

Das deutsche Allgemeine Gleichbehandlungsgesetz (AGG) basiert auf einer primär geschlossenen Liste von Diskriminierungsgründen (Geschlecht oder sexuelle Identität, Rasse oder ethnische Herkunft, Behinderung, Alter und Religion oder Weltanschauung) und dem Verbot der Ungleichbehandlung auf Basis solcher Kategorien. Diese Diskriminierungsgründe stehen im Gesetz in einer komplizierten Hierarchie des Rechtsschutzes. Damit gehen Risiken eines mechanischen, essentialisierenden Denkens einher: Homogenisierung von intersektionalen Diskriminierungserfahrungen, Essentialisierung von Diskriminierungsgründen und Ausschluss von Ausreißern oder mehrdimensionalen Diskriminierungserfahrungen neben dem rechtlichen Schutz.

Menschliche Identitäten sind indes mehrdimensional (Frau, Muslima, schwarz, geschieden, alleinerziehend etc.), ebenso wie die Diskriminierung.[21] Der Katalog von Kategorien im Art. 3. Abs. 3 des Grundgesetzes, in dem Ungleichbehandlung verboten wird, ist abschließend:

> »Niemand darf wegen seines Geschlechtes, seiner Abstammung, seiner Rasse, seiner Sprache, seiner Heimat und Herkunft, seines Glaubens, seiner re-

21 Siehe hierzu auch den Beitrag von Francesca Schmidt und Nicole Shephard in diesem Band.

> ligiösen oder politischen Anschauungen benachteiligt oder bevorzugt werden. Niemand darf wegen seiner Behinderung benachteiligt werden.«

Die aufgelisteten Merkmale sind gruppenkonstituierend. Weitere Merkmale, die in der Praxis als Anlass für Diskriminierung genommen werden, wie etwa Alter, Übergewicht oder sexuelle Identität, sprich Merkmale, die zu einer *unverschuldeten Diskriminierung* geführt haben, werden in der Rechtspraxis ebenfalls auf Verhältnismäßigkeit geprüft und insbesondere geschützt, »je mehr sich die personenbezogenen Merkmale den in Art. 3 Abs. 3 GG genannten annähern und je größer deshalb die Gefahr ist, dass eine an sie anknüpfende Ungleichbehandlung zur Diskriminierung einer Minderheit führt«[22]. Doch diese Merkmale erfahren eine Hierarchisierung im Recht. So verringert sich das Schutzniveau im Grundgesetz im Vergleich von Geschlecht zu Behinderung und von Behinderung zu rassistischer und religionsbezogener Diskriminierung.[23]

Die deutsche Gesetzgebung normiert das Differenzierungsverbot nicht konsistent in allen gesellschaftlichen Sektoren. Dies hat künstliche Trennungen in der Identität von Betroffenen zur Folge. Es wird also davon ausgegangen, dass die verschiedenen Merkmale, die beispielsweise zur Diskriminierung einer muslimischen Frau führen, einzeln auseinanderstrukturiert und deren Gewichtung einzeln berechnet werden können:

> »Wird einer Hijab oder Niqab tragenden Frau der Abschluss eines Mietvertrages durch eine_n Vermieter_in mit weniger als 50 Wohnungen verweigert, muss sie gut überlegen, auf welchen Diskriminierungsgrund sie sich beruft. Da es sich nicht um ein sog. Massengeschäft handelt, schützt das AGG insoweit nicht vor geschlechter- und religionsbezogener Diskriminierung (§19 AGG); beim Abschluss von Waren- und Dienstleistungsverträgen gilt das Benachteiligungsverbot des AGG nur bei rassistischer Diskriminierung uneingeschränkt. Allerdings könnte ein rechtlich und rechtspolitisch höchst fragwürdiger, spezieller Rechtfertigungsgrund greifen: §19 Abs.3 AGG ermöglicht die Ablehnung von Mieter_innen bestimmter Religion

22 BVerfGE 88, 87 (96); BVerfGE 91, 346 (363); vgl. auch BVerfGE 124, 199(220).

23 Vgl. Lembke, Ulrike; Liebscher, Doris: »Postkategoriales Antidiskriminierungsrecht? – Oder: Wie kommen Konzepte der Intersektionalität in die Rechtsdogmatik?«, in: Simone Philipp et.al. (Hg.), Intersektionelle Benachteiligung und Diskriminierung. Soziale Realitäten und Rechtspraxis, Baden-Baden: Nomos 2014. S. 261-290.

> oder Herkunft zur ›Schaffung und Erhaltung sozial stabiler ausgeglichener Bewohner- und Siedlungsstrukturen‹ – ein Einfallstor für rassistische Segregation.«[24]

Gleiches gilt im Übrigen auch für eine gezielte Förderung benachteiligter Gruppen. Eine Person, die abstrakt aufgrund der Gruppenzugehörigkeit dreifach diskriminiert ist, wird nicht automatisch dreifach gefördert. In diesem Umkehrschluss zeigen sich Schwierigkeiten, die im individualistischen Ansatz des Antidiskriminierungsrechts begründet liegen. Das deutsche Recht versucht, mehrdimensionaler, sprich intersektionaler Diskriminierung mit einer künstlichen Unterscheidung zwischen mittelbarer und unmittelbarer Diskriminierung anhand von Merkmalen zu begegnen, die nicht im Grundgesetz unter Art. 3 Abs. 3 genannt werden.[25] Sie bleibt jedoch bezogen auf starre, aneinandergereihte Merkmale.

Durch dieses mechanistische und essentialistische Denken werden Menschen auf einzelne Merkmale reduziert und in eindimensionalen Identitätscluster korsettiert. Die Kategorien werden ständig angepasst, die Identität ständig durch diesen Prozess eingeengt und verzerrt. Diskriminierung wird nicht als Prozess wahrgenommen, in dem Strukturen sozialer Positionen mehr oder weniger Teilhabe, Zugang und Handlungschancen ermöglichen, kurz Gemeinwohlziele. Diskriminierung wird vielmehr als kategoriales Problem gesehen, das mit der Eingabe eines Inputs (Diskriminierungsmerkmale), durch Beobachtung des Outputs (gesellschaftliche Asymmetrien) und entsprechende Aufbereitung des Feedbacks (Anpassung der Kategorien) angeglichen und behoben werden kann.

Recht und algorithmische Systeme erliegen beide einem Denken, das Diskriminierung fördert. Sie zu überwinden verlangt eine Einhegung von algorithmischen Systemen in Prozessen, die mehr Kontext ermöglichen. Nötig ist ein Weiterdenken der Systematik des Rechts und der Rechtsdogmatik, jenseits der Kategorienbildung, um auch dort mehr Kontext zu erlauben.

> »Renaissance thinkers like Montaigne acknowledged that universal, foundational principles cannot be applied to such practical matters as law, medicine

24 Ebd.

25 Erstes Urteil zu mittelbarer Diskriminierung BVerfG vom 27.11.1997, BVerfGE97, 35-49.

and ethics; the role that context and history play in those areas prevents it.«[26]

Eine Erweiterung der Kategorien im AGG oder Veränderungen im Verfahren, die weiterhin auf einer Kategorienliste gründen, werden in Zeiten von künstlicher Intelligenz den Kategorien hinterherhecheln. Algorithmische Systeme arbeiten sehr differenziert und diskriminieren aufgrund Korrelationen von Kategorien, die sich nicht immer menschlich identifizieren oder erklären lassen. Auch der eher technisch orientierte, risikobasierte Ansatz setzt weiterhin auf den hier im Beitrag problematisierten Verallgemeinerungsansatz und auf Kategorienbildung.

Diskriminierung ist ein strukturelles Phänomen. Individualrechtliche Methoden sind nicht vorrangig geeignet, um Phänomene kollektiver Natur aufzugreifen. Wie auch im Umgang mit Umwelt, sind individuelle Kriterien und Maßnahmen kaum geeignet, systemische Veränderungen von Diskriminierung zu erwirken. Eine inklusive Gesellschaft verlangt mehr als die Summe aller Einzelinteressen. Und das bedeutet zu verstehen, wie die Geographie der Gesellschaft aussieht. Das heißt auch zu verstehen, welche gesellschaftlichen Macht-Asymmetrien austariert werden müssen, um eine tatsächliche Gemeinwohlziele wie Inklusion zu ermöglichen. Es bedeutet, zu verstehen, dass gesellschaftliche Asymmetrien dem permanenten Wandel durch sozio-ökonomische Entwicklungen unterworfen sind. Folglich ist Inklusion nicht als Ziel, sondern als Prozess zu verstehen.

Dementsprechend ist eine Regelungstechnik empfehlenswert, die flexibler und offener ist und möglichst auf Kontextualisierung und Abstraktion von Fallabbildungen setzt. Ein Vorbild könnte das Äußerungsrecht oder auch das Recht gegen unlauteren Wettbewerb (mit Fokus auf Asymmetrien) sein. Beide Rechtsgebiete sind von einer Kontextualisierung abhängig und auch im kontinentaleuropäischen Recht von der Jurisprudenz geprägt.

Inklusion ist demzufolge eine Art Barometer, an dem der Grad der Legitimität innerhalb einer Gesellschaft gemessen werden kann. Für diese Metrik müssen demokratische Gesellschaften ihre Prinzipien und Regeln stets weiter denken und entwickeln.

26 Juarrero, Alicia: Dynamics in action: intentional behavior as a complex system Emergence, 2 2000, S. 24-57.

2.2.2 Menschenrechte

Gemeinwohlorientierte Gesetzgebung auf Basis der Vorschläge der EU »High-Level-Expert Group on Artificial Intelligence«

Eric Hilgendorf

I Ethik und Rechtspolitik im Zeitalter von Digitalisierung und künstlicher Intelligenz

Die Digitalisierung und ihr derzeit meist diskutiertes Anwendungsfeld, die künstliche Intelligenz (KI), sind dabei, unsere gesamte Lebens- und Arbeitswelt umzugestalten. Die Corona-Pandemie hat der Digitalisierung einen zusätzlichen, so noch nie dagewesenen Schub verliehen. Gleichzeitig werden die Notwendigkeit und die Schwierigkeiten einer Regulierung der Digitalisierung in Wirtschaft, Staat und Gesellschaft in teilweise drastischer Weise beleuchtet und hervorgehoben.[1]

1 Die Literatur zur normativen Bewältigung von KI ist inzwischen nicht mehr überschaubar, vgl. nur Anderson, Michael/Anderson, Susan Leigh: Machine Ethics, Cambridge: Cambridge University Press 2011; Beck; Susanne/Kusche, Carsten/Valerius, Brian: Digitalisierung, Automatisierung, KI und Recht, Baden-Baden: Nomos 2020; Bendel, Oliver: Handbuch Maschinenethik, Wiesbaden: Springer 2019; Coeckelbergh, Mark: AI Ethics, Cambridge: The MIT Press 2020; Dignum, Virginia: Responsible Artificial Intelligence, Schweiz: Springer 2019; Hengstschläger, Markus: Digital Transformation and Ethics, Elsbethen: Ecowin 2020; Misselhorn, Catrin: Grundfragen der Maschinenethik, Ditzingen: Reclam 2018; Nida-Rümelin, Julian/Weidenfeld, Nathalie: Digitaler Humanismus. Eine Ethik für das Zeitalter der Künstlichen Intelligenz, München: Piper 2018. Zu Regulierungsfragen Schallbruch, Martin: Schwacher Staat im Netz. Wie die Digitalisierung den Staat in Frage stellt, Wiesbaden: Springer 2018 und zuletzt Nemitz, Paul/Pfeffer, Matthias: Prinzip Mensch. Macht, Freiheit und Demokratie im Zeitalter der Künstlichen Intelligenz, Bonn: J.H.W. Dietz Nachf. 2020.

Den neuen Technologien wird eine in höchstem Maße innovative, ja geradezu »disruptive« Macht zugesprochen.[2] Es liegt auf der Hand, dass ein derart radikaler Veränderungsprozess zahlreiche normative Probleme, und damit ethische und rechtspolitische Herausforderungen aufwerfen muss. Die westlichen Gesellschaften (aber nicht nur sie) haben sich nach dem letzten Weltkrieg mit in Rechtsform gebrachten Menschenrechten einen normativen Rahmen gegeben, der die Staatsmacht bindet und sie verpflichtet, bei Verletzungen der Menschenrechte einzuschreiten. Die Basis der Menschenrechte bildet die Menschenwürde, die sich als ein Ensemble aus grundlegenden subjektiven Rechten des Individuums verstehen lässt.[3] Auf diese Weise wird das Individuum besonders wirksam geschützt.

Der Rückbezug auf die Menschenrechte ermöglicht es, Rechtspolitik und Ethik miteinander zu verknüpfen. Beide werden oft als gegensätzliche Tätigkeitsfelder beschrieben: Die Ethik, so meinen manche, habe es mit übergeordneten Werten und Maßstäben zu tun, die Rechtspolitik dagegen werde bestimmt durch kurzfristige Ziele und bloße »instrumentelle Vernunft«. Bei näherem Hinsehen zeigt sich indes, dass normative Ethik und Rechtspolitik schon deswegen eng aufeinander bezogen sind, weil es in beiden Bereichen um gut begründete oder erst zu begründende Normen geht, an denen sich die menschliche Praxis orientieren kann.

Dementsprechend muss gefragt werden: Welche normativen Vorgaben sollten die Rechtspolitik auf dem Gebiet der Digitalisierung leiten? Zunächst gilt, dass die ethische Analyse für eine rationale Rechtspolitik unverzichtbar ist. Es überrascht deswegen nicht, dass auf vielen politischen Handlungsfeldern ethische Expertise herangezogen wird, und zwar nicht als bloße Bemäntelung anderweitig gefundener Entscheidungen, Ethics-Washing[4] oder als Inspirationsquelle für Sonntagsreden, sondern als wichtiges und in vielen Bereichen sogar unverzichtbares Analyse- und Reflexionsangebot. Dies

2 Zu den Anwendungsfeldern der neuen Technologien eingehend Grunwald, Armin: Der unterlegene Mensch. Die Zukunft der Menschheit im Angesicht von Algorithmen, künstlicher Intelligenz und Robotern, Teil II, München: Riva 2019.

3 Dazu näher unter 2.1. am Anfang.

4 Darunter versteht man die Formulierung hochtrabender ethischer Prinzipen, um öffentlicher Kontrolle und einer wirksamen (weil verpflichtenden) rechtlichen Regulierung zu entgehen. Möglicherweise liegt hier eine Ursache für die auffällige Inflation ethischer Regeln für KI, dazu auch Jobin, Anna/Lenca, Marcello/Vayena, Effy: The global landscape of AI ethics guidelines, Berlin: Nature Machine Intelligence 1, 2019, S. 389-399.

betrifft neben Europa auch andere Länder und Großregionen, die sich anschicken, den technischen Fortschritt auf dem Gebiet von Digitalisierung und KI im Einklang mit ihren jeweiligen kulturellen und gesellschaftspolitischen Vorstellungen zu regulieren, insbesondere die USA und China.[5]

Allerdings scheint Europa auf dem Gebiet der Regulierung anderen Ländern und Großregionen einen Schritt voraus zu sein. In den *Ethics Guidelines for Trustworthy AI* der EU, die am 8. April 2019 veröffentlicht wurden,[6] hat die EU eine Basis für weitere Regulierungsmaßnahmen geschaffen. Die Ethik-Leitlinien stellen den Menschen und seine Bedürfnisse in den Mittelpunkt; immer wieder wird darin von einem »human-centric approach« gesprochen. Dieser Ansatz lässt sich am ehesten als »humanorientiert« oder »humanistisch« einstufen.[7] Die Vorteile der neuen Technologien sollen nicht in erster Linie einzelnen Großunternehmen zugutekommen oder die Macht des Staates mehren, sondern dem Gemeinwohl dienen, also dem Wohlergehen aller Menschen.[8]

---

5 Dementsprechend haben praktisch alle technisch fortgeschrittenen Länder auch entsprechende Ethik-Entwürfe für die Regulierung von KI vorgestellt, siehe den Überblick bei M. Coeckelbergh: AI Ethics, S. 150ff.; P. Nemitz/M. Pfeffer: Prinzip Mensch. Macht, Freiheit und Demokratie im Zeitalter der Künstlichen Intelligenz, S. 314.

6 https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Insgesamt publizierte die HLEG AI vier Dokumente: (1) Die »Ethics Guidelines for Trustworthy AI«, welche die grundlegenden ethischen und rechtspolitischen Erwägungen enthalten, (2) die »Policy and Investment Recommendations«, welche sich mit Fragen der Umsetzung der Grundlagenerwägungen in Politik und Wirtschaft beschäftigen, (3) die »Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment«, durch die den beteiligten Unternehmen die Möglichkeit gegeben wurde, den eigenen Stand der Umsetzung zu überprüfen, und schließlich (4) die »Sectoral Considerations on the Policy and Investment Recommendations for Trustworthy Artificial Intelligence«, in denen vier ausgewählte Anwendungsgebiete, nämlich die industrielle Produktion, E-Government, die Rechtspflege und der Gesundheitsbereich, näher analysiert und potenzielle Anwendungsmöglichkeiten von künstlicher Intelligenz herausgearbeitet wurden.

7 Ausführlich Nida-Rümelin, Julian/Weidenfeld, Nathalie: Digitaler Humanismus. Eine Ethik für das Zeitalter der Künstlichen Intelligenz; Hilgendorf, Eric: Humanismus und Recht – Humanistisches Recht? Eine erste Orientierung, in: Groschopp, Horst (Hg.), Humanismus und Humanisierung, Aschaffenburg: Alibri 2014, S. 36-56.

8 Coeckelbergh, Mark: AI Ethics, S. 183f. hat zu Recht darauf hingewiesen, dass eine solche Humanorientierung schon deshalb nicht selbstverständlich ist, weil andere empfindungsfähige Lebewesen, also heute Tiere und in Zukunft vielleicht einmal Maschinen, ausgeschlossen bleiben.

Einige Beispiele für rechtspolitische Herausforderungen durch KI-Anwendungen

Warum ist die ethische und rechtspolitische Auseinandersetzung mit KI-Anwendungen überhaupt so wichtig? Die folgenden Beispiele machen deutlich, vor welchen Problemen wir stehen.

Drängend, aber ethisch und rechtspolitisch schwierig zu beantworten, sind zunächst Fragen im Zusammenhang mit der modernen digitalisierten Kommunikation, etwa in den sozialen Netzwerken, in denen offenbar zunehmend »autonome« Algorithmen Botschaften formulieren, über sogenannte Social Bots verbreiten und so das wahrgenommene Meinungsspektrum beeinflussen. Eine der größten ethischen wie rechtspolitischen Herausforderungen stellt daher die Frage nach der Reichweite von Meinungsfreiheit im digitalisierten Raum dar.[9] Es ist kaum zu übersehen, dass die Kommunikation im Internet mehr und mehr verroht und Hassrede zu einem Alltagsphänomen geworden ist. KI-gestützte Filtertechnologien können hier helfen, werfen aber das Problem auf, wer über die »herauszufilternden« Inhalte entscheiden soll – die Gesellschaft, Tech-Konzerne oder gar die KI selbst? Haftungsrisiken können für Plattform-Unternehmen ein wirkungsvolles Motiv sein, sich um die über sie verbreiteten Inhalte zu kümmern. Die Haftungsprivilegien der großen Internet-Provider erscheinen deshalb zunehmend als problematisch. Des Weiteren stellen sich interessante interkulturelle Fragen, die sich aus der globalen Reichweite moderner Kommunikation ergeben, etwa wenn Äußerungen, die nach westlichen Standards unbedenklich sind, in einer anderen Großregion (etwa in der arabischen Welt) als grob beleidigend oder gotteslästerlich angesehen werden.

Mit Blick auf die durch autonome Systeme gesteuerte automatisierte Produktion – die Industrie 4.0 – stellt sich die Frage nach dem normativen Rahmen neuer Formen von Arbeit, etwa wenn Menschen direkt mit maschinellen »Kollegen« zusammenarbeiten. Für die industrielle Produktion, die auf ein Zusammenspiel von Mensch und Maschine setzt, rücken Sorgfaltsstandards in den Mittelpunkt: Wie sicher muss die verwendete Technologie sein? Welche Schutzmaßnahmen hat der Arbeitgeber vorzuhalten? Hinzu treten Haftungsfragen: Wer trägt bei einem Unfall die Verantwortung und muss Schadensersatz leisten? Noch komplizierter werden die Haftungsfragen im Zusammen-

9 Umfassend Garton Ash, Timothy: Redefreiheit. Prinzipien für eine vernetzte Welt, München: Carl Hanser Verlag GmbH 2016 (deutlich angelsächsisch geprägte Sicht).

hang mit der Nutzung von Augmented Reality, etwa wenn Menschen über eine VR-Brille missverständliche Arbeitsanweisungen erhalten (und in der Folge ein Schaden entsteht) oder wenn der Kontakt mit dem Gegenüber nicht mehr von Mensch zu Mensch geschieht, sondern mittels Avataren in einer virtuellen Umgebung.[10]

Ein weiteres, ebenfalls bereits intensiv diskutiertes Problemfeld bilden neue Formen digital gestützter Mobilität, so etwa Dilemma-Probleme, die sich ergeben, wenn ein Fahrzeug bzw. dessen autonom agierender Kollisionsvermeide-Assistent zwischen der Verletzung oder gar Tötung von Menschen zu entscheiden hat.[11] Dürfen wir Entscheidungen über Leben und Tod an Maschinen übertragen? Welche Regeln sollen gelten, wenn eine solche Übertragung vorgenommen wurde? Welchen ethischen und rechtlichen Kriterien soll die Maschine folgen? Ebenfalls bislang nicht hinreichend thematisiert ist die Frage, inwieweit der Staat mithilfe technischer Mittel in den Straßenverkehr eingreifen darf, um Verhalten zu unterbinden, durch das sich die Fahrzeugführer selbst oder andere gefährden. Man könnte hier von den Herausforderungen, aber auch Chancen eines »technologischen Paternalismus« sprechen.[12]

Auch die digitalisierte Medizin, die mehr und mehr an Aufmerksamkeit gewinnt, wirft erhebliche ethische wie rechtspolitische Probleme auf, etwa solche der Verteilungsgerechtigkeit (sollten leistungsfähige und dementsprechend teure medizinische Technologien auch den Armen zur Verfügung gestellt werden?) oder ob Maschinen als »Gefährten« von hochbetagten oder geistig beeinträchtigten Menschen eingesetzt werden dürfen. Es droht die Abhängigkeit von außereuropäischen Monopolanbietern, wenn Europa unter Berufung auf den Datenschutz darauf verzichtet, konkurrenzfähige E-

10 In Würzburg kam es schon vor einigen Jahren zu einem Zwischenfall in einem VR-Testlabor, als der (weibliche) Avatar einer Studentin vom (männlichen) Avatar einer anderen Person massiv sexuell bedrängt wurde.

11 Zusammenfassend Hilgendorf, Eric: Dilemma-Probleme beim automatisierten Fahren. Ein Beitrag zum Problem des Verrechnungsverbots im Zeitalter der Digitalisierung, Berlin: Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) Bd. 130, 2018, S. 674-703. Es ist sehr bemerkenswert, dass das Dilemma-Problem sogar im neuen Gesetzentwurf zu einer Reform des Straßenverkehrsgesetzes (StVG) behandelt wird, vgl. Bundesrats-Drucks. 155/21 vom 12.2.2021 – »Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren«, S. 27.

12 Dazu näher unter III.6 sowie den Beitrag von Timo Radermacher und Erik Schilling in diesem Band.

Health-Angebote zu entwickeln. Darüber hinaus stellen sich Fragen, die gemeinhin mit dem Schlagwort »Enhancement« umschrieben werden. Dabei geht es letztlich um die »Verbesserung« von Menschen mit technischen Mitteln. Eine extreme, zugleich aber durchaus herausfordernde Position nimmt hier der Transhumanismus ein, der eine Fortentwicklung des Menschen mithilfe der Technik offen begrüßt.[13]

Alle genannten Problemfelder werden verknüpft durch die Herausforderungen, die die KI selbst aufwirft. Handelt es sich nur um ein Werkzeug von Menschen, sodass die Regulierung und Festlegung von Verantwortlichkeiten zum Beispiel bei Personen ansetzen sollte, die KI herstellen, vermitteln oder verwenden? Oder ist es zweckmäßiger, KI als eigenständigen Akteur und eigenständiges Verantwortungssubjekt zu sehen? Letzteres würde die überkommenen Mechanismen der Verantwortungszuschreibung und der Trennung zwischen Rechtssubjekten (die Rechte besitzen können) und bloßen Objekten (die als solche nicht »rechtsfähig« sind) auf eine harte Probe stellen.

II Die Ethischen Leitlinien für eine vertrauenswürdige KI und ihre Rezeption

2.1 Die Ethics Guidelines der EU High-Level Expert Group

Im Frühjahr 2018 hatte die EU-Kommission angekündigt, zur Förderung der KI-Forschung in Europa tätig werden zu wollen.[14] Zu diesem Zweck wurde im Herbst 2018 eine Kommission aus 52 Fachleuten zusammengestellt, die je zu einem Drittel aus der Industrie, der akademischen Welt und aus NGOs kamen: die EU High-Level Expert Group on Artificial Intelligence (HLEG AI). Die Gruppe erhielt den Auftrag, tragfähige und praktisch umsetzbare Regeln für die neue Welt der KI in Europa zu entwerfen. Bereits am 8. April 2019 veröffentlichte die HLEG AI ihre Vorschläge für eine vertrauenswürdige (*trust-*

13 Coeckelbergh, Mark: AI Ethics, S. 38ff.; ausführlich Hilgendorf, Eric: Menschenwürde und die Idee des Posthumanen, Menschenwürde und Medizin: Ein interdisziplinäres Handbuch, Berlin: Duncker & Humblot 2013, S. 1047-1067.

14 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe, COM (2018) 237 final (vom 25.4.2018).

worthy) KI.[15] Danach gehören zu einer vertrauenswürdigen KI drei zentrale Elemente: Die KI muss (1) rechtmäßig sein, also den jeweiligen rechtlichen Vorgaben entsprechen, sie muss (2) ethisch akzeptabel sein und (3) (technisch wie sozial) robust. Zu Letzterem gehört auch und gerade der Gesichtspunkt der IT-Sicherheit gegenüber Angriffen, ein fundamental wichtiges Erfordernis, das in sämtlichen Anwendungszusammenhängen von KI zu beachten ist.

Von Anfang an wurde in der HLEG AI die praktische Umsetzbarkeit der zu entwickelnden Vorschläge mit bedacht.[16] Deshalb wurden die Industrie und Verbraucherschutzverbände gleich zu Beginn in die Arbeit eingebunden. Zudem wurde eine Testphase eingeführt, in der die Vorschläge in ausgewählten Unternehmen[17] praktisch auf ihre Umsetzbarkeit geprüft wurden. Dadurch unterscheiden sich die Empfehlungen der HLEG AI von vielen eher akademisch orientierten und nur in zweiter Linie auf konkrete Wirkung hin angelegten Regelwerken.

Menschzentrierter Ansatz

Eine leitende Idee der hier vorgestellten Regeln ist, dass die Entwicklung von KI am konkreten Menschen mit seinen faktisch vorfindbaren Bedürfnissen orientiert sein soll. Dies ist mit dem Konzept des *human-centric approach* gemeint. Als Leitwert verweist die HLEG AI ausdrücklich auf die Menschenwürde. Sie lässt sich als ein Ensemble von sieben grundlegenden subjektiven Rechten verstehen: (1) einem Recht auf ein materielles Existenzminimum, (2) dem Recht auf autonome Selbstentfaltung (minimale Freiheitsrechte), (3) dem Recht auf Freiheit von extremen Schmerzen (z.B. gegen Folter), (4) dem Recht auf Wahrung einer minimalen Privatsphäre, (5) dem Recht auf geistig-see-

15 Siehe oben Fn. 6. Zum Terminus »trustworthy« ebd. M. Coeckelbergh: AI Ethics, S, 152f.; zum Konzept einer »trustless technology« Nemitz, Paul /. Pfeffer, Matthias: Prinzip Mensch. Macht, Freiheit und Demokratie im Zeitalter der Künstlichen Intelligenz, S. 168. Die HLEG AI beschäftigte sich mit sogenannter schwacher, also bereichsspezifischer KI, nicht mit »starker«, menschenähnlicher KI. Diese Grundentscheidung führte mehrfach zu scharfen Auseinandersetzungen in der Gruppe. Letztlich wurden die interessanten, aber eher theoretischen Fragen starker KI ausgespart, um sich auf die praktisch derzeit wesentlich relevanteren Fragen »schwacher« KI konzentrieren zu können.

16 Zur Bedeutung dieses Ansatzes ebd. Coeckelbergh, Mark: AI Ethics, S. 168ff.

17 Dazu gehört etwa die Firma BOSCH. Der Leiter der KI-Forschung von BOSCH, Christoph Peylo, wirkte in der HLEG AI als Experte mit.

lische Integrität, (6) dem Recht auf grundsätzliche Rechtsgleichheit und (7) dem Recht auf minimale Achtung.[18]

Es handelt sich nach dieser Konzeption um echte subjektive Rechte von Individuen auf Schutz ihrer basalen Interessen, nicht bloß um objektives Recht ohne unmittelbaren Individualbezug. Nur subjektive Rechte erlauben es der berechtigten Person, ihr Recht einzuklagen. Durch die Konzeption der Menschenwürde als Bündel von grundlegenden subjektiven Rechten wird also die Stellung der beziehungsweise des Einzelnen mithilfe des wirkungsvollsten verfügbaren Rechtsinstruments gestärkt, der Einräumung eines einklagbaren, relativ präzise umrissenen subjektiven Rechts. Die Menschenwürde schützt nach dieser Konzeption aber nur einen Kernbereich menschlicher Interessen; die oben genannten Rechte sind eng zu interpretieren. So ist nur der innerste Bereich der Privatsphäre (»Intimsphäre«) durch die Menschenwürde absolut geschützt; hier sind keinerlei Abwägungen zulässig. Dagegen ist die weitere Privatsphäre nicht primär durch die Menschenwürde geschützt, sondern durch das abgeleitete und fortentwickelte Recht auf informationelle Selbstbestimmung.[19] Auch bei den anderen Ausprägungen der Menschenwürde kann zwischen einem unantastbaren Kernbereich und einem Außenbereich unterschieden werden, in dem die entsprechenden Interessen zwar grundrechtlich geschützt sind (etwa durch die allgemeine Handlungsfreiheit oder den Gleichheitsgrundsatz), aber eben nicht mehr absolut.

Vier grundlegende ethische Prinzipien

Ausgehend von der Menschenwürdegarantie werden in den Ethik-Leitlinien vier grundlegende ethische Prinzipien identifiziert und daraus sieben Anforderungen abgeleitet, die vertrauenswürdige KI-Systeme erfüllen müssen. Zusätzlich hat die HLEG AI eine Reihe von Fragen und Kriterien formuliert, die dabei helfen sollen, die Leitlinien zu testen und ihre Anforderungen umzusetzen. Die in den Leitlinien festgehaltenen vier ethischen Prinzipien werden explizit auf die europäischen Grundrechtevorgaben gestützt, insbesondere auf

18 Hilgendorf, Eric: Problem Areas in the Dignity Debate and the Ensemble Theory of Human Dignity, in: Grimm, Dieter, Kemmerer, Alexandra und Möllers, Christoph (Hg.), Human Dignity in Context. Explorations of a Contested Concept, Baden-Baden: Nomos 2018, S. 325ff.

19 Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz.

die Charta der Grundrechte der EU, und so im geltenden Recht verankert.[20] Es handelt sich um die vier folgenden Grundsätze:

(1) Respekt vor der menschlichen Autonomie: KI-Systeme müssen so entwickelt werden, dass sie der Freiheit und der Autonomie von Individuen hinreichend Rechnung tragen,
(2) Schadensvermeidung: KI-Systeme dürfen Menschen nicht schädigen,
(3) Fairness: Zu diesem relativ unbestimmten Begriff soll unter anderem gehören, dass Anstrengungen unternommen werden, um individuelle oder Gruppenvorurteile zu verhindern, die zu Diskriminierung oder Stigmatisierung von Minderheiten führen könnten,[21]
(4) Erklärbarkeit: Die Transparenz und Kommunikationsfähigkeiten von KI-Systemen sollen verbessert werden, um ihre Entscheidungen nachvollziehen und kontrollieren zu können.

Sieben zu erfüllende Anforderungen

Aus diesen Grundsätzen ergeben sich sieben Anforderungen: (1) »human agency and oversight«, (2) »technical robustness and safety«, (3) »privacy and data governance«, (4) »transparency«, (5) »diversity, non-discrimination and fairness«, (6) »societal and environmental wellbeing« und (7) »accountability«.[22]

Der Grundsatz der »human agency and oversight« ruft dazu auf, menschliche Entscheidungsmacht und Kontrolle über KI zu wahren.[23] Dazu gehört auch die Möglichkeit, KI-gesteuerte Vorgänge zumindest grundsätzlich zu verstehen. Die Forderung nach »technical robustness and safety« beinhaltet, dass die Systeme so konzipiert sind, dass die Schädigung anderer vermieden

20 Dieser Punkt war in der Gruppe durchaus nicht unbestritten. Manche hätten sich eine stärker theoretisch ausgerichtete philosophische Begründung gewünscht. Derartige philosophische Vorgaben konnten aber nicht eindeutig identifiziert werden; außerdem entbehren sie, anders als die EU-Menschenrechte, der rechtlichen Verbindlichkeit. Dies bedeutet aber nicht, dass bei der Interpretation menschenrechtlicher Vorgaben nicht auch philosophische Erwägungen angestellt werden müssen.

21 Zur »Fairness« wird ferner eine gleiche Verteilung von Nutzen und Kosten gerechnet; es soll Möglichkeiten geben, Kompensationen für Schäden (Schadensersatz) zu erhalten.

22 Ethics Guidelines (oben Fn. 6), S. 14ff.

23 Beispiele für einen Übergang von »agency« vom Menschen auf die Maschine bei Köszegi, Sabine: The Autonomous Human in the Age of Digital Transformation, in: Digital Transformation and Ethics (Fn. 1), Heidelberg: Springer 2020, S. 60-84 (71f.).

wird. Für die HLEG AI gehört dazu auch die Sicherung gegen Angriffe von außen. »Privacy and data government« meint nicht bloß den Schutz des Rechts auf informationelle Selbstbestimmung, sondern darüber hinaus die Kontrolle über sämtliche »eigene« Daten.[24] Mit »transparency« ist die grundsätzliche Erklärbarkeit der Arbeitsweise und Arbeitsergebnisse der KI gemeint. »transparency« kann man als eine Voraussetzung der meisten Formen von »accountability« verstehen.[25] Der Punkt »diversity, non-discrimination and fairness« umfasst unter anderem die Sicherung gegenüber einer unfairen, vorurteilsbehafteten KI. Zum »societal and environmental wellbeing« zählt der Schutz der gesamten Gesellschaft, der Umwelt und auch anderer empfindungsfähiger Wesen. Die Forderung nach »accountability« von KI-Systemen schließlich soll sicherstellen, dass im Falle von Schädigungen durch KI angemessene Haftungs- und Verantwortungsmechanismen existieren.

Die Corona-Krise hat die Zusammenarbeit in der Gruppe seit Frühjahr 2020 stark beeinträchtigt.[26] Dennoch können sich die Arbeitsergebnisse sehen lassen. Die Reaktionen in Deutschland und anderer EU-Partner waren überwiegend positiv. Inzwischen haben die Empfehlungen außerdem Eingang in die wissenschaftliche Diskussion gefunden und teilweise auch in konkrete Policy-Vorschläge.[27] Die betroffenen Verbände stimmten den Vorschlä-

24 Der Fokus der Gruppe lag allerdings auf dem Umgang mit personenbezogenen Daten; technische und andere nicht-personenbezogenen Daten und Fragen nach einem möglichen »Dateneigentum« wurden nur am Rande diskutiert.

25 Eine reine Gefährdungshaftung käme wohl ohne Transparenz der KI aus.

26 Eine Erklärung dafür könnte sein, dass sich Kompromisse im persönlichen Miteinander eher finden lassen als in der Kommunikation online.

27 Siehe etwa die Texte von Coeckelburgh, Mark: AI Ethics, V. Dignum: Responsible Artificial Intelligence und S. Köszegi: The Autonomous Human in the Age of Digital Trasformation. Alle drei waren Mitglieder der HLEG. Vgl. ferner Heinz-Uwe Dettling/Stefan Krüger, Erste Schritte im Recht der Künstlichen Intelligenz. Entwurf der »Ethik-Leitlinien für eine vertrauenswürdige KI«, in: MMR 4/2019, S. 211-217 (mit interessanten Hinweisen auf parallele Fragestellungen im Arzneimittelrecht). Die Autoren orientieren sich am Arbeitsentwurf der Leitlinien vom 18.12.2018. Eine Parallele zum Arzneimittelrecht thematisieren auch P. Nemitz/M. Pfeffer: Prinzip Mensch. Macht, Freiheit und Demokratie im Zeitalter der Künstlichen Intelligenz, S. 327f. Eine »Innenperspektive« bietet der vorzügliche Artikel von Nathalie A. Smuha, The EU Approach to Ethics Gudelines for Trustworthy Artificial Intelligence. A continuous journey towards an appropriate governance framework for AI, Computer Law Review International (Cri), 4/2019, S. 97-106. Smuha hat die Arbeit der Gruppe über fast zwei Jahre hinweg als Projektassistentin souverän betreut und gemanagt.

gen ganz überwiegend zu,[28] was zeigt, dass die HLEG AI eines ihrer wichtigsten Ziele erreicht hat, nämlich die elitären Zirkel universitärer Ethik-Debatten zu verlassen und praktisch wirksam zu werden. Die Mitglieder der HLEG AI haben ihre Arbeit übrigens von Anfang an als *work in progress* angesehen; es wäre naiv und vermessen zu meinen, man könne in vier knappen Dokumenten die normativen Grundlagen für ein so dynamisches Feld wie die künstlichen Intelligenz ein für alle Mal festschreiben.

Im Folgenden wird zunächst die Aufnahme der HLEG-Empfehlungen im neuen EU-Weißbuch zur künstlichen Intelligenz vorgestellt. Europäische Rechtsvorgaben werden in vielen Teilen der Welt beachtet und oft sogar kopiert. Gelegentlich spricht man gar von einem »Brüssel Effekt«.[29] Deshalb soll auch kurz dargelegt werden, welche Wirkung die EU-Vorschläge in China und den USA erzielen. Schon die Tatsache der Rezeption deutet übrigens darauf hin, dass die These vom »Brüssel Effekt« jedenfalls nicht völlig aus der Luft gegriffen ist. Umso wichtiger wird es, das EU-Regelwerk konstruktiv kritisch zu begleiten und auf die reale Bedeutung für das Gemeinwohl hin zu überprüfen.

2.2 Das EU-Weißbuch zur künstlichen Intelligenz

Am 19. Februar 2020 erschien das *EU White Paper on Artificial Intelligence: a European approach to excellence and trust*.[30] Darin werden die Ansätze der Ethik-Leitlinien und der Policy-Vorschläge weiterentwickelt. Europa sei in der Lage, die Entwicklung und Nutzung von KI an vorderster Stelle voranzutreiben.[31] Besonders bemerkenswert ist die große Bedeutung, die der Analyse und Nutzung von Daten zugemessen wird.[32] Auch wird hervorgehoben, wie wichtig es ist, entsprechende Kompetenzen in der Bevölkerung zu entwickeln.[33] Als Grundlage für das durch angemessene Regulierung zu schaffende »Ecosystem of Trust« werden die sieben Kernvoraussetzungen der oben erwähnten Ethik-

28 Siehe nur das gut durchdachte Positionspapier der Bitkom, https://www.bitkom.org/sites/default/files/2019-02/HLEG_Consultation_Bitkom.pdf

29 Bradford, Anu: The Brussels Effect. How the European Union Rules the World, Oxford: Oxford University Press 2020.

30 COM (2020) 65 final.

31 Ebd., S. 3.

32 Ebd., S. 4.

33 Ebd., S. 6f.

Leitlinien genannt.[34] Mehrfach wird außerdem auf die Gefahren »vorurteilsbehafteter« und diskriminierender KI hingewiesen.[35] Mit Blick auf eventuell erforderliche gesetzgeberische Änderungen erwähnt das Weißbuch insbesondere eine Anpassung des geltenden Produktsicherheits- und Produkthaftungsrechts.[36] Flankiert wird das Weißbuch durch einen detaillierten Bericht über die Sicherheit und Verantwortlichkeit für KI[37] sowie eine Zusammenfassung zur Europäischen Datenstrategie.[38] Im Oktober 2020 fand die 2. European AI Alliance Assembly statt, weitere sind geplant.[39]

2.3 Erste Reaktionen aus China und den USA

Die chinesische Regierung hat die Arbeit der EU HLEG AI nicht direkt kommentiert. Verschiedene offizielle Websites (einschließlich der Parteimedien)[40] haben jedoch über die Veröffentlichung der KI-Leitlinien berichtet oder diese nachgedruckt. Besonders hervorgehoben wird, dass Unternehmen, Forschungsinstitute und Regierungsbehörden die Leitlinien testen sollen. Interessant ist auch die Vermutung, dass die EU möglicherweise versuchen werde, mit den Leitlinien den technologischen Wettbewerb zwischen den USA und China zu unterlaufen, und eine regulative Führungsrolle anstrebe.[41]

---

34 Ebd., S. 9. »human agency and oversight«, »technical robustness and safety«, »privacy and data governance«, »transparency, diversity, non-discrimination and fairness«; »societal and environmental wellbeing«, und »accountability«

35 Ebd., S. 11f. und passim.

36 Ebd., S. 13ff.

37 Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee: Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM (2020) 64 final (vom 19.2.2020). Der Bericht stützt sich auf folgendes Dokument: »Liability for Artificial Intelligence and other Emerging Digital Technologies«, verfasst von der Expert Group on Liablity and New Technologies. New Technology Formation (2019).

38 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Eine europäische Datenstrategie, COM (2020) 66 final (vom 19.2.2020).

39 https://fra.europa.eu/en/news/2020/second-ai-alliance-assembly

40 Für die Übersetzung dieser Seiten und der dort abgedruckten Dokumente und die Unterstützung bei ihrer Auswertung danke ich meinem Mitarbeiter Herrn Liu, Chang sehr herzlich.

41 Siehe oben Fn. 8 zum »Brussels Effect«.

Die Haltung der chinesischen Regierung seither lässt sich (aufgrund einer Reihe von Regierungsbeschlüssen und Reden) grob wie folgt zusammenfassen: Die chinesische Regierung ist der Ansicht, dass 1) eine ethische Regulierung und damit auch ethische Leitlinien notwendig seien, 2) es einige Grundprinzipien gebe, auf die sich unterschiedliche Länder einigen könnten, 3) die EU und die USA verschiedene Entwicklungsrichtungen aufweisen, wobei die EU den Schwerpunkt auf Gesetzgebung und Regulierung lege, während die USA bei der Regulierung einen liberaleren Ansatz verfolge und auf die Förderung technischer Innovation setze, 4) China seinen eigenen Weg zwischen beiden Positionen finden müsse und dabei weder die Innovation ersticken noch technologische und ethische Risiken unkontrolliert zulassen solle. Ethische Standards werden in China meist mit Sicherheitsstandards zusammengebracht, wobei die Entwicklung ethischer Standards insbesondere in Bereichen erfolgt, in denen spezifische ethische Fragen auftreten können, wie zum Beispiel medizinische Behandlung und Notfallmaßnahmen. Zwei Monate nach der Veröffentlichung der EU-Leitlinien legte die chinesische Regierung die *Governance Principles for the New Generation of AI – Developing Responsible Artificial Intelligence* vor.[42] Die darin formulierten Prinzipien unterscheiden sich kaum von den sieben Anforderungen, die durch die HLEG AI aufgestellt wurden.

Auch in den USA wurde über die Arbeit der EU HLEG AI berichtet, allerdings seltener und zurückhaltender als in China. Beispielsweise zieht ein Autor des *Forbes Magazine*[43] insgesamt eine positive Bilanz und betont, dass die EU-Leitlinien über die vielen ähnlichen, ebenfalls nicht verbindlichen ethischen Leitlinien in der Welt hinausgingen und zumindest einen detaillierten Rahmen böten, der Einfluss auf die Regulierungspraxis der Vereinigten Staaten haben könnte. Ein Autor von *The Verge*[44] verweist auch auf die Unver-

42 http://govt.chinadaily.com.cn/a/201906/17/WS5d08a7be498e12256565e009.html. Die acht Grundprinzipien lauten: Harmonie und Freundlichkeit (»Harmony and Human-friendly«), Fairness und Gerechtigkeit (»Fairness and Justice«) Integration und Teilen (»Inclusion and Sharing«), Respekt der Privatsphäre (»Respect for Privacy«), Sicherheit und Kontrollierbarkeit (»Safety and Controllability«), geteilte Verantwortung (»Shared Responsibility«), Offenheit und Kooperation (»Open and Collaboration«) und agile Regulierung (»Agile Governance«).

43 https://www.forbes.com/sites/washingtonbytes/2019/04/11/europes-quest-for-ethics-in-artificial-intelligence/

44 https://www.theverge.com/2019/4/8/18300149/eu-artificial-intelligence-ai-ethical-guidelines-recommendations

bindlichkeit und vermutet, dass die EU anstrebe, die Wettbewerbsfähigkeit der EU auf internationaler Ebene durch die Gestaltung ethischer und rechtlicher Normen zu gewährleisten, da Investitionen und Spitzenforschung nicht mit den USA und China konkurrieren könnten. Besonders positiv fiel die Resonanz von Microsoft aus.[45] Die Leitlinien werden als Meilenstein für die ethische und rechtliche Regulierung von KI bewertet. Der Konzern gibt an, die von der HLEG AI formulierten Werte zu teilen, und erklärt sich bereit, an entsprechenden Tests und weiteren Experimenten teilzunehmen. Bemerkenswerterweise unterzeichnete schließlich auch der damalige US-Präsident Donald Trump am 3. Dezember 2020 eine Executive Order zum Einsatz von KI durch die US-amerikanische Regierung, die schon im Titel den Bezug zu den EU-Leitlinien erkennen lässt, ohne sie aber im Text zu erwähnen. Dagegen sind die inhaltlichen Überschneidungen offensichtlich.[46]

III Legislative Herausforderungen – wie könnte ein europäischer Weg bei der Regulierung von KI aussehen?

Die Empfehlungen der HLEG AI sowie das EU-Weißbuch zur künstlichen Intelligenz bieten eine Grundlage für weitergehende Überlegungen, wie die neuen digitalen Technologien reguliert werden sollten. Dabei lassen sich zumindest folgende, besonders wichtige Themenbereiche unterscheiden:

3.1 Haftung und strafrechtliche Verantwortung

Wer für was, wann und wie Verantwortung im Internet oder bei digitalen Prozessen übernimmt, ist eine der drängendsten und schwierigsten ethischen und rechtspolitischen Fragen in der digitalen Welt. Das Thema *Haftung und Verantwortung für von Maschinen verursachte Schäden* wird bereits seit Län-

45 https://blogs.microsoft.com/eupolicy/2019/04/09/ethical-guidelines-trustworthy-ai/

46 Executive Order on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, https://www.whitehouse.gov/presidential-actions/executive-order-promoting-use-trustworthy-artificial-intelligence-federal-government. Vgl. auch schon die Executive Order on Maintaining American Leadership in Artificial Intelligence, unter https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence, vom 11.2.2019.

gerem intensiv diskutiert.[47] Durch den Einsatz autonomer Systeme und KI drohen Haftungslücken und eine damit einhergehende Diffusion von Verantwortung, die mit einem sozialstaatlichen Werten verpflichteten und auf Schadensausgleich angelegten Gemeinwesen schwer vereinbar erscheinen.[48] Gerade am Arbeitsplatz sollte sichergestellt sein, dass bei der Verletzung von Menschen durch Maschinen ein angemessener Schadensausgleich erfolgt. Mit der überkommenen Verschuldenshaftung ist die Zuschreibung von Verantwortung in der Beziehung von Mensch und Maschine oft nur schwer möglich. Deshalb treten manche für die Einführung einer E-Person, also einer elektronischen Person, als Haftungssubjekt ein, was es ermöglichen würde, die Maschinen selbst auf Schadensersatz zu verklagen.[49]

Ein Beispiel mag dies verdeutlichen: Vor einigen Jahren stellte Microsoft den lernfähigen Chatbot »Tay« online, der mit Menschen Gespräche führen und so seine kommunikativen Fähigkeiten perfektionieren sollte. Unerkannt gebliebenen Hackern gelang es, das System so zu beeinflussen, dass es rassistische und frauenfeindliche Äußerungen abgab. Daraufhin musste »Tay« vom Netz genommen werden. Angenommen, durch die Äußerungen des Chatbots

47 Zusammenfassend Hilgendorf, Eric: Zivil- und Strafrechtliche Haftung für von Maschinen verursachte Schäden, in: Bendel, Handbuch Maschinenethik (Fn. 1), S. 437-452; vertiefend für das Zivilrecht jüngst Spindler, Gerald: Haftung für autonome Systeme – ein Update, in: Beck u.a. (Hg.), Digitalisierung, Automatisierung, KI und Recht (Fn. 1), S. 255-284; Zech, Herbert: Gutachten A zum 73. Deutschen Juristentag Hamburg 2020/Bonn 2022: Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung?, München: C.H. Beck 2020; für das Strafrecht Joerden, Jan: Zur strafrechtlichen Verantwortlichkeit bei der Integration von (intelligenten) Robotern in einen Geschehensablauf, in: Beck u.a. (Hg.), Digitalisierung, Automatisierung, KI und Strafrecht (Fn. 1), Baden-Baden: Nomos 2020, S. 287-304; Schuster, Frank: Künstliche Intelligenz, Automatisierung und strafrechtliche Verantwortung ebd., Baden-Baden: Nomos 2020, S. 387-400.

48 Zum Problem der Verantwortungsdiffusion Hilgendorf, Eric: Verantwortungsdiffusion und selbstlernende Systeme in der Industrie 4.0 – ein Problemaufriß aus strafrechtlicher Perspektive, in: Gerrit Hornung (Hg.), Rechtsfragen der Industrie 4.0. Datenhoheit, Verantwortlichkeit, rechtliche Grenzen der Vernetzung, Baden-Baden: Nomos 2018, S. 119-137.

49 Die »E-Person« wäre juristisch als Sonderform einer juristischen Person anzusehen, von der man wie z.B. von einer GmbH oder einer anderen juristischen Person Schadensersatz verlangen könnte. Praktisch würde dies des Weiteren erfordern, haftungsfähigen Maschinen eine hinreichend große Vermögenssumme zuzuordnen, was aber z.B. über eine obligatorische Versicherung leicht zu erreichen wäre.

wäre ein finanzieller Schaden aufgetreten (etwa infolge eines behandlungsbedürftigen Traumas bei einer verbal attackierten Person) – wer wäre dann zum Schadensersatz verpflichtet gewesen? Die Hacker waren nicht zu belangen, der Hersteller beziehungsweise Programmierer konnte darauf verweisen, dass sein System fehlerfrei funktioniert habe. Demnach wäre das Opfer auf seinem Schaden sitzengeblieben. Hier könnte das Modell einer E-Person helfen, als neuer Form einer juristischen Person, die es Betroffenen ermöglichen würde, das Computersystem selbst zur Verantwortung zu ziehen.[50]

Das Konzept einer E-Person entstammt allerdings angelsächsischen Rechtsvorstellungen und ist mit der europäischen, zumal der deutschen, Rechtstradition nicht ohne Weiteres zu vereinbaren, obwohl die Schaffung eines E-Person gesellschaftsrechtlich wohl möglich wäre. Vorzugswürdig erscheint es deshalb, der Gefahr von Haftungslücken und Haftungsdiffusion zu begegnen, indem die (schuldunabhängige) Gefährdungshaftung ausgeweitet wird und etwa die Produkthaftung auch für unkörperliche Produkte wie Algorithmen gilt. Allerdings dürfte noch sehr viel gesetzgeberische Detailarbeit erforderlich sein, bis eine den Leitwerten Europas angemessene Verteilung der Haftungsrisiken im Zusammenhang mit KI erreicht ist.

Noch problematischer ist die Situation im Strafrecht, in dem wegen des (in Deutschland auch in der Verfassung festgeschriebenen) Schuldgrundsatzes (niemand kann für eine Tat bestraft werden, wenn ihn keine Schuld trifft) eine Verantwortung von Maschinen von vornherein ausgeschlossen ist. Überlegungen, Maschinen strafrechtlich zu belangen (etwa aus Gründen der Generalprävention), haben allenfalls den Charakter von (durchaus interessanten!) Gedankenexperimenten, könnten jedoch praktisch nicht ohne massive Verletzungen zentraler Basisannahmen rechtsstaatlichen Strafens in Europa umgesetzt werden. Bis auf Weiteres muss hier also die Möglichkeit von Strafbarkeitslücken akzeptiert werden; bislang scheint es übrigens kaum reale Fälle zu geben, in denen die Strafbarkeit einer Maschine (etwa »Tay«) sinnvoll wäre.[51]

50 Näher dazu Hilgendorf, Eric: Autonome Systeme, Künstliche Intelligenz und Roboter, in: Stephan Barton u.a. (Hg.), Festschrift für Thomas Fischer, München: C.H. Beck 2018, S. 99-113 (109f.).

51 Ebd. E. Hilgendorf, Autonome Systeme, Künstliche Intelligenz und Roboter, S. 110.

3.2 Schutz von Persönlichkeitsrechten – auch mittels des Strafrechts

Ein zweiter wichtiger Problemkreis ist der Schutz von Persönlichkeitsrechten, die im Internet, zumal den sozialen Netzwerken, offenbar zunehmend auch durch Bots und autonome Systeme angegriffen werden. Die Probleme, die sich hier stellen, sind außerordentlich vielschichtig und entsprechend schwierig zu lösen:

In den USA wird die in der Verfassung festgelegte Redefreiheit (*freedom of speech*) von den Gerichten so weit ausgedehnt, dass Persönlichkeitsrechte in aller Regel dahinter zurückzutreten haben.[52] Ein Beleidigungsstrafrecht in unserem Sinne, durch das ein Minimum an zwischenmenschlichem Respekt gesichert wird, existiert nicht. Dieses extrem weite Verständnis von Redefreiheit findet sich im Wesentlichen nur in den USA; im Rest der Welt, angefangen von Ländern des angelsächsischen Rechtskreises wie Großbritannien oder Kanada über Kontinentaleuropa bis hin zu Lateinamerika oder Ostasien, gelten Regelungen zum Schutz der Persönlichkeitsrechte. Da aber die Internettechnologie und insbesondere die sozialen Netzwerke von US-Anbietern dominiert werden, zählen dort grundsätzlich die US-amerikanischen Standards, die so über die USA hinaus Geltung beanspruchen, ohne nennenswerte Mitspracherechte der davon Betroffenen vorzusehen. Dies führt in vielen Ländern zu erheblichen Problemen bei der Umsetzung nationalen Persönlichkeitsschutzrechts, wie sich auch während den hitzigen Debatten um das inzwischen reformierte Netzwerkdurchsetzungsgesetz[53] zeigte.

Phänomene in den sozialen Netzwerken, wie Hassrede, Fake News, sexuelle Anzüglichkeiten und Cybermobbing, werden inzwischen auch in den USA als massives Problem empfunden. Der Verzicht auf eine gesetzliche Kontrolle von Hassrede,[54] der sich früher vor allem zulasten der afroamerikanischen Bevölkerung und anderer unterprivilegierter Minderheiten auswirkte,

52 Vgl. T. Garton Ash, Redefreiheit. Prinzipien für eine vernetzte Welt, S. 198ff. In fast allen anderen Ländern existiert ein Beleidigungsstrafrecht, das besonders drastische Verletzungen zwischenmenschlichen Respekts mit Strafe belegt. Siehe für Deutschland etwa Hilgendorf, Eric: Beleidigungsstrafrecht, in: Eric Hilgendorf, Hans Kudlich und Brian Valerius (Hg.), Handbuch des Strafrechts, Band 4, Heidelberg: C.F. Müller 2019, § 12.

53 Die Reform des NetzDG wurde Anfang April 2021 vom Bundespräsidenten unterzeichnet.

54 Zu Kompensationsphänomenen wie »political correctness« E. Hilgendorf, Beleidigungsstrafrecht (Fn. 52), Rn. 8.

hat im Zeitalter sozialer Netzwerke zu einer bisher nicht dagewesenen Spaltung der US-amerikanischen Gesellschaft geführt. Seit einigen Jahren wird darüber spekuliert, dass viele der besonders enthemmten Posts möglicherweise gar nicht von Menschen stammen, sondern von KI-gestützten Bots, die mehr oder weniger autonom, aber nicht ohne Ziel aktiv sind. Die rechtliche Begrenzung und Kontrolle derartiger Einsatzformen von KI[55] gehört weltweit zu den wichtigsten, neuen rechtspolitischen Aufgaben.

In diesen Zusammenhang gehört auch die Frage nach einer angemessenen zivilrechtlichen und strafrechtlichen Haftung von Providern und Intermediären. Bislang wurden Diensteanbieter im Internet europaweit von zivil- und strafrechtlicher Haftung weitgehend freigestellt.[56] Ziel der Regelung war es seinerzeit, der sich entwickelnden Internetwirtschaft und der Entfaltung des offenen Internets keine unnötigen Steine in den Weg zu legen und klarzustellen, dass ein Provider nicht ohne Weiteres für rechtswidrige Inhalte haftet, zu denen er technisch den Zugang eröffnet. Ob diese Haftungsprivilegien heute noch zeitgemäß sind, ist sehr zweifelhaft.

3.3 Diskriminierungsfreiheit

Eines der schwierigsten Themen bezüglich der Regulierung von KI stellt der Umgang mit potenziell vorurteilsgeprägter Technologie dar.[57] Ein Ausgangspunkt vieler Debatten ist die von US-Gerichten verwendete Software Correctional Offender Management Profiling for Alternative Sanctions (COMPAS). Damit wird unter anderem die Rückfallwahrscheinlichkeit von Straftätern eingeschätzt und so die richterliche Entscheidung unterstützt. Dem Hersteller wurde vorgeworfen, das System würde infolge selektiver Datenauswahl Menschen mit Afroamerikanischer Herkunft benachteiligen, es arbeite mit

55 Vgl. Grunwald, Arnim: Der unterlegene Mensch. Die Zukunft der Menschheit im Angesicht von Algorithmen, künstlicher Intelligenz und Robotern, S. 167ff. bezeichnet derartige Algorithmen geradezu als »Totengräber der Demokratie«.

56 Diese Privilegierung geht zurück auf die Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (»Richtlinie über den elektronischen Geschäftsverkehr«) Amtsblatt Nr. L 178 vom 17/07/2000 S. 0001-0016. In Deutschland wurden diese Vorgaben im Telemediengesetz umgesetzt.

57 Vgl. Coeckelbergh, Mark: AI Ethics, S. 125ff. Siehe außerdem den Beitrag von Hustedt und Beining in diesem Band.

einem Bias gegenüber Schwarzen.[58] In anderen Studien wurde dem jedoch widersprochen;[59] auch das Oberste Gericht des US-Bundesstaates Wisconsin hielt die Verwendung von COMPAS für zulässig.[60]

KI entscheidet anhand der ihr zur Verfügung gestellten Daten. Schon darin kann man einen Vorteil gegenüber manchen menschlichen Entscheidungen sehen. Auch lassen sich Maschinen nicht durch Emotionen oder eigene Interessen beeinflussen. Allerdings hängt die Qualität maschineller Entscheidungen von der Qualität des Dateninputs ab, schlechte Daten bewirken schlechte Entscheidungen.[61] Daher wäre es verfehlt, Entscheidungen – oder entsprechende Vorschläge – durch Maschinen von vornherein für objektiver zu halten als menschliche Entscheidungen. Bei der Bewertung einer maschinellen Entscheidung sollte die Datenbasis stets mit geprüft werden.

Ein zweiter Aspekt tritt hinzu. Als Beispiel mag eine KI dienen, die anhand aller öffentlich verfügbaren Daten Entscheidungsvorschläge für die Besetzung von Vorstandsposten erarbeiten soll. Da in der Vergangenheit derartige Positionen ganz überwiegend von älteren Männern besetzt waren, schlägt die KI weiterhin in erster Linie Personen mit eben diesen Eigenschaften vor. Ähnliche Beispiele ließen sich für die Besetzung einer Stelle als Hebamme oder Fachkraft im Kindergarten bilden. Das wesentliche Problem liegt wohl im Folgenden: Auch wenn eine bestimmte Gruppe oder Menschen mit bestimmten Eigenschaften in der Vergangenheit stets mit einer bestimmten Stellung oder Tätigkeit in Verbindung gebracht werden konnten, ist es nicht ohne Weiteres zwingend und möglicherweise sogar problematisch, diesen Zustand in die Zukunft zu verlängern. Der auf früheren Daten aufgebaute maschinelle Entscheidungsvorschlag ist von einem Konservativismus geprägt, der seinerseits einer Begründung bedarf. Möglicherweise sprechen normative Gesichtspunkte dagegen, die Vergangenheit einfach in

58 Vgl. Angwin, Julia/Larson, Jeff u.a.: »Machine Bias« https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (23.5.2016), weiterführend und das Problem kontextualisierend Lobe, Adrian: Speichern und Strafen. Die Gesellschaft im Datengefängnis, 2019, S. 173ff. (Standardbestimmung durch KI), S. 186ff. (COMPAS).

59 Vgl. Flores, Anthony W./Lowenkamp, Christopher T./Bechtel, Kristin: False Positives, False Negatives, and False Analyses: A Rejoinder to »Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks.« https://www.crj.org/assets/2017/07/9_Machine_bias_rejoinder.pdf

60 Vgl. https ://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690

61 Informatiker nutzen oft die Formulierung »garbage in – garbage out«.

die Zukunft zu übertragen. Eine derartige »normative Kontrollebene« fehlt der maschinellen Intelligenz.

Allerdings sollte man es sich hier nicht zu einfach machen. In vielen Fällen wird eine auf feststehenden Daten beruhende maschinelle Einschätzung zutreffend und überzeugend sein. Nehmen wir an, ein KI-System soll anhand öffentlich verfügbarer Daten einen Vorschlag darüber unterbreiten, ob die Stelle eines Fahrrad-Pizzaboten an einen 20-jährigen Sportler oder eine 75-jährige Rentnerin vergeben wird. Unter Berücksichtigung der bisherigen Besetzung ähnlicher Positionen empfiehlt die Maschine den 20-Jährigen. Liegt darin eine ungerechtfertigte Diskriminierung? Die meisten würden das wohl verneinen, weil das Lebensalter und die damit normalerweise einhergehende körperliche Leistungsfähigkeit für die angebotene Stelle entscheidend sind. Das Alter ist hier also ein guter Grund für eine Ungleichbehandlung und seine Berücksichtigung stellt keine ungerechtfertigte Diskriminierung dar.

Damit wird deutlich, dass das Problem potenziell vorurteilsbehafteter KI eng mit dem wesentlich weitergehenden Problem verknüpft ist, welche Gesichtspunkte wir als zulässige Kriterien einer Ungleichbehandlung ansehen. Letzteres ist eine gesellschaftliche Frage, die nicht nur in zeitlicher Perspektive, sondern auch von Gruppe zu Gruppe unterschiedlich beantwortet wird. Rechtliche Vorgaben lassen sich in Artikel 3 Grundgesetz (Gleichheitsgrundsatz), aber auch im Allgemeinen Gleichbehandlungsgesetz finden; ihre Übertragbarkeit auf KI-generierte Entscheidungsvorschläge oder Entscheidungen ist aber im Detail noch ungeklärt. Die Forderung nach Transparenz darf sich jedenfalls nicht bloß auf Daten beziehen, sondern muss auch die zugrunde gelegten Kriterien umfassen. Die Analyse und systematische Aufarbeitung der damit zusammenhängenden Fragen stellt derzeit eine der wichtigsten Forschungsaufgaben und politisch-regulativen Herausforderungen im Zusammenhang mit KI dar.

3.4 Transparenz und Erklärbarkeit von KI-Entscheidungen

Das Thema explicabilty beziehungsweise transparency, also die Erklärbarkeit beziehungsweise Transparenz von KI-Systemen, spielte in den Diskussionen der HLEG AI eine erhebliche Rolle, da es sich um ein neues Prinzip handelt, das im traditionellen Diskurs über Menschenrechte so noch nicht vorkam.[62]

62 Eine gewisse Parallele lässt sich allerdings zu den in den 1990er und früher 2000er Jahren verbreiteten Vorstellungen ziehen, das seinerzeit neue Internet könne helfen,

Außerdem gab und gibt es erhebliche Meinungsunterschiede darüber, worauf explicability oder explainability genau abzielen.[63] Wegen seines innovativen Charakters und der daraus entstehenden Interpretationsoffenheit überschneiden sich explicability und transparency mit anderen Themen, etwa accountability oder responsibility, meines Erachtens, ohne dass bisher eine hinreichend klare Abgrenzung gelungen wäre.[64] In den Ethik-Leitlinien heißt es, explicability sei:

> »crucial for building user's trust in AI systems. This means that processes need to be transparent, the capabilities and purpose of AI systems openly communicated, and decisions – to the extent possible – explainable to those directly or indirectly affected. Without such information, a decision cannot be duly contested.«[65]

Es liegt auf der Hand, dass eine so verstandene »Erklärbarkeit« bei vielen Systemen an technische Grenzen stößt. Im Bereich des Deep Learnings scheint es sogar von vornherein ausgeschlossen zu sein, dass es zu erklären ist, warum die (sich selbstständig weiterentwickelnde) Maschine zu einem bestimmten Ergebnis gekommen ist. Man sollte überdies bedenken, dass Detailinformationen über Arbeitsabläufe im Computer und die Art und Weise der Ergebnisgenerierung in vielen Fällen Betriebsgeheimnisse sind, die die betroffenen Firmen weder offenbaren wollen noch (nach derzeitigem Gesetzesstand) müssen. Schließlich sei der Hinweis erlaubt, dass die entsprechenden Prozesse im menschlichen Gehirn ebenfalls im Dunklen liegen; warum jemand zu einer bestimmten Aussage oder Wertung gelangt, kann im Detail nicht nachvollzogen werden, auch wenn Ex-ante-Prognosen und Ex-post-Erklärungen möglich sind, die allerdings auch fehlerhaft sein können, wie die Lebenserfahrung zeigt.

---

politische Prozesse »transparenter« zu gestalten. Damals bezog sich die Transparenzforderung allerdings auf (menschliche) Entscheidungsprozesse, heute auf maschinell generierte Entscheidungen.

63 Guter Überblick bei M. Coeckelbergh, AI Ethics, S. 116ff.

64 Auch zum Grundsatz der »human agency« existieren Überschneidungen. So heißt es auf S. 16 der »Ethics Guidelines (Fn. 6): »Human agency. Users should be able to make informed autonomous decisions regarding AI systems. They should be given the knowledge and tools to comprehend and interact with AI systems to a satisfactory degree and, where possible, be enabled to reasonably self-assess or challenge the system. AI systems should support individuals in making better, more informed choices in accordance with their goals.«

65 Ethics Guidelines (Fn. 6), S. 13.

Andererseits erscheint es nicht bloß ethisch, sondern auch rechtlich erforderlich, KI-gestützte Entscheidungen und die zugrunde liegenden Kriterien transparent zu gestalten und bei Unklarheiten eine Erklärung fordern zu können. Ohne eine solche Transparenz würde die Klärung eventueller Haftungsfragen erheblich erschwert, von dem rechtsstaatlichen Erfordernis einer Erklärung KI-gestützter hoheitlicher Entscheidungen ganz zu schweigen. Es gehört deshalb zu den wesentlichen Aufgaben des KI-Rechts, die Konzepte *Erklärbarkeit* und *Transparenz* von KI-gestützten Entscheidungen zu vertiefen und ihnen einen Ort im überkommenen Rechtssystem, gerade im Verwaltungs- und Haftungsrecht, zuzuweisen.

3.5 Schutz der Privatsphäre und Datenhoheit[66]

Alle technisch fortgeschrittenen Gesellschaften der Erde, auch und gerade in Europa, entwickeln sich derzeit in Richtung auf das »panoptische Modell«, in dem einige wenige die Kontrolle über die Daten der überwältigenden Mehrheit der Menschen besitzen.[67] So ist offensichtlich, dass immer mehr Daten aus Europa von ausländischen, vor allem US-amerikanischen Großunternehmen erhoben und dort kommerziell genutzt werden, ohne dass erstere irgendein Mitspracherecht hätten oder gar an dem aus der Verwendung »ihrer« Daten entstehenden Profit irgendwie beteiligt wären. Im Mai 2018 ist die Europäische Datenschutz-Grundverordnung (DSGVO) in Kraft getreten. Damit wurde das traditionelle Datenschutzmodell noch einmal eindrucksvoll aktualisiert und revitalisiert. Die DSGVO liegt auch den entsprechenden Konzepten der HLEG AI zugrunde. Sie hat sich in den ersten drei Jahren ihrer Geltung als erfolgreicher erwiesen, als es anfangs vorausgesagt wurde. Dennoch ist nicht zu übersehen, dass sich der Datenschutz in Deutschland – und Deutschland steht hier pars pro toto für ganz Europa – in einer Krise befindet.

Schon die Bezeichnung »Datenschutz« ist irreführend, denn streng genommen werden nicht Daten geschützt, sondern das Grundrecht auf informationelle Selbstbestimmung, also das Recht, über die auf die eigene Person

66 Siehe auch den Beitrag von Nils Leopold in diesem Band.

67 Es sei die Anmerkung erlaubt, dass Jeremy Bentham, auf dessen Ideen die Vorstellung eines »panoptischen Modells« zurückgehen, das Problem »Wer kontrolliert die Kontrolleure?« gesehen und sogar eine bemerkenswerte Lösung dafür angeboten hat: die Öffentlichkeit! Bedauerlicherweise scheint Benthams Problembewusstsein heute verloren gegangen zu sein.

bezogenen Daten selbst zu bestimmen. Der Fokus auf personenbezogene Daten zeigt, dass es sich beim überkommenen Datenschutzrecht im Kern um eine Kommunikationsordnung handelt, die den Umgang mit personenbezogenen Daten regelt. Durch die gewaltigen Fortschritte der Digitalisierung in den letzten zwei Jahrzehnten hat sich die Problematik aber über den Schutz personenbezogener Daten hinaus hin zur Frage gewandelt, wie sich der Umgang mit Daten jeder Art regulieren lässt. Daten besitzen heute, anders als noch vor zwei Jahrzehnten, einen gewaltigen ökonomischen Wert, sie sind zu einem bedeutenden Wirtschaftsgut geworden. Es geht nicht mehr nur um Kommunikation, sondern um den Rohstoff für datengetriebene Geschäftsmodelle und damit letztlich um wirtschaftlichen Erfolg.

Umso fataler ist es, dass das europäische Datenschutzrecht nur personenbezogene Daten erfasst und der Umgang mit sowie der Schutz von Daten anderer Art, etwa technischer Daten, nicht angemessen reguliert werden. Da sie keine Sachqualität aufweisen, sind Daten nicht eigentumsfähig, die Rede von den »eigenen« Daten ist, wenn sie sich nicht auf eigene personenbezogene Daten bezieht, juristisch gesehen irreführend. Es existiert derzeit keine allgemein akzeptierte Möglichkeit, Daten originär eigentumsrechtlich zuzuordnen. Dies bedeutet unter anderem, dass nicht-personenbezogene Daten fast nach Belieben abgezogen und verwertet werden dürfen, ohne dass die Betroffenen dagegen Einspruch erheben können.[68]

Die meisten Menschen sind dem Datenschutz gegenüber sehr gleichgültig: Datenschutzverletzungen werden, sofern eine breitere Öffentlichkeit überhaupt davon erfährt, mehr oder weniger teilnahmslos hingenommen. Damit hängt ein paradoxes Phänomen zusammen: Auf der einen Seite fordern Viele vom Staat zu Recht ein hohes Maß an Privatsphäre und einen besonderen rechtlichen Schutz ihrer personenbezogenen Daten. Auf der anderen Seite ist der ganz überwiegende Teil der Bevölkerung ohne größere Bedenken bereit, seine Daten ausländischen (Quasi-)Monopolisten zur Verfügung zu stellen, wenn dafür (scheinbar) kostenfrei ein Dienst in Anspruch genommen oder eine App genutzt werden kann. Die Informationspflichten der Datenverarbeiter, die der beziehungsweise dem Einzelnen die Konsequenzen einer Einwilligungserteilung vor Augen führen sollen, werden (faktisch unbeanstandet) in Gestalt mehrseitiger Dokumente erfüllt, von

68 Vgl. Hilgendorf, Eric: Offene Fragen der neuen Mobilität: Problemfelder im Kontext von automatisiertem Fahren und Recht, Frankfurt a.M.: Recht – Automobil – Wirtschaft (RAW) 2018, S. 85-93 (89f.).

denen allgemein bekannt (und überdies häufig auch so gewollt) ist, dass sie nur von einem Bruchteil der Betroffenen gelesen werden. Dieses Phänomen setzt sich bei nicht-personenbezogenen Daten fort. Ein wirksames Datenschutzrecht müsste in puncto Information und Aufklärung mehr bieten als einfach zu erfüllende Informationspflichten, wenn es von mündigen Grundrechtsberechtigten wahrgenommen werden soll.

Die technische Entwicklung lässt außerdem zentrale Grundsätze des überkommenen Datenschutzrechtes als unzeitgemäß erscheinen. Prinzipien wie das der Datenminimierung (es sollen so wenig Daten wie möglich aufgenommen werden) und Zweckbindung (Daten sollen nur zu dem Zweck verwendet werden dürfen, zu dem sie erhoben wurden) sind im Zeitalter von Big Data und KI nahezu sinnlos geworden, da die neuen Geschäftsmodelle gerade voraussetzen, möglichst viele Daten einzusammeln, die dann zu beliebigen Zwecken im Data Mining verwendet werden können. Eine derart groß angelegte Datenanalyse ist keineswegs per se verwerflich, sie kann vielmehr durchaus sinnvoll und gesellschaftlich erwünscht sein. So lassen sich etwa in einem großen Fundus medizinischer Daten möglicherweise Muster erkennen und Korrelationen finden, die helfen, Krankheitsursachen zu identifizieren.

Um KI im medizinischen Sektor in großem Umfang einsetzen zu können, muss diese KI allerdings mit Daten, und zwar mit möglichst vielen Daten, trainiert werden. Dies ist mit dem geltenden Datenschutzrecht nicht ohne Weiteres vereinbar, da das Sammeln größerer Datenmengen von vornherein durch das Regelungsmodell »Verbot mit Erlaubnisvorbehalt« beschränkt wird. Der verbreitete und oft gänzlich unreflektierte »Datenschutz-Absolutismus«, der die gesetzlich verbürgten Einschränkungsmöglichkeiten beim Datenschutz[69] ignorieren zu können glaubt, verschärft die ohnehin große Gefahr einer Monopolbildung bei ausländischen Anbietern und läuft dem Gemeinwohl zuwider. Eine vorherige Anonymisierung der Daten ist schwer möglich, zumal sich heute mit hinreichendem Aufwand praktisch alle Daten wieder mit einem Personenbezug versehen lassen. Ohne Übertreibung

69 Kein Grundrecht, die Menschenwürde ausgenommen, gilt schrankenlos; vielmehr können alle Grundrechte eingeschränkt werden, um höher zu gewichtende Belange des Gemeinwohls zu verwirklichen. Dabei ist allerdings stets der Grundsatz der Verhältnismäßigkeit zu beachten. So enthält etwa die DSGVO in Art. 89 eine großzügige Öffnungsklausel für die Forschung; bei medizinischen Daten ist außerdem Art. 9 DSGVO zu beachten.

lässt sich sagen, dass durch den technischen Fortschritt bereits das Konzept des »anonymisierten Datums« als solches fragwürdig geworden ist.

Gerade im medizinischen Bereich, der zunehmend in den Mittelpunkt rückt, droht eine Monopolisierung der Daten und damit des verfügbaren Wissens. Es dürfte kein anderes Gebiet geben, in dem der Grundsatz *The winner takes it all* in dem Maße gilt wie in der Medizin.[70] Wenn es um die Gesundheit oder gar das Leben der eigenen Person oder naher Angehöriger geht, ist niemand bereit, sich mit der zweitbesten Lösung zufriedenzugeben, und kein Aufwand ist zu groß, wenn er nur Hilfe verspricht. Eine Abhängigkeit von kommerziell orientierten und nicht mehr regulierbaren außereuropäischen Mega-Unternehmen wäre hier fatal.

Der Befund lässt sich so zusammenfassen: Das Recht auf informationelle Selbstbestimmung ist heute wichtiger denn je. Gleichzeitig wird es aber so massiv bedroht, dass ein Überdenken des bisherigen Schutzansatzes dringend nötig geworden ist. Datenschutz ist kein Selbstzweck, sondern muss sich am Gemeinwohl orientieren. Ein neuer Ansatz ist auch deshalb zentral, weil das überkommene Datenschutzrecht lediglich personenbezogene Daten erfasst und nicht-personenbezogene Daten, etwa Daten technischer Art, außer Betracht lässt, obwohl gerade diese Daten inzwischen für zahlreiche Geschäftsmodelle eine besonders große Rolle spielen. Mit ihrer neuen »Datenstrategie«[71] hat die Bundesregierung einen großen Schritt in die richtige Richtung unternommen; ob die wohlklingenden Worte auch umgesetzt werden, bleibt abzuwarten.

3.6 Technologischer Paternalismus

Ein weiteres schwieriges Problemfeld eröffnet sich mit der Frage, ob beziehungsweise inwieweit durch technische Mittel wie KI Rechtsverstöße erschwert, ganz unmöglich gemacht oder zumindest automatisiert sanktioniert werden dürfen oder sollten. Man kann das Problem anhand eines Beispiels aus dem Straßenverkehr verdeutlichen: Statt Geschwindigkeitsüberschreitungen oder das Überfahren roter Ampeln zu verbieten und im

70 Vgl. Hilgendorf, Eric: Medizin und Digitalisierung, Freiburg: ContraLegem 2019, S. 274-282 (280), https://www.contralegem.ch/2019-2-l-medizin-und-digitalisierung-(e-health)

71 https://www.bundesregierung.de/breg-de/themen/digitalisierung/datenstrategie-1693546

Entdeckungsfall mit Bußgeldern zu ahnden, ließen sich Fahrzeuge mit autonomen und vernetzten Systemen von vornherein so gestalten, dass ein Verstoß gegen die Verkehrsordnung unmöglich wäre. Derartige Fahrzeuge könnten gar nicht mehr mit 150 Kilometern pro Stunde in einer Innenstadt unterwegs sein, weil eine mit der Verkehrsüberwachung betraute KI sie schon lange vor Erreichen dieser Geschwindigkeit abbremsen würde.[72]

Im angelsächsischen Schrifttum werden ähnliche Probleme gelegentlich unter dem Stichwort »impossibility structures« behandelt.[73] Dieser Begriff dürfte die Problematik allerdings kaum angemessen bezeichnen, denn es geht meist nicht darum, Fehlverhalten ganz unmöglich zu machen, sondern nur darum, es zu erschweren beziehungsweise zu dokumentieren. So wäre es im obigen Beispiel eines autonomen und vernetzten Fahrzeugs fatal, wenn der Wagen unter keinen Umständen mehr die vorgeschriebene Höchstgeschwindigkeit überschreiten könnte. In Notfällen, etwa bei einem Krankenhaustransport, muss es möglich sein, die von der KI gezogene Grenze zu überwinden. Allerdings sollten solche Fälle automatisch dokumentiert werden, sodass sie später (juristisch) auf ihre Berechtigung überprüft werden können. Dabei sollten die technischen Möglichkeiten einer Notfall-Übersteuerung durchaus unterschiedlich ausgestaltet sein; zum Beispiel sollte die Überwindung eines »Alkolocks« (Wegfahrsperre bei Alkoholisierung des Fahrers oder der Fahrerin) nur gelingen, wenn er oder sie durch Ausschalten einer entsprechenden Sicherung die eigene Fahrtauglichkeit bewiesen hat.

Wie die Beispiele zeigen, wird es also im Regelfall nicht um die 100-prozentige faktische Verhinderung von Fehlverhalten gehen, sondern um seine Erschwerung. Es handelt sich meist um »safety by default«-Einstellungen, die eine mehr oder weniger starke Präventionswirkung besitzen. Denkbar ist sogar, dass eine überwachende KI sich auf Informationen, Warnhinweise oder (mehr oder weniger stark ausgestaltete) Anreize zu korrektem Verhalten beschränkt. Gemeinsam ist allen diesen Fällen, dass das Fahrverhalten technisch überwacht und zum Wohle des Fahrers beziehungsweise der Fahrerin und Dritter gesteuert wird. Man kann die hier einschlägige Problemklasse deshalb als »technologischen Paternalismus« bezeichnen.[74]

---

72 Im Flugverkehr sind derartige Technologien schon seit Langem im Einsatz.

73 Siehe hierzu auch den Beitrag von Timo Rademacher und Erik Schilling in diesem Band.

74 E. Hilgendorf: Offene Fragen der neuen Mobilität: Problemfelder im Kontext von automatisiertem Fahren und Recht, S. 92.

Technologischer Paternalismus wirft eine Fülle von Problemen auf: Zwar vermag die Technik, Leben und andere wichtige Rechtsgüter zu schützen, technologischer Paternalismus impliziert aber eine weitreichende, unter Umständen dauerhafte Beobachtung von Personen in risikoträchtigen Situationen (etwa im Straßenverkehr oder bei chirurgischen Eingriffen). Dies führt, neben datenschutzrechtlichen Bedenken, zu grundsätzlichen Fragen nach unserem Freiheits- und Autonomieverständnis. Darüber hinaus geht es um die Belange des Gemeinwohls, das durch einen verstärkten Einsatz intelligenter Technik zur Risikokontrolle und Risikoverhinderung erheblich befördert werden könnte. Problematisch ist weiter, dass vernetzte Technik stets gehackt und manipuliert werden kann. Aus einer philosophisch-theologischen Perspektive ließe sich schließlich fragen, ob sittliches Verhalten nicht die faktische Möglichkeit von Fehlverhalten voraussetzt.

3.7 Private Quasi-Monopole und der Bedeutungsverlust des Staates

Europäische Werte werden sich in der digitalisierten und damit global vernetzten Welt nur dann durchsetzen lassen, wenn hinreichend viele Menschen sie nicht nur theoretisch befürworten, sondern auch im realen Leben praktisch unterstützen. Solange ohne viel nachzudenken auf die Angebote US-amerikanischer Quasi-Monopolisten zurückgegriffen wird, sind die Chancen, europäische (Wert-)Vorstellungen zur Geltung zu bringen, vom guten Willen der US-Anbieter abhängig, selbst wenn die EU zunehmend versucht, europäisches Recht dem entgegenzustellen. Auch in der digitalisierten Welt sind Monopole gefährlich.[75] Um die Orientierung der staatlichen Ordnung auf das Gemeinwohl zu wahren und unsere sozialen Werte zu verteidigen, wäre es oft sinnvoll, europäische Anbieter zu wählen, die den rechtlichen Vorgaben Europas uneingeschränkt unterworfen sind. Es geht also nicht darum, von Staats wegen Konkurrenzangebote zu den US-Tech-Giganten aufzubauen. Staatliche Stellen sollten aber genau prüfen, ob bestimmte Aufgaben nicht auch von einem europäischen Anbieter angemessen erfüllt werden könnten.[76]

Leider steht dem bislang unsere Bequemlichkeit entgegen. Selbst die Regierungen Europas sind in dieser Hinsicht vor Fehlern nicht gefeit. Ein

75 Ramge, Thomas: Mensch und Maschine. Wie Künstliche Intelligenz und Roboter unser Leben verändern, Ditzingen: Reclam 2018, S. 87f.

76 So dürfte das europäische Übersetzungsprogramm DeepL mit den meisten anderen einschlägigen Angeboten gut mithalten können.

gutes Beispiel ist die Corona-Warn-App, die ursprünglich als europäische Entwicklung geplant war. Nachdem Akzeptanz-Probleme auftraten, wurde in Deutschland eine enge Anbindung an die US-Tech-Riesen Apple und Google vollzogen, wobei als Argument auch ein besserer Datenschutz (!) genannt wurde. Die europäische Lösung wurde fallengelassen, und auch die Möglichkeit betriebssystemunabhängiger Lösungen nicht mit dem nötigen Nachdruck verfolgt. Die von der Regierung enorm gehypte Corona-Warn-App hat sich inzwischen als stumpfes Schwert im Kampf gegen die Pandemie erwiesen. Nicht nur ältere Smartphones konnten sie zunächst nicht nutzen, auch auf neueren Modellen des chinesischen Konkurrenzanbieters Huawei war die App nicht einsetzbar. Hier wird deutlich, wie die unkritische Orientierung an den marktbeherrschenden Unternehmen dazu führt, deren Standards und damit deren Dominanz weiter zu stärken.

Besonders problematisch ist, dass in der digitalisierten Welt immer mehr traditionell staatliche Aufgaben an private Anbieter übertragen werden, etwa die Bereitstellung und Sicherung der Kommunikationsinfrastruktur (wie E-Mail), Zahlungsdienste und digitale Währungen, die Sicherung von Dokumenten in Clouds, sogar hoheitliche Aufgaben, wie die Sicherung von (digitalen) Identitäten usw. Viele Menschen achten nur auf das Funktionieren der Angebote und übersehen, dass der Staat grundsätzlich als Anbieter in anderer Weise gebunden ist als Private: Der Staat besitzt einen Versorgungsauftrag, er ist für die Daseinsvorsorge zuständig und unterliegt demokratischer Kontrolle und Steuerung. Bei privaten Mega-Unternehmen, noch dazu solchen, die aus dem Ausland agieren, ist dies nicht so. Zwar lassen sich manche staatliche Bindungen auf Private übertragen, doch sind diese stets fragil und müssen oft erst durchgesetzt werden. Deshalb ist es umso wichtiger, dafür zu sorgen, dass der Staat in der digitalisierten Welt nicht noch weiter geschwächt wird.[77]

77 Grundlegend hierzu Schallbruch, Martin: Schwacher Staat im Netz. Wie die Digitalisierung den Staat in Frage stellt, der überzeugend herausarbeitet, wie staatliche Instanzen (gerade in Deutschland) oft selbst daran mitwirken, ihren Einfluss abzubauen; überaus kritisch gegenüber den US-Tech-Giganten auch ebd. P. Nemitz/M. Pfeffer: Prinzip Mensch. Macht, Freiheit und Demokratie im Zeitalter der Künstlichen Intelligenz, S. 301ff. und passim.

IV Zusammenfassung

Die in den Jahren 2019 und 2020 von der HLEG AI vorgestellten Leitlinien für eine vertrauenswürdige KI gehen einen Mittelweg zwischen einem bloßen akademischen Ethik-Kodex und nur partikular geltenden betrieblichen Compliance-Regeln. Vielmehr wurde versucht, auf der Grundlage der Menschenwürdegarantie und der europäischen Menschenrechtskataloge ethische Leitlinien zu formulieren, die hinreichend konkret und praktikabel sind, um auch in Unternehmen tatsächlich angewendet zu werden. Auf diese Weise ist es gelungen, akzeptanzfähige Grundlagen für konkrete Regulierungsmaßnahmen in Europa zu formulieren. Die ethische und rechtliche Einhegung der KI muss allerdings fortlaufend neuen technischen Entwicklungen angepasst werden, um den Vorrang des Gemeinwohls gegen kommerzielle oder hegemoniale Interessen zu verteidigen. Die Leitlinien der EU zur Regulierung von KI sollte man deshalb nicht als den Abschluss von Regulierungsüberlegungen verstehen, sondern als ihren Ausgangspunkt.

2.2.3 Geschlechtergerechtigkeit
Intersektionale Perspektiven auf den Digital Gender Gap

Francesca Schmidt und Nicole Shephard

Die Digitalisierung verändert unsere Arbeits- und Lebenswelten seit geraumer Zeit grundlegend. Über die technologischen und wirtschaftlichen Chancen und Risiken der digitalen Transformation wird inzwischen eine breite politische und gesellschaftliche Debatte geführt. Die Wechselwirkungen zwischen Digitalisierungsprozessen und Geschlechterverhältnissen werden dabei noch zu häufig ausgeblendet. Verschiedene Ebenen von Vergeschlechtlichung zeugen jedoch von der digitalen (Re-)Produktion sozialer Ungleichheiten: digitale Gewalt, blinde Flecken für Diskriminierungen bei automatisierten Entscheidungssystemen oder die unterdurchschnittliche Vertretung von Frauen, nicht-*weißen*[1] oder queeren Menschen, und zwar überall da, wo digitale Technologien entstehen und angewendet werden. All diese Phänomene verstärken vorhandene sozio-ökonomische Benachteiligungen und Ausgrenzungen.

Der sogenannte Digital Gender Gap[2] existiert nach wie vor, wie sich mithilfe des D21-Digital-Indexes belegen lässt, der einen Hinweis auf den Digitalisierungsgrad der deutschen Gesellschaft gibt. Dabei werden vier Berei-

1 Wir verwenden für *weiß* oder *weiß-sein* immer die kleine und kursive Schreibweise. Denn anders als Schwarz ist es kein Begriff für eine politisch empowernde Selbstdarstellung. Zudem verweist diese Schreibweise von *weiß* oder *weiß-sein* auf die üblicherweise unmarkierten Differenzmarkierungen sozialer Konstruktionen. Vgl: Eggers, Maureen Maisha et al.: »Konzeptionelle Überlegungen«, in: Eggers, Maureen Maisha et al. (Hg.), Mythen, Masken und Subjekte. Kritische Weißseinsforschung in Deutschland, Münster: Unrast 2005, S. 11-13.

2 Der Digital Gender Gap bezeichnet digitale Ungleichheiten zwischen Geschlechtern, zum Beispiel im Zugang zu digitalen Technologien, in der Kompetenz im Umgang mit ihnen und in ihrer Gestaltung.

che berücksichtigt: der Zugang zu digitalen Technologien, das Nutzungsverhalten, die Digitalkompetenz und die Offenheit gegenüber digitalen Trends. Gesamtgesellschaftlich liegt der durchschnittliche Digitalisierungsgrad bei 55 (von 100 möglichen) Punkten. In allen vier Bereichen zeigen sich Unterschiede zwischen den Geschlechtern im Umfang von 6 bis 12 Punkten. Insgesamt erreichen Frauen einen Digitalisierungsgrad von 51 gegenüber Männern mit 61 Indexpunkten. Frauen sind in der Gruppe der »digital Abseitsstehenden« überproportional vertreten, während die Gruppe der »digitalen Vorreiter« überwiegend männlich besetzt ist.[3]

Der Corona-Pandemie wird ein regelrechter Digitalisierungsschub nachgesagt,[4] denn aktuell verlagern sich für mehr Menschen mehr Lebensbereiche in digitale Räume als je zuvor. Das gilt beispielsweise für Arbeit und Bildung, das Aufrechterhalten sozialer Kontakte oder die Freizeitgestaltung. Um dadurch Fortschritte bei der Geschlechtergerechtigkeit nicht rückgängig zu machen und bereits benachteiligte Bevölkerungsgruppen nicht zusätzlich zu marginalisieren, ist es gerade jetzt besonders wichtig, die Digitalisierungsdebatte intersektional zu führen.

In diesem Beitrag erläutern wir zunächst die intersektionale Perspektive, an der wir uns orientieren. Um Geschlechtergerechtigkeit und Digitalisierung durch feministische Werte zu filtern, greifen wir danach Erkenntnisse aus der Geschichte des Technofeminismus auf. Im Anschluss beleuchten wir mittels dreier aktueller Themenfelder, wie Geschlechterfragen die digitalisierte Gegenwart prägen: digitale Gewalt, algorithmische Diskriminierung und Vielfalt in Technologie und Technologiesektor. Abschließend rufen wir zu einer intersektionalen Perspektive auf, die einen gemeinwohlorientierten Gestaltungsrahmen einer digitalisierten Gesellschaft ermöglicht.

3 Initiative D21: Digital Gender Gap: Lagebild zu Gender(un)gleichheiten in der digitalisierten Welt 2019. https://initiatived21.de/publikationen/digital-gender-gap/

4 Vgl. Streim, Andreas/Zacharias, Fabian: »Corona sorgt für Digitalisierungsschub in deutschen Haushalten«, in: Bitkom e.V. 2021. https://www.bitkom.org/Presse/Presseinformation/Corona-sorgt-fuer-Digitalisierungsschub-in-deutschen-Haushalten

Geschlechtergerechtigkeit intersektional gedacht

Gesellschaftliche Konstrukte[5] wie Geschlecht und *Rasse*, aber auch soziale Herkunft, sexuelle Orientierung, Alter, Behinderung oder Religion treten oft miteinander verschränkt auf. Diskriminierungs- und Ausgrenzungserfahrungen können sich deshalb auch unterschiedlich für Menschen äußern, die gleichzeitig in verschiedene Differenzkategorien eingeordnet werden.

Intersektionalität wurde durch die afroamerikanische Rechtswissenschaftlerin Kimberlé Crenshaw benannt und konzeptualisiert.[6] Sie zeigte anhand verschiedener Diskriminierungsfälle, dass die spezifischen Erfahrungen afroamerikanischer Frauen am Arbeitsplatz in der Rechtsprechung kaum Gehör fanden. Um eine Diskriminierung vor Gericht geltend zu machen, musste jeweils Diskriminierung aufgrund genau einer rechtlich geschützten Kategorie belegt werden. Dies gestaltete sich oft schwierig, da die Diskriminierungserfahrungen afroamerikanischer Frauen sowohl von der genderbasierten Diskriminierung *weißer* Frauen als auch von der rassistischen Diskriminierung Schwarzer[7] Männer abweichen. Diskriminierungserfahrungen, die auf der Gleichzeitigkeit von Geschlecht und *Rasse* beruhen, wurden so oft unsichtbar. Das Potenzial für Mehrfachdiskriminierung beschränkt sich dabei auch nicht auf *Rasse* und Geschlecht. Sie kann situativ und kontextuell auch viele andere Differenzkategorien betreffen.[8]

---

5 Zu Fragen der Konstruktion vs. Biologie vgl. Butler, Judith: Das Unbehagen der Geschlechter, Frankfurt a.M.: Suhrkamp 1991.

6 Crenshaw, Kimberlé: »Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics«, in: University of Chicago Legal Forum 1989, S. 139-167; Crenshaw, Kimberlé: »Mapping the Margins: Intersectionality, Identity Politics, and Violence Against Women of Color«, in: Stanford Law Review 43/6 1991, S. 1241-1299.

7 Der Begriff Schwarz wird im Folgenden immer groß geschrieben, um das von People of Color und Schwarzen Menschen eingeschriebene Widerstandspotenzial zu verdeutlichen. Vgl. Eggers, Maureen Maisha et al.: »Konzeptionelle Überlegungen«, in: Eggers, Maureen Maisha et al. (Hg.), Mythen, Masken und Subjekte. Kritische Weißseinsforschung in Deutschland, Münster: Unrast 2005, S. 11-13.

8 Vgl. Lutz, Helma, Maria Teresa Herrera Vivar und Linda Supik (Hg.): Fokus Intersektionalität: Bewegungen und Verortungen eines vielschichtigen Konzeptes, Wiesbaden: Springer VS 2010; Winker, Gabriele und Nina Degele (Hg.): Intersektionalität: Zur Analyse sozialer Ungleichheiten, Bielefeld: transcript 2009; Knapp, Gudrun-Axeli und Angelika Wetterer (Hg.): Achsen der Differenz. Gesellschaftstheorie und feministische Kritik, Münster: Westfälisches Dampfboot 2003.

Seither hat Intersektionalität sich nicht nur als Paradigma in der Geschlechterforschung durchgesetzt, sondern wird in der Sozialforschung interdisziplinär und grenzübergreifend angewendet. Auch außerhalb der Wissenschaften erfährt das Konzept inzwischen viel Beachtung, zum Beispiel in sozialen Bewegungen, in internationalen Organisationen und immer öfter auch in der Privatwirtschaft und der Politik. Die EU-Strategie zur Gleichstellung der Geschlechter 2020-2025 zum Beispiel bekennt sich neben dem Gender Mainstreaming nun auch zu einer intersektionalen Perspektive in allen EU-politischen Belangen.[9]

Eine Geschlechterperspektive alleine reicht also nicht aus. Um mehrschichtige Ausgrenzungen in Digitalisierungsprozessen und in der Technologie-Entwicklung und -Produktion zu erfassen, ist eine intersektionale Perspektive notwendig, die unterschiedliche Differenzkategorien im Blick behält. Denn Geschlecht ist nicht synonym mit Frau zu setzen, und nicht jede Frau ist eine *weiße* heterosexuelle cisgender[10] Frau.

Gender und Technologie: Eine kurze Geschichte

Die Verhandlung von Technologie und Geschlecht ist nicht neu, sondern folgt einer langen wissenschaftlichen und auch aktivistischen Tradition. Technofeminismus wurde von Judy Wajcman, einer australischen Soziologin, geprägt. Cyberfeminismus geht hingegen auf eine Reihe von Künstler*innen zurück, insbesondere auf das australische Kollektiv VNS Matrix mit ihrem cyberfeministischen Manifest.[11] Wissenschaftlich wurden der Begriff und die Bewegung beispielsweise durch die US-amerikanische Biologin Donna Haraway beeinflusst, vor allem durch ihre Überlegungen zur Figur der*des Cyborg. Wajcman schreibt, dass »[…] cyberfeminism needs to be understood as a reaction to the pessimism of the 1980s feminist approaches that stressed the inherently masculine nature of technoscience. In contrast, cyberfeminism emphasizes women's subjectivity and agency, and the pleasure immanent in digital technologies.«[12] Nach Wajcman ist Technologie sowohl Ursache als auch

9 Europäische Kommission: *Eine Union der Gleichheit: Strategie für die Gleichstellung der Geschlechter 2020-2025*, Brüssel: Europäische Kommission 2020.

10 Cisgender bezeichnet Menschen, die sich aktuell mit demselben Geschlecht identifizieren, das ihnen bei der Geburt zugeschrieben wurde.

11 https://vnsmatrix.net/projects/the-cyberfeminist-manifesto-for-the-21st-century

12 Wajcman, Judy: TechnoFeminism. Cambridge: Polity Press 2004, S. 63

Konsequenz von Geschlechterverhältnissen. So sind Geschlechterverhältnisse in Technologie materialisiert und Geschlecht wiederum erhält seine Bedeutung durch dessen Einschreibung und Einbettung in Technologie.[13] Technologie kann demnach nicht als neutral verstanden werden. Auch nicht mit dem Verweis darauf, dass Diskriminierung durch eine vermeintlich neutrale Technologie nicht stattfinden kann.

Mit der Figur der*des Cyborgs geht Haraway[14] noch einen Schritt weiter als Wajcman, wenn sie nicht nur die Bedingtheit und jeweilige Eingeschriebenheit, also von Geschlecht in Technologie und Technologie in Geschlecht, betont, sondern vielmehr die Trennung zwischen Mensch und Maschine vollkommen aufhebt. Die Figur der*des Cyborgs steht für ein hybrides Verhältnis von Mensch und Maschine. Im gleichen Zuge löst diese Figur auch die binäre Codierung von Geschlecht auf und ermöglicht somit den Traum eines Internets, das frei ist von diskriminierenden Strukturen. Feminist*innen unterstützten diese Idee, kritisierten sie jedoch auch von Anfang an scharf. Denn aus feministischer Perspektive wurde schnell widerlegt, dass das Internet quasi ein körperloser Ort ist. Sandy Allucquére Stone, eine US-amerikanische Akademikerin, Medientheoretikerin, Autorin und Performancekünstlerin, sieht in dem Verzicht beziehungsweise dem Vergessen des Körpers im Internet das Vergessen von minoritären Positionen, also genau jenen, die auch in der *analogen* Welt Diskriminierung und Ausschlüsse, vor allem nach intersektionalen Gesichtspunkten, erfahren.[15] Die ursprüngliche Hoffnung, dass ein *Raum* inklusiver sei, weil äußere Merkmale, wie zum Beispiel Geschlecht, *Rasse* oder Alter, keine Rolle spielen, erwies sich als trügerisch. Denn Macht- und Herrschaftsverhältnisse wurden damit sozusagen *unsichtbar* in das Internet übertragen. Inklusiv wurde der Raum nur für den auch in der analogen Welt unmarkierten Körper, der *weiß* und männlich ist und der Heteronorm[16] entspricht. Rosi Braidotti, italienische Philosophin,

13 Vgl. ebd., S. 107.

14 Haraway, Donna: »A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century«, in: Haraway, Donna: Simians, Cyborgs and Women: The Reinvention of Nature. New York: Routledge 1991, S. 149-181.

15 Vgl. Stone, Allucquère Rosanne: »Würde sich der wirkliche Körper bitte erheben? Grenzgeschichten über virtuelle Kulturen«, in: Peters, Kathrin und Andrea Seier (Hg.), Gender & Medien-Reader, Zürich/Berlin: Diaphanes 2016, S. 225-248.

16 Peter Wagenknecht beschreibt den Begriff treffend: »Der Begriff benennt Heterosexualität als Norm der Geschlechterverhältnisse, die Subjektivität, Lebenspraxis, symbolische Ordnung und das Gefüge der gesellschaftlichen Organisation strukturiert.

plädiert gar dafür, den Körper zu nutzen, um Diskriminierung im und über das Internet hinaus nicht nur benenn- und sichtbar zu machen, sondern den Raum auch zu nutzen, um Körper und Körperlichkeit neu zu verhandeln. Damit schließt sie an Haraways Gedanken zur*zum Cyborg an.[17]

Wie zeitgemäß diese Verhandlungen, Konzepte und Ideen sind, zeigen gegenwärtige Debatten auf zwei Ebenen: einerseits Diskussionen zur Diskriminierung im Internet, Beleidigungen und Drohungen beispielsweise durch digitale Gewalt oder Benachteiligungen durch automatisierte Entscheidungssysteme (künstliche Intelligenz); andererseits die visionären Debatten darüber, welches Potenzial digitale Technologien zum Neu-Denken gesellschaftlicher Strukturen haben.

Gegenwärtige Debatten zu Gender und Digitalisierung

Auf diese aktuellen Phänomene gehen wir im Folgenden intensiver ein und untersuchen, wie Geschlechterfragen den Umgang mit und die Gestaltung von Technologien prägen. Dabei betrachten wir Formen der digitalen Gewalt, algorithmische Diskriminierungen sowie den Bereich Vielfalt (*diversity*) im Technologiesektor.

Die Heteronormativität drängt die Menschen in die Form zweier körperlich und sozial klar voneinander unterschiedener Geschlechter, deren sexuelles Verlangen ausschließlich auf das jeweils andere gerichtet ist. Heteronormativität wirkt als apriorische Kategorie des Verstehens und setzt ein Bündel von Verhaltensnormen. Was ihr nicht entspricht, wird diskriminiert, verfolgt oder ausgelöscht (so in der medizinischen Vernichtung der Intersexualität) – oder den Verhältnissen in ästhetisch-symbolischer Verschiebung dienstbar gemacht. In der Subjekt-Konstitution erzeugt Heteronormativität den Druck, sich selbst über eine geschlechtlich und sexuell bestimmte Identität zu verstehen, wobei die Vielfalt möglicher Identitäten hierarchisch angeordnet ist und im Zentrum der Norm die kohärenten heterosexuellen Geschlechter Mann und Frau stehen.«
Wagenknecht, Peter: »Was ist Heteronormativität? Zu Geschichte und Gehalt des Begriffs«, in: Hartmann, Jutta et al. (Hg.), Heteronormativität: Empirische Studien zu Geschlecht, Sexualität und Macht, Wiesbaden: VS Verlag für Sozialwissenschaften 2007, S. 17-34.

17 Braidotti, Rosi: »Cyberfeminism with a difference«, in: Mui, Constance L. und Julien S. Murphy (Hg.), Gender Struggles: Practical Approaches to Contemporary Feminism, Lanham: Rowman & Littlefield 2002, S. 347-357.

Digitale Gewalt

Digitale Gewalt erscheint vielen als ein neueres Phänomen, ausgelöst durch die zahlreichen digitalen Kommunikationsmöglichkeiten vor allem in den sozialen Medien. Doch wovon sprechen wir eigentlich, wenn es um digitale Gewalt geht? Dieser Begriff fasst unterschiedliche Formen von Gewalt zusammen. So können sowohl Hatespeech, Online-Belästigungen (*online harassment)*, Cyberstalking, aber auch partnerschaftliche Gewalt, die mit digitalen Tools ausgeübt wird, als digitale Gewalt bezeichnet werden.[18] Es bleibt jedoch wichtig festzuhalten, dass all diese Begriffe unterschiedliche Formen digitaler Gewalt beschreiben, die dementsprechend vielschichtige Lösungsansätze benötigen und zum Teil als unterschiedliche Straftatbestände nach dem Strafgesetzbuch (z.B. Beleidigung oder Volksverhetzung) geahndet werden können. In diesem Artikel ist es uns nicht möglich, auf alle Formen in gleicher Tiefe einzugehen. Deshalb werden wir zwei in aller Kürze etwas näher vorstellen, über die auch gesellschaftlich zunehmend diskutiert wird.

Hatespeech ist mittlerweile ein gesellschaftlich breit genutzter Begriff, wenn es um kommunikative digitale Gewalt geht. Die Spanne reicht dabei von »einfachen Beleidigungen« bis hin zu Mord- und Vergewaltigungsdrohungen online. Die Gewalt bleibt jedoch nicht im digitalen Raum, wie der Fall Walter Lübke, aber auch der Mord an Ashley Arzaga[19] zeigen. Walter Lübke wurde aufgrund rechtsextremer Motive ermordet, Ashley Arzaga mutmaßlich aus Frauenhass. Beide Täter haben sich nachweislich im Internet und in den sozialen Medien radikalisiert.

Hatespeech ist vom Ministerkomitee des Europarates 1997 folgendermaßen definiert worden:

> »Jegliche Ausdrucksformen, welche Rassenhass, Fremdenfeindlichkeit, Antisemitismus oder andere Formen von Hass, die auf Intoleranz gründen, propagieren, dazu anstiften, sie fördern oder rechtfertigen, einschließlich der Intoleranz, die sich in Form eines aggressiven Nationalismus und Ethnozentrismus, einer Diskriminierung und Feindseligkeit gegenüber Min-

18 Vgl. Schmidt, Francesca: Netzpolitik: Eine feministische Einführung, 1. Auflage, Leverkusen: Verlag Barbara Budrich 2020.

19 Vgl. Pickert, Bernd: Anklage gegen Frauenmörder in Kanada: »Incel«-Mord gilt als Terrorismus, in: taz.de 2020. https://taz.de/Anklage-gegen-Frauenmoerder-in-Kanada/!5687349/

derheiten, Einwanderern und der Einwanderung entstammenden Personen ausdrückt.«[20]

Die Definition ist nach wie vor aktuell. Auch wenn sie nicht explizit auf digitale Inhalte abzielt, ändert sich doch nichts an den grundlegenden Mechanismen von Diskriminierung und Gewalt, wenngleich die Digitalisierung neue Formen hervorgebracht hat.

Aus feministischer Perspektive fällt trotzdem sofort auf, dass sexistische, homo- oder transphobe, ableistische[21] oder klassistische[22] Äußerungen nicht explizit genannt werden, jedoch unter »andere Formen von Hass« mitgedacht werden können. Das ist besonders für einen intersektionalen Blick wichtig, denn die unterschiedliche Betroffenheit lässt sich an diesen *fehlenden* Kategorien sehr gut beschreiben.

Digitale Gewalt gibt es schon seit Anbeginn des Internets. Sie kann potenziell jede Person treffen, so wie potenziell jede Person von Gewalt an sich betroffen sein kann. Wie vor allem internationale Studien zeigen, trifft digitale Gewalt aber nicht jede Person gleich. Das Risiko, Opfer digitaler Gewalt zu werden, ist entlang verschiedener, intersektional miteinander verknüpfter Achsen der Ungleichheit und Diskriminierung verteilt. Menschen, die entlang dieser Achsen im *analogen* Leben Gewalt erfahren, werden sie wahrscheinlich auch im Internet erfahren. Dies kann zum Verlust von Teilhabe am öffentlichen Raum Internet führen, aber auch zu psychischen Folgen wie Depressionen oder Angststörungen.[23]

Wenngleich digitale Gewalt schon in den 1990er Jahren aus feministischer Perspektive untersucht und besprochen wurde, nimmt die Forschung erst in

20 Europarat Ministerkomitee: Empfehlung Nr. R(97) 20 des Ministerkomitees an die Mitgliedsstaaten über die »Hassrede«, Europarat Ministerkomitee 1997. https://www.egmr.org/minkom/ch/rec1997-20.pdf

21 Ableismus beschreibt eine Ungleichbehandlung aufgrund körperlicher oder psychischer Beeinträchtigung.

22 Klassismus bezeichnet die Diskriminierung aufgrund der sozialen Herkunft und/oder der sozialen und/oder ökonomischen Position. Klassismus richtet sich mehrheitlich gegen Personen einer *niedrigeren* Klasse.

23 Vgl. Citron, Danielle Keats: Hate Crimes in Cyberspace, Cambridge, Mass: Harvard University Press 2014; Herring, Susan et al.: »Searching for Safety Online: Managing ›Trolling‹ in a Feminist Forum« in: The Information Society 18 2002, S. 371-384; Fawzi, Nayla: Cyber-Mobbing: Ursachen und Auswirkungen von Mobbing im Internet, 2., durchgesehene Auflage, Baden-Baden: Nomos 2015.

den letzten Jahren stetig zu[24] und ermöglicht es so, Lösungsansätze zu entwickeln.

Dies trifft allerdings nur sehr bedingt auf Deutschland zu, denn hier fehlen bisher Zahlen, die sich auch nach intersektionalen Gesichtspunkten auswerten lassen. Dennoch werden die vorhandenen Studien für die politische Arbeit genutzt. So wurde zwar in der Studie des Instituts für Demokratie und Zivilgesellschaft allgemein festgestellt, dass Hatespeech die Meinungsfreiheit im Netz einschränkt, aber es ist eben keine differenzierte Aussage über Betroffenheit(en) möglich. Zunächst wird Hatespeech als »Aggressive oder allgemein abwertende Aussage[] gegenüber Personen, die bestimmten Gruppen zugeordnet werden […]«[25] gefasst. Individuelle Formen der Herabsetzung werden explizit ausgeschlossen, da es weniger um Emotionen als vielmehr um »negative Vorurteile gegenüber spezifischen Gruppen von Menschen« gehe. Allerdings lässt sich die individuelle nicht von einer strukturellen Ebene, etwa einer Gruppenzugehörigkeit, trennen. Das wissen viele Betroffene digitaler Gewalt. Denn Mord- und Vergewaltigungsdrohungen mögen zwar im ersten Moment individuell erscheinen, speisen sich aber aus kulturellen und gesellschaftlichen Normen sexualisierter Gewalt gegen Frauen im Allgemeinen. In der Studie wird schließlich festgehalten, dass Menschen mit Migrationshintergrund mehr Hatespeech erfahren. Diese Gruppe wird aber nicht weiter nach Geschlecht, Alter oder sexueller Identität aufgeschlüsselt.

Nach dieser Studie sind mehr Männer von Hatespeech betroffen, welche Form die Hasskommentare haben, bleibt aber offen. Ebenso wird grundsätzlich benannt, worauf sich die Hassrede bezieht, aber nicht, für wen welcher Bezug relevant war. Erfahren also mehr Frauen Hassrede in Bezug auf ihr Geschlecht, oder sind es Männer? Welche Formen von Hassrede erleiden migrantisierte Frauen? Bleibt es also bei der allgemeinen Aussage, dass Hatespeech »ein schleichender Angriff auf die Demokratie« ist? Und damit bei der unspezifischen Forderung nach besser ausgestatteten Polizei-, Justiz- und Beratungsbehörden? Wissen beispielsweise um die Funktionsweisen von Sexismus und Rassismus (auch in ihrer Verschränkung) ist mindestens genauso wichtig. Wenn jedoch Studien die Fälle nicht abbilden, werden die notwendigen Lösungsansätze nicht in politische Prozesse übersetzt.

---

24 Vgl. Ganz, Kathrin: »Hate Speech im Internet« in: Dorer, Johanna et al. (Hg.): Handbuch Medien und Geschlecht, Wiesbaden: Springer Fachmedien 2019, S. 1-10.

25 Institut für Demokratie und Zivilgesellschaft (IDZ) (Hg.): #Hass im Netz: der schleichende Angriff auf unsere Demokratie, Jena: IDZ 2019, S. 15.

Internationale Untersuchungen zeigen dagegen, wie sich digitale Gewalt intersektional auswirkt. Für Aufsehen sorgte vor einigen Jahren die Auswertung von 1,4 Millionen Kommentaren auf der Seite des *Guardian*, einer britischen Nachrichten- und Medienwebseite. Demnach sind Frauen und Frauen *of Color*[26] besonders von Hatespeech betroffen. Obwohl mehr *weiße* Männer für die Online-Ausgabe schreiben, richten sich die Kommentare in ihrer Vehemenz und Brutalität jedoch überproportional häufig gegen Artikel von Frauen und Schwarzen Menschen. Von den zehn Journalist*innen, die regelmäßig digitale Gewalt erfahren und auch regelmäßig für den *Guardian* schreiben, sind acht Frauen (vier *weiß* und vier of Color) am schwersten von digitaler Gewalt betroffen. Auch die Kategorien sexuelle Identität und Religion scheinen eine Rolle zu spielen. Zwei der acht Frauen sind homosexuell, eine ist Muslima und eine Jüdin.[27]

2020 hat Plan International untersucht, wie Mädchen und junge Frauen von digitaler Gewalt weltweit betroffen sind.[28] Befragt wurden über 14.000 Mädchen und junge Frauen in Ländern wie Brasilien, Indonesien, Tansania, USA, Spanien und Deutschland. 58 Prozent der Befragten gaben an, irgendeine Form digitaler Gewalt erfahren zu haben. Die meisten von ihnen berichteten über erste Erfahrungen mit Belästigungen in sozialen Medien im Alter von 14-16 Jahren. Insgesamt gaben 85 Prozent an, dass sie mehrere Arten von Belästigungen erlebt haben, nur 17 Prozent sagten, dass sie nur einer Art von Belästigung ausgesetzt waren, und 9 Prozent berichteten, dass sie jede genannte Belästigung erfahren haben.[29]

In der Studie wird zudem festgestellt, das Mädchen und junge Frauen angegriffen werden, allein weil sie online sind und sich damit im öffentlichen Raum bewegen. Die Gewalt steht oft in keinem Zusammenhang mit

26 Der Begriff Frauen *of Color* oder auch Personen *of Color* (PoC) ist, ähnlich wie Schwarz, eine Selbstbezeichnung von Menschen, die Rassismus erfahren. Dabei geht es nicht um Hautschattierungen, sondern um Marginalisierung aufgrund von Rassismus.

27 Vgl. Gardiner, Becky et al.: »The dark side of Guardian comments«, in: The Guardian 2016. https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments

28 Vgl. Plan International: Free To Be Online? Plan International 2020. https://plan-international.org/publications/freetobeonline

29 Beschimpfung und Beleidigung (59 Prozent); absichtliches Herstellen peinlicher Situationen (41 Prozent); Body Shaming (39 Prozent); Bedrohungen mittels sexueller Gewalt (39 Prozent); sexuelle Belästigung (37 Prozent); Stalking (32 Prozent); rassistische Kommentare (29 Prozent); Anti-LGBTIQ+-Kommentare (26 Prozent); Bedrohungen durch physische Gewalt (21 Prozent).

dem von ihnen geposteten Inhalt. Wenn sie aktivistisch oder politisch das Internet nutzen, werden sie ebenfalls angegriffen und ihnen wird das Recht auf (politische) Öffentlichkeit abgesprochen. Die Gewalterfahrung nimmt zu, wenn sie Schwarz sind, sich als LGBTIQ+[30] identifizieren oder eine Behinderung haben. All diese Ergebnisse zeigen auf, wie wichtig eine intersektionale Analyse von Gewaltverhältnissen im Allgemeinen und von digitaler Gewalt im Besonderen ist.

Der andere Bereich von digitaler Gewalt, der in diesem Rahmen noch kurz beleuchtet werden soll, ist partnerschaftliche Gewalt. Die Debatte hierzu ist vergleichsweise jung, zumindest was den digitalen Aspekt betrifft. Frauen, die partnerschaftlicher Gewalt ausgesetzt sind, erfahren diese zunehmend auch digital, zum Beispiel in Form sogenannter Spy-Apps, die Betroffene jederzeit orten, ausspionieren (Kameras) oder digitale Aktivitäten nachverfolgen können.[31] Das ist an sich bereits sehr problematisch. Die Gefahr potenziert sich jedoch, wenn Frauen beispielsweise in Frauenhäusern Schutz suchen und so unfreiwillig den geheimen Standort preisgeben, zumal das Problem oft selbst in den Fraueneinrichtungen noch unbekannt ist oder aber das technische Wissen um diese Apps fehlt. Auch in dem immer besser vernetzen Smart Home findet digitale Gewalt statt, indem die Technologie genutzt wird, um Frauen ein- oder auszusperren, das Licht an- oder auszuschalten oder die Smart Speaker auf volle Lautstärke zu bringen, ohne dass die betroffenen Frauen einen Einfluss darauf haben.[32] Die vermeintliche Befreiung durch Technologie wird in diesem Fall zur sprichwörtlichen Falle.

Für beide Phänomene gibt es Lösungsansätze, die in unterschiedlicher Intensität bereits umgesetzt werden. So werden Mitarbeitende in Frauenberatungsstellen entsprechend geschult. Grundsätzlich fehlt es aber an personellen und finanziellen Ressourcen, um diese Probleme in all ihren Auswirkungen anzugehen. Bei kommunikativer Gewalt wurde mit dem Netzwerk-

30 LGBTIQ+ steht als Akronym für Lesbian, Gay, Bisexual, Trans*, Intersexual, Queer, das Plus öffnet den Raum für weitere sexuelle Identitätsentwürfe. (Das deutsche Akronym LSBTIQ+ wird in der Community nur selten verwendet.).

31 Vgl. Peteranderl, Sonja: »Digitale Spione: Wie Frauen mit Spysoftware ausgespäht werden«, In: Der Spiegel 2019. https://www.spiegel.de/netzwelt/netzpolitik/spysoftware-wie-frauen-ausgespaeht-werden-a-1267225.html

32 Vgl. Bowles, Nellie: »Thermostats, Locks and Lights: Digital Tools of Domestic Abuse», in: The New York Times 2018; Tanczer, Leonie: »Das ›Internet der Dinge‹: Digitale Gewalt wird ›smart‹«, in: an.schläge 2018. https://anschlaege.at/das-internet-der-dinge-digitale-gewalt-wird-smart/

durchsetzungsgesetz (NetzDG) sogar eine neue Rechtsnorm geschaffen, deren tatsächlicher Nutzen, vor allem für die betroffenen Frauen, aber noch zu beweisen ist.[33]

Algorithmische Diskriminierung

Die Schnittstelle zwischen Daten, Algorithmen und Diskriminierung wird schon länger wissenschaftlich,[34] journalistisch[35] und auch zivilgesellschaftlich[36] bearbeitet. Von algorithmischer Diskriminierung ist dann die Rede, wenn die Ergebnisse algorithmischer Entscheidungssysteme und maschinellen Lernens Frauen und marginalisierte Personengruppen benachteiligen oder ausschließen. Das Besondere der datenbasierten und algorithmischen Diskriminierung ist, dass die zugrunde liegenden Datenverarbeitungsverfahren oft kaum transparent, das heißt kaum noch versteh- und erklärbar sind, und mehrheitlich indirekt diskriminieren. Sie zielen nicht direkt auf persönliche Merkmale wie Geschlechteridentität, *Rasse*, soziale Herkunft oder sexuelle Orientierung, sondern benachteiligen über Proxies, also über scheinbar neutrale Merkmale, die indirekt Rückschluss auf diskriminierungsrelevante Identitäten zulassen.[37] Gleichzeitig können algorithmische Entscheidungssysteme eine große gesellschaftliche Trag- und Reichweite haben, da sie zum Beispiel im Rechtssystem, im Bildungswesen, bei der Kreditvergabe, in der Personalbeschaffung großer Unternehmen oder auf globalen Online-Plattformen (insbesondere den soziale Medien) zum Einsatz kommen.

Wie algorithmische Diskriminierung in der Praxis aussehen kann, hat sich in den letzten Jahren immer wieder gezeigt, etwa wenn der Sensor am

33 Ebenfalls neu geschaffen wurde § 184k (StGB) Verletzung des Intimbereichs durch Bildaufnahmen zu Upskirting.

34 Vgl. Citron, Danielle K./Pasquale, Frank A.: »The Scored Society: Due Process for Automated Predictions« in: Washington Law Review 89 2014; Noble, Safiya Umoja: Algorithms of oppression: How search engines reinforce racism, New York: NYU Press 2018; O'Neil, Cathy: Weapons of Math Destruction: how big data increases inequality and threatens democracy, New York: CROWN 2016.

35 Vgl. Angwin, Julia et al.: »Machine Bias«, in: ProPublica 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Siehe auch https://www.propublica.org/series/machine-bias

36 Siehe zum Beispiel https://algorithmwatch.org/

37 Vgl. O'Neil, Cathy: Weapons of Math Destruction.

Seifenspender nur auf *weiße* Hände reagiert,[38] wenn Frauen weniger kreditwürdig erscheinen als Männer[39] oder wenn Gesichtserkennung für dunkelhäutige Frauen deutlich schlechter funktioniert als für *weiße* Männer.[40] In einer Studie des Georgia Institute of Technology wurde herausgefunden, dass selbstfahrende Fahrzeuge Fußgänger*innen mit heller Hautfarbe besser erkennen können als solche mit dunklerer Haut. Dabei lag die Erkennungsrate für Menschen mit hellerer Hautfarbe durchschnittlich um fünf Prozentpunkte über der für Menschen mit dunklerer Hautfarbe.[41] Es handelt sich hier also weder um ein theoretisches Problem noch um rein technische Unzulänglichkeiten, sondern um sehr konkrete Benachteiligungen, die sogar lebensgefährlich sein können.

Die Ursachen für algorithmische Diskriminierung können dabei vielschichtig sein. Bestehende Machtverhältnisse und Ausschlüsse können bereits in den Trainingsdaten abgebildet sein, die für maschinelles Lernen verwendet werden. Ein gutes Beispiel dafür, wie maschinelles Lernen bestehende Diskriminierung übernimmt und repliziert, lieferte Amazon. Ein internes Personalsystem sollte dabei helfen, Bewerbungen vorzusortieren und die jeweils besten Kandidat*innen vorzuschlagen. Allerdings hatte das System aus dem Fundus an Bewerbungen und Einstellungen der vergangenen zehn Jahre gelernt, dass technische Stellen wie Software-Entwickler durch Männer besetzt werden. In der Folge sortierte es Bewerbungen von Kandidatinnen aus, deren Lebenslauf etwa die Mitgliedschaft in Frauenorganisationen, einem Frauen-Sportteam oder ein Studium an einem Frauen-College enthielten. Nachdem dieser algorithmische Gender-Bias festgestellt worden war, wurde das geplante System aufgegeben.[42]

---

38 Vgl. Franken, Franziska/Bazrak, Dilara: »Wenn es für dich keine Seife gibt«, in: Technikjournal 2020. https://technikjournal.de/2020/08/27/wenn-es-fuer-dich-keine-seife-gibt/

39 Vgl. Gupta, Alisha Haridasani: »Are Algorithms Sexist?«, in: The New York Times 2019. https://www.nytimes.com/2019/11/15/us/apple-card-goldman-sachs.html

40 Vgl. Buolamwini, Joy/Gebru, Timnit: Gender Shades: »Intersectional Accuracy Disparities in Commercial Gender Classification Joy«, in: Proceedings of Machine Learning Research 81 2018.

41 Vgl. Wilson, Benjamin/Hoffman, Judy/Morgenstern, Jamie: »Predictive Inequity in Object Detection«, in: arXiv:1902.11097 2019.

42 Vgl. Dastin, Jeffrey: »Amazon scraps secret AI recruiting tool that showed bias against women«, in: Reuters 2018. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

Aber auch ein Mangel an Vielfalt in den Unternehmen und Teams, die algorithmische Entscheidungssysteme konzipieren und entwickeln oder den Output bewerten und verwenden, kann zu blinden Flecken führen. Schließlich wird maschinelles Lernen von Menschenhand entwickelt und betreut. Da geht es einerseits um die Vielfalt an Menschenkörpern, etwa im Sinne von Geschlechteridentitäten, ethnischer und sozialer Herkunft, sexueller Orientierung oder Behinderung, andererseits aber auch um die Vielfalt an Fachdisziplinen beziehungsweise eine engere Verschränkung der Computerwissenschaften mit den kritischen Science and Technology Studies und der Geschlechterforschung.

Algorithmische Entscheidungen beruhen notwendigerweise auf Korrelationen und der Annäherung an eine statistische Norm. Datenbeziehungen dieser Art können bestehende Machtverhältnisse und Diskriminierungsformen replizieren, besonders wenn die gesellschaftliche Vielfalt nicht angemessen berücksichtigt wird und die Norm, an der sich Algorithmen orientieren, primär jung, *weiß* und männlich ist. So bilden Algorithmen keine wertneutrale Zukunft ab, sondern sie zementieren bestehende gesellschaftliche Muster, Machtverhältnisse und Diskriminierungsformen.

Vielfalt in Technologie und Technologiesektor

Je digitalisierter sich die Wirtschaft gestaltet, je mehr wir für Bildung, Arbeit, politische Partizipation und soziales Leben auf digitale Dienste angewiesen sind, desto dringlicher stellt sich auch die Frage nach gleichberechtigter und inklusiver Teilhabe an und Gestaltung von digitalen Technologien. Dabei folgen digitale Ungleichheiten und Ausschlüsse oft bestehenden sozialen Ungleichheiten.[43]

Bereits sozial benachteiligte Menschen erleben in der digitalen Welt zusätzliche Benachteiligungen, wie einen durch fehlende finanzielle Mittel eingeschränkten Zugang zu digitalen Technologien, weniger Möglichkeiten, digitale Technologien anzuwenden oder fehlende Digitalkompetenz.[44] Vielfältige Faktoren wie Alter, Geschlecht, Bildungsstand, soziale Herkunft oder Ein-

43 Vgl. Robinson, Laura et al.: »Digital inequalities and why they matter«, in: Information, Communication & Society 18 2015, 569-582.

44 Vgl. Hargittai, Eszter: »View of Second-Level Digital Divide: Differences in People's Online Skills«, in: First Monday 2002. https://firstmonday.org/article/view/942/864

kommen kommen zusammen und beeinflussen die Möglichkeiten zur Teilhabe und digitale Ausschlüsse intersektional.

Ein aktuelles Beispiel liefern hier pandemiebedingte Lockdowns, besonders wenn ein Großteil der Bildung durch Schulschließungen plötzlich in den digitalen Raum verlegt wird. Kinder aus bildungsfernen Haushalten und Familien mit Migrationshintergrund werden durch diese Verschiebung besonders benachteiligt. Denn während Eltern aus bildungsnahen Milieus meist in der Lage sind, den Ausfall von Präsenzunterricht durch Homeschooling zu kompensieren, finden Kinder aus bildungsfernen Haushalten wenig Unterstützung.[45] Auch der Zugang zu (eigenen) Geräten, um am Online-Unterricht teilzunehmen und Aufgaben zu erledigen, oder ein ruhiger Arbeitsplatz für konzentriertes Lernen sind Voraussetzungen für die Chancengleichheit, die längst nicht allen Kindern gleichermaßen zuteilwerden.[46]

Nicht nur die Teilhabe an digitalisierten Lebensbereichen, sondern bereits die Gestaltung digitaler Räume und Technologien ist durch Ungleichheiten geprägt. Zurzeit liegt der Frauenanteil im deutschen Tech-Sektor bei gerade mal 17 Prozent. Das ist auch im europäischen Vergleich niedrig.[47] Der Gender Pay Gap in IT-Berufen liegt bei 7 Prozent.[48] Die digitalisierungs- und innovationslastige Start-up-Szene ist mit einem Gründerinnen-Anteil von knapp 16 Prozent nicht besser aufgestellt.[49] Und auch der Nachwuchsbereich ist männerdominiert: Der Frauenanteil beim Informatikstudium lag für das Studienjahr 2019/2020 bei knapp 22 Prozent,[50] und eine berufliche Ausbildung zur Fachinformatiker*in verfolgten per Ende 2019 nur 8 Prozent Frauen.[51]

---

45 Vgl. Anger, Christina/Plünnecke, Axel: »Schulische Bildung zu Zeiten der Corona-Krise«, in: Perspektiven der Wirtschaftspolitik 21 2020, 353-360.

46 Vgl. Packeiser, Karsten: »Internet-Unterricht erreicht sozial benachteiligte Kinder nicht«, in: MigAZIN 2020. https://www.migazin.de/2020/04/09/eine-katastrophe-internet-unterricht-kinder/

47 Anteil Frauen in der IT-Branche absolut und prozentual für ausgewählte europäische Länder siehe https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_sks_itsps&lang=en

48 Vgl. Zucco, Aline: Der Gender Pay Gap in IT-Berufen. Geschäftsstelle Dritter Gleichstellungsbericht der Bundesregierung 2020. https://www.dritter-gleichstellungsbericht.de/de/article/222.gender-pay-gap.html.

49 https://deutscherstartupmonitor.de/

50 Siehe https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bildung-Forschung-Kultur/Hochschulen/Tabellen/studierende-mint-faechern.html

51 Gemäß Datensystem Auszubildende des Bundesinstituts für Berufsbildung, https://www.bibb.de/de/2252.php

Beim Thema Vielfalt geht es aber um mehr als Frauenanteile. Denn während Frauen in der Technologie-Branche untervertreten sind, sind marginalisierte Gruppen wie Menschen *of Color*, trans* und queere Menschen oder behinderte Menschen wenig sichtbar. Die Zahlen zur Geschlechterungleichheit, wie auch das Fehlen greifbarer Zahlen zu anderen Ungleichheiten, verdeutlichen, wie dringend es weiterhin bleibt, da anzusetzen, wo Digitalisierung entsteht, nämlich beim Arbeitsmarkt und bei der Tech-Pipeline.

Damit die Digitalisierung einer möglichst breiten Bevölkerung zugutekommen kann, ist es wichtig, dass digitale Technologien auch *an sich* nicht diskriminieren und ausschließen.[52] Dass dies nicht immer der Fall ist, veranschaulichen die bereits erwähnten Fälle algorithmischer Diskriminierung. Zudem gibt es historisch wie auch aus jüngerer Zeit viele Technologien, die längst nicht für alle Menschen gleich gut funktionieren.

Farbfilm und -fotografie waren zum Beispiel seit ihrer Entstehung zu Beginn des 20. Jahrhunderts bis in die 1990er Jahre nicht in der Lage, Menschen mit dunkler Hautfarbe in guter Qualität darzustellen.[53] Auch bei der Spracherkennungssoftware als jüngeres Beispiel wurde der Benutzer*innenkreis zu klein gedacht. Sprachbasierte virtuelle Assistent*innen wie Apple's Siri, Amazon's Alexa oder Google's Assistant sind inzwischen zwar allgegenwärtig. Doch Forschung hat mehrfach belegt, dass Spracherkennungssoftware nicht nur männliche Stimmen deutlich besser erkennt als weibliche, sondern auch Schwierigkeiten hat, nicht-*weiße* Sprecher*innen zu verstehen, zum Beispiel bei unterschiedlichen Akzenten und Dialekten.[54] Etwas überspitzt formuliert bedeutet das, wer nicht wie ein *weißer* Mann Englisch spricht, wird von

52 Vgl. Perez, Caroline Criado: Invisible women. Exposing data bias in a world designed for men, London: Vintage Books 2019. Siehe zur Frage der Diskriminierung auch die Beiträge von Lorena Jaume-Palasí und Eric Hilgendorf in diesem Band.

53 Vgl. Caswell, Estelle: »Color film was built for white people. Here's what it did to dark skin«, in: Vox 2015. https://www.vox.com/2015/9/18/9348821/photography-race-bias;Roth, Lorna: »Looking at Shirley, the Ultimate Norm: Colour Balance, Image Technologies, and Cognitive Equity«, in: Canadian Journal of Communication 34 2009.

54 Vgl. Koenecke, Allison et al.: »Racial disparities in automated speech recognition«, in: Proceedings of the National Academy of Sciences 117 2020, 7684-7689; Tatman, Rachael: »Gender and Dialect Bias in YouTube's Automatic Captions«, in: Proceedings of the First ACL Workshop on Ethics in Natural Language Processing. Valencia, Spain: Association for Computational Linguistics 2017, S. 53-59; Rodger, James/Pendharkar, Parag: »A field study of the impact of gender and user's technical experience on the performance of voice-activated medical tracking application«, in: Int. J. Hum.-Comput. Stud. 60 2004, S. 529-544.

Spracherkennungssoftware häufiger missverstanden. Bei Siri oder Alexa ist das in erster Linie ärgerlich, ist doch der Benutzer*innenkreis deutlich vielfältiger. Aber Spracherkennung kommt auch in immer mehr Bereichen zum Einsatz, in denen solche Ungleichheiten schwerwiegender diskriminieren können, zum Beispiel im Berufsleben, bei Einwanderungsbehörden oder in der Personalbeschaffung.[55]

Vieles spricht dafür, dass vielfältige Teams auch inklusivere Technologien entwickeln. Das Zusammenspiel von Vielfalt in Unternehmen und Innovation ist längst belegt.[56] Und wenn ein vielfältiger Personenkreis an der Gestaltung von Digitalisierung mitwirkt, also wenn etwa Frauen, ältere Menschen, queere Menschen und nicht-*weiße* Menschen repräsentativ an Design und Entwicklung von Technologie beteiligt sind, liegt es nahe, dass blinde Flecken in den Ergebnissen reduziert werden.[57] Ein inklusives Arbeitsumfeld ist die Voraussetzung dafür, dass sich diese Vielfalt auch in der Praxis nachhaltig entfalten kann. Inklusion bedeutet, dass *alle* Mitarbeitenden nicht nur formal gleichberechtigt sind, sondern sich auch individuell zugehörig, sicher und gehört fühlen, um sich vollumfänglich einbringen zu können. Inklusion gestaltet sich als Zusammenspiel zwischen Faktoren wie der aktiven Gestaltung von Unternehmenskultur, gelebter Werte, der Führung, der Arbeitsplatzgestaltung oder der Kommunikation.[58]

Trotzdem garantiert das Vorhandensein von Vielfalt und Inklusion noch keine diskriminierungsfreie digitale Zukunft. Vielmehr müssen gesellschaftliche Vielfalt, bestehende soziale Ungleichheiten, Chancen und Risiken digitaler Technologien für unterschiedlich betroffene Personenkreise sowie für

55 Vgl. Bajorek, Joan Palmiter: »Voice Recognition Still Has Significant Race and Gender Biases«, in: Harvard Business Review 2019. https://hbr.org/2019/05/voice-recognition-still-has-significant-race-and-gender-biases

56 Vgl. Turner, Laure: »Gender diversity and innovative performance«, in: International Journal of Innovation and Sustainable Development 4 2009, 123-134; Charta der Vielfalt: Diversity Management. Mehrwert für den Mittelstand. Charta der Vielfalt 2017; Østergaard, Christian R./Timmermans, Bram/Kristinsson, Kari: »Does a different view create something new? The effect of employee diversity on innovation«, in: Research Policy 40 2011, 500-509.

57 Vgl. Peña, Mike: »Ignoring Diversity Hurts Tech Products and Ventures«, in: Stanford eCorner 2016. https://ecorner.stanford.edu/articles/ignoring-diversity-hurts-tech-products-and-ventures/

58 Vgl. Ferdman, Bernardo M./Deane, Barbara R.: Diversity at Work: The Practice of Inclusion, San Francisco: Jossey-Bass 2014.

das Design und die Entwicklung spezifischer Anwendungen konsequent zusammengedacht werden.

Digitalisierung intersektional denken

Ein intersektionaler Blickwinkel berücksichtigt nicht nur die geschlechtliche Identität, sondern gleichzeitig auch andere Kategorien der Differenzierung, wie zum Beispiel *Rasse*, soziale Herkunft oder sexuelle Orientierung, da diese in der Praxis oft miteinander verschränkt auftreten. Die Auseinandersetzung mit den Erkenntnissen des Technofeminismus der letzten Jahrzehnte zeigt, dass die Verhandlung der Vergeschlechtlichung von Technologie durch die Figur der*des Cyborgs und der Materialität von Körpern wie auch der digitalen Infrastruktur nicht an Aktualität verloren hat. Das Gegenteil ist der Fall, wie die aktuelle Aushandlung vergeschlechtlichter Digitalthemen verdeutlicht, etwa die allgegenwärtige digitale Gewalt, das Diskriminierungspotenzial in automatisierten Entscheidungssystemen oder der Mangel an Vielfalt und Inklusion in der Technologiebranche und in der Technik *an sich*.

Eine intersektionale Perspektive auf die Digitalisierung und ihre Auswirkungen ist nicht nur im Sinne der Geschlechtergerechtigkeit und zur Überwindung des Digital Gender Gaps dringend notwendig. Sie ermöglicht und erweitert vielmehr den politischen und zivilgesellschaftlichen Gestaltungsrahmen von Digitalisierung. So können wir an einem gemeinwohlorientierten, geschlechtergerechten Gesellschaftsentwurf arbeiten, der Technologie nutzt, um gesellschaftliche Einschlüsse statt Ausschlüsse zu gewährleisten.

2.2.4 Nachhaltigkeit

Wie Digitalisierung zur Sicherung existenzieller Menschenrechte und zur Klimagerechtigkeit beitragen kann

Tilman Santarius

Kann Nachhaltigkeit als Wert für den Digitalisierungsdiskurs und die Gestaltung der Digitalisierung fruchtbar gemacht werden? Nachhaltigkeit ist ein wertebasiertes Konzept, das unmittelbar relevant ist für das grundlegende Ziel des Gemeinwohls und für die Anliegen der Gerechtigkeit. Denn Nachhaltigkeit beruht schon per Definition auf normativen Zielen. Diese schließen die Erhaltung der planetaren Belastungsgrenzen ebenso ein (ökologische »Säule« der Nachhaltigkeit) wie intra- und internationale Gerechtigkeit und ein »Gutes Leben« auf individueller Ebene (soziale Dimensionen der Nachhaltigkeit).

In diesem Beitrag wird zunächst das Konzept der Nachhaltigkeit normativ festgeschrieben. Darauf aufbauend wird dann zum einen aufgezeigt, welche Nachhaltigkeitswerte eine gemeinwohlorientierte Gestaltung der Digitalisierung leiten sollten. Zum anderen wird skizziert, wie Digitalisierung dazu beitragen kann, globale Nachhaltigkeitsziele (etwa Klimaschutz) zu erreichen. Um hier eine noch spezifischere Fundierung einer werteorientierten Digitalisierung herauszuarbeiten, wird dabei ein Schwerpunkt auf vier Dimensionen der Klimagerechtigkeit gelegt und diskutiert, welche Chancen und Risiken Digitalisierung für Klimagerechtigkeit bereithält. Abschließend werden einige Politiken für eine nachhaltigkeitsorientierte Digitalisierung vorgestellt.

Nachhaltigkeit als wertebasiertes Konzept

Der Begriff *Nachhaltigkeit* hat eine lange Geschichte. Erstmals wurde er von Hans Carl von Carlowitz im Jahr 1713 mit Bezug zur Forstwirtschaft verwendet. Holz und Wälder waren in Europa zunehmend knapp geworden, und eine nachhaltige Forstwirtschaft sollte dafür sorgen, dass nur noch so viel Holz geschlagen wird, wie auch nachwachsen kann. Dieser Gedanke erwies sich als bahnbrechend, und seine Bedeutung ist seit dem letzten Viertel des 20. Jahrhunderts bis heute angestiegen.[1] Inzwischen gilt der Grundgedanke der Nachhaltigkeit von Holz auch für alle anderen knappen natürlichen Ressourcen – von Frischwasser über saubere Luft (z.B. in Städten, Industriegebieten) bis hin zu Seltenen Erden und anderen knappen Metallen, die für die Herstellung digitaler Geräte entscheidend sind. Er gilt aber auch für alle vom Verschleiß bedrohten, lokalen und globalen Ökosystemleistungen – allen voran den Erhalt des fragilen Klimasystems der Erde und die ökosystematischen lebenswichtigen Funktionen von Artenvielfalt.

Mit dem Report *Our Common Future,* dem sogenannten Brundtland-Bericht von 1987, wurde der Begriff der Nachhaltigkeit nicht nur auf die globale politische Agenda gesetzt, sondern zugleich seine bisher ausschließlich ökologischen Ziele um soziale und ökonomische Anliegen erweitert. Damit einher ging der wichtige Paradigmenwechsel insbesondere für die Länder des globalen Südens, statt nach*holender* Entwicklung nach dem Vorbild des Westens/Nordens nun eine nach*haltige* Entwicklung anzustreben, die vor allem auf die Realisierung der Menschenrechte setzt.

Allerdings sorgt die Definition von Nachhaltigkeit als Drei-Säulen-Modell im Brundtland-Bericht bis heute für begriffliche Verwirrung und Verwässerung: Ökologie, Soziales und Ökonomie sollten gleich gewichtet und integriert behandelt werden. Doch während sich für die Säulen Ökologie (etwa Klimaschutz, Artenvielfalt) und Soziales (etwa Gerechtigkeit, Einkommenssicherheit) klare Ziele definieren lassen, konnte nie abschließend geklärt werden, welches Ziel eigentlich die ökonomische Säule verkörpern sollte. Das Verständnis, dass damit *anhaltendes Wirtschaftswachstum* (*sustained growth*) gemeint sei, hat sich früh im Diskurs durchgesetzt, stellt genau betrachtet aber keinen Zweck, sondern allenthalben ein Mittel zur Erreichung von Zielen dar.

1 Vgl. Grober, Ulrich: Die Entdeckung der Nachhaltigkeit. Kulturgeschichte eines Begriffs, München: Kunstmann 2010.

Die Verwechslung von Mittel und Zweck hat bis heute fatale Folgen: Seit Jahrzehnten hemmen Politiken und Maßnahmen, die das Wirtschaftswachstum anfachen, oft die Erlangung ökologischer Nachhaltigkeit.[2] Das zeigt sich nicht nur, aber besonders deutlich in Krisenzeiten, etwa während der Weltwirtschafts- und Finanzkrise 2007-2009 oder während der Corona-Lockdowns 2020 und 2021, als wachstumsorientierte staatliche Ausgabenprogramme eine sozial und ökologisch motivierte Politik an den Rand gedrängt haben. Während viele noch immer denken, Wachstum sei ein probates Mittel, um soziale Ziele wie Gerechtigkeit oder gute Arbeit zu erreichen, ist dieser Zusammenhang für den globalen Süden bereits früh kritisiert worden. In Zeiten zunehmender sozialer Polarisierung und Verarmung bestimmter Bevölkerungsschichten verliert der Wachstumsfetischismus auch in den Ländern des globalen Nordens zunehmend seine Gültigkeit.[3]

Die 1990er Jahre können als die *hohe Zeit* des Nachhaltigkeits-Diskurses bezeichnet werden. Insbesondere rund um den Erdgipfel von Rio de Janeiro (1992) war der Begriff stark umkämpft. Zugleich wurden dort eine Reihe wichtiger nationaler und internationaler Nachhaltigkeits-Politiken ins Leben gerufen, darunter die Lokale Agenda 21, die Klimarahmenkonvention (UNFCCC) und die Biodiversitätskonvention (CBD) sowie später die Millenniums-Entwicklungsziele. In Deutschland waren vor allem die beiden Berichte *Zukunftsfähiges Deutschland* des Wuppertal Instituts (1996; 2008) diskursprägend. Spätestens seit der Finanzkrise 2007 und den Debatten um grünes Wachstum (*green growth*) versus Postwachstum (beziehungsweise *degrowth*) im Kontext des 20. Jubiläums des Erdgipfels im Jahr 2012 hat der Begriff Nachhaltigkeit aber an Schlagkraft verloren. In Fachkreisen wurde er vom Begriff der *sozial-ökologischen Transformation* abgelöst,[4] der in der breiteren Öffentlichkeit bisher jedoch geringere Wirkmächtigkeit entfalten konnte. Nach wie vor basieren zahlreiche Politikprozesse auf dem Nachhaltigkeitsbegriff, so etwa die Deutsche Nachhaltigkeitsstrategie, auf UN-Ebene die Sustainable Development Goals (SDGs) oder auf EU-Ebene der European

2 Vgl. Santarius, Tilman: Nachhaltigkeit. In: Braunmühl, Claudia von/Gerstenberger, Heide/Ptak, Ralf/Wichterich, Christa (Hg.): ABC der globalen (Un)Ordnung. Vom »Anthropozän« bis »Zivilgesellschaft«, VSA: Hamburg, 2019, S. 168-170.

3 Siehe u.a. Paech, Niko: Befreiung vom Überfluss, München: oekom 2012; Adler, Frank/Schachtschneider, Ulrich (Hg.): Postwachstumspolitiken Wege zur wachstumsunabhängigen Gesellschaft, München: oekom 2017.

4 Siehe z.B. WBGU 2011

Green Deal. Und seit einigen Jahren gibt es auch eine zunehmende Debatte darüber, welche Chancen und Risiken Digitalisierung für Nachhaltigkeit bereithält und wie Digitalisierung selber nachhaltiger gestaltet werden kann.[5] Haargenau 300 Jahre nach der ersten Begriffsnennung durch Carl von Carlowitz wurde im Jahr 2013 die erste internationale Konferenz zum Thema »ICT for Sustainability« in Zürich abgehalten.

Ohne Ökologie keine Gerechtigkeit – ohne Gerechtigkeit keine Ökologie

Die Dimensionen Ökologie und Soziales im wertebasierten Konzept der Nachhaltigkeit belegen, wie bedeutsam es für Anliegen der Gerechtigkeit ist. Denn Soziales und Ökologie sind zwei unmittelbar miteinander verschränkte Ziele: Wenn die Ungleichheit zunimmt und immer weniger Menschen eine Chance auf ein Leben in Würde erhalten, dann schrumpfen die Bereitschaft und das (u.a. auch finanzielle) Vermögen, in den Umbau von Wirtschaft und Gesellschaft zu investieren und nachhaltigere Formen von Produktion, Konsum, Mobilität und Wohnen zu praktizieren. Und wenn wiederum der Klimawandel, die Erosion fruchtbarer Böden, das Artensterben und die Übernutzung endlicher Ressourcen vulnerablen Gruppen im globalen Süden schon heute und nachfolgenden Generationen weltweit die Lebens- und Wirtschaftsgrundlagen entziehen, dann werden soziale Konflikte zunehmen und hierzulande wie global immer mehr Bevölkerungsgruppen von Arbeitsplatzverlusten, sozialer Ausgrenzung und Verarmung betroffen sein. Auf den Punkt gebracht heißt das: Ohne Gerechtigkeit wird kein Umweltschutz zu machen sein, und ohne Umweltschutz lässt sich keine soziale Gerechtigkeit erzielen.[6]

Gerechtigkeit muss indessen nicht nur unter dem Aspekt von Verteilungsfragen betrachtet, sondern auch im Sinne *absoluter Gerechtigkeit* beziehungsweise einer Gerechtigkeit als Anerkennung der grundlegenden Menschen-

5 Siehe z.B. Hilty, Lorenz M./Aebischer, Bernard: ICT Innovations for Sustainability, Cham/Heidelberg/New York/Dordrecht/London: Springer 2015; Lange, Steffen/Santarius, Tilman: Smarte grüne Welt? Digitalisierung zwischen Überwachung, Konsum und Nachhaltigkeit, München: oekom 2018; WBGU: Unsere gemeinsame digitale Zukunft, Berlin: WBGU 2019.

6 Vgl. Sachs, Wolfgang: Nach uns die Zukunft. Der globale Konflikt um Gerechtigkeit und Ökologie, Frankfurt a.M.: Brandes & Apsel 2002.

rechte verstanden werden.[7] In der Menschenrechts-Charta der Vereinten Nationen von 1948 wird die Unantastbarkeit der Würde jeder einzelnen Erdenbürgerin und jedes einzelnen Erdenbürgers von fast allen Ländern der Welt anerkannt. Nach 1948 wurden die Allgemeinen Menschenrechte konkretisiert – zum einen als *politische und bürgerliche Menschenrechte*, zum anderen als *wirtschaftliche, soziale und kulturelle Menschenrechte* – und knapp zwei Jahrzehnte später entsprechend mit dem UN-Zivilpakt und dem UN-Sozialpakt verabschiedet.

Zwei Stränge der Gerechtigkeit

Die Differenzierung in diese beiden *Stränge* der Menschenrechte (UN-Zivilpakt und UN-Sozialpakt) zeigt nicht nur den inneren Zusammenhang zwischen (ökologischer) Nachhaltigkeit und internationaler Gerechtigkeit auf, sondern ist auch für die Verbindung von Digitalisierung und Nachhaltigkeit aufschlussreich. Denn die Diskurse über Nachhaltigkeit einerseits und Digitalisierung andererseits konzentrieren sich auf je einen der beiden Stränge.

Ökologische Nachhaltigkeit zielt vor allen Dingen auf die Sicherung der Existenzrechte – etwa auf das Recht auf Nahrung, Trinkwasser und Gesundheitsfürsorge sowie das Recht auf einen auskömmlichen Lebensunterhalt. Diese Existenzrechte stellen gewissermaßen den elementaren Kern der wirtschaftlichen, sozialen und kulturellen Menschenrechte dar. Sie sind heute nicht nur durch korrupte Eliten, Kriege und Konflikte in Gefahr, sondern auch durch den Klimawandel, den Verlust der Artenvielfalt und den Verschleiß der Funktionsfähigkeit globaler und lokaler Ökosysteme. Das betrifft vor allem, aber nicht nur, die Existenzgrundlage der zwei bis drei Milliarden Menschen auf der Erde, die direkt von der Natur leben und deren Ernten durch Dürren, Überschwemmungen oder die Verschmutzung von Böden oder Gewässern bedroht werden. Für die Verwirklichung der wirtschaftlichen, sozialen und kulturellen Menschenrechte ist es daher unerlässlich, die Umweltzerstörung aufzuhalten und die Belastungsgrenzen des Planeten nicht zu überschreiten.

7 Vgl. Rawls, John: A theory of justice, Cambridge, MA: Belknap Press 1999; Sachs, Wolfgang/Santarius, Tilman (Hg.): Fair Future: Begrenzte Ressourcen und globale Gerechtigkeit, München: C.H. Beck 2005.

Tatsächlich aber findet derzeit bekanntermaßen das Gegenteil statt: Die *transnationale Konsumentenklasse* in den Industriegesellschaften in Nord und Süd ist dabei, den blauen Planeten in eine ungastliche Wüste zu verwandeln, weil ihr Naturverbrauch und ihre Umweltbelastungen viel zu hoch sind. Die Kernforderung der Nachhaltigkeit lautet daher, die Ressourcenverbräuche und schädlichen Emissionen insbesondere in den Hochverbrauchsregionen der Erde in den nächsten Jahrzehnten circa um den Faktor zehn zu reduzieren.[8]

Kritische Diskussionen über Digitalisierung hingegen haben sich in den letzten Jahrzehnten vor allem auf den anderen Strang bezogen, auf die politischen und bürgerlichen Menschenrechte. Auch diese Menschenrechte werden in vielen Staaten und Regionen der Welt mit Füßen getreten. Und auch in liberalen und wohlhabenden Ländern wie Deutschland geraten sie zunehmend in Gefahr, beispielsweise durch wachsenden Populismus. Derzeit werden sie jedoch auch und in besonderem Maße durch Prozesse gefährdet, die direkt mit Digitalisierungseffekten zusammenhängen. Entsprechend fokussieren viele Akteure, die sich für eine gemeinwohlorientierte Digitalisierung einsetzen, auf spezifische politische und bürgerliche Menschenrechte – etwa auf das Recht auf Freiheit vor willkürlichen Eingriffen in die Privatsphäre, auf Informationsfreiheit, Meinungsfreiheit und Pressefreiheit.

Während in bisherigen Digitalisierungs-Debatten die Sicherung der wirtschaftlichen, sozialen und kulturellen Menschenrechte kaum eine Rolle gespielt hat, sind wiederum die politischen und bürgerlichen Menschenrechte in den Debatten und Kämpfen für (ökologische) Nachhaltigkeit zwar nicht irrelevant, werden in den konkreten Analysen, Strategien oder Politiken jedoch oft nicht erwähnt. Versuche, im Rahmen des Konzepts der Nachhaltigkeit eine *politische Dimension* oder *Säule* zu reklamieren, konnten sich im Diskurs nicht durchsetzen. Auch deshalb ist der Nexus aus Digitalisierung und Nachhaltigkeit interessant: Eine Verbindung der Themenfelder, aber auch der Akteursnetzwerke hinter einerseits sozialer und ökologischer Nachhaltigkeit und andererseits Digitalisierung birgt das Potenzial, die beiden Diskursstränge um

8 siehe z.B. Steffen, Will u.a.: »Planetary boundaries: Guiding human development on a changing planet«, in: Science 347 (2015); Rogelj, Joeri u.a.: »Mitigation Pathways Compatible with 1.5°C in the Context of Sustainable Development«, in: IPCC (Hg.), Global Warming of 1.5°C. An IPCC Special Report on the impacts of global warming of 1.5°C above pre-industrial levels and related global greenhouse gas emission pathways, in the context of strengthening the global response to the threat of climate change, sustainable development, and efforts to eradicate poverty, Switzerland: IPCC 2018, S. 93-174.

den UN-Zivilpakt und den UN-Sozialpakt stärker zusammenzuführen.[9] Und wie im nächsten Abschnitt gezeigt wird, ist die kritische Debatte über eine werteorientierte Digitalisierung tatsächlich gut beraten, auch die wirtschaftlichen, sozialen und kulturellen Menschenrechte zu berücksichtigen.

Digitalisierung, Ressourcenverbrauch und Existenzrechte

Um die Bedeutung der Digitalisierung für die wirtschaftlichen, sozialen und kulturellen Menschenrechte in den Blick zu nehmen, müssen zuerst die hohen Ressourcen- und Energieverbräuche für die Herstellung digitaler Hardware angesprochen werden. Beispielsweise wurden allein für die Produktion der rund sieben Milliarden Smartphones, die in den zehn Jahren seit Einführung des ersten iPhones im Jahr 2007 auf den Markt kamen, schiere 38.000 Tonnen Kobalt, 107.000 Tonnen Kupfer, 157.000 Tonnen Aluminium und Tausende Tonnen weiterer Materialien verbaut. Diese riesigen Summen erschließen sich für die Nutzer*innen nicht, weil ein einzelnes Smartphone im Schnitt nur 5 Gramm Kobalt, 15 Gramm Kupfer, 22 Gramm Aluminium enthält.[10] Diese und weitere knappe und seltene Rohstoffe werden teils unter erbärmlichen Sozial- und Umweltstandards in Konfliktregionen des globalen Südens abgebaut. Und Smartphones sind nur ein Gerät unter vielen: Auch der Aufbau und Betrieb der digitalen Infrastrukturen hat menschenrechtliche Implikationen – all die Datenkabel, Serverparks und Rechenzentren, die Nutzer*innen selten zu sehen bekommen, ihnen aber erst den Zugang zum Internet ermöglichen, sind keinesfalls immateriell in der Cloud, sondern haben eine höchst materielle Basis. Auch deren Herstellung geht nicht nur mit direkten Beeinträchtigungen von Menschenrechten am Arbeitsplatz – von den Rohstoffminen bis zu den High-Tech-Fabriken – einher. Diese Rechte werden auch indirekt verletzt, weil die Emissionen aus den Hardware-Fabriken lokale Ökosysteme verschmutzen können und den Klimawandel anheizen, was beides die Lebensgrundlagen insbesondere von vulnerablen

9 Vgl. Santarius, Tilman/Kurz, Constanze: »Warum Bits und Bäume zusammengehören. Vier Gründe, um zwei Communities zu vernetzen«, in: Höfner, Anja/Frick, Vivian (Hg.): Was Bits und Bäume verbindet. Digitalisierung nachhaltig gestalten, München: Oekom Verlag 2018, S. 8-11.

10 Vgl. Greenpeace: 10 Jahre Smartphone. Die globalen Umweltfolgen von 7 Milliarden Mobiltelefonen, Hamburg: Greenpeace 2017.

Bevölkerungsgruppen in den Ländern des globalen Südens gefährdet. Tatsächlich ist die Hardwareproduktion eine der wenigen Branchen weltweit, deren Energieintensität im vergangenen Jahrzehnt um rund 4 Prozent pro Jahr nicht ab-, sondern zugenommen hat.[11]

In der Nutzung verbrauchen digitale Geräte dann vor allem Strom. Schon heute entfallen rund 10 Prozent des weltweiten Stromverbrauchs auf alle mit dem Internet vernetzten Geräte und Rechenzentren – wobei die meisten Szenarien davon ausgehen, dass der Stromverbrauch in den nächsten Jahren sogar noch weiter ansteigen wird.[12] Zwar werden die Server einiger großer Plattformanbieter (wie Google, Apple) bereits zu guten Teilen mit Strom aus erneuerbaren Energien gespeist, was ohne Zweifel für die ganze Branche wünschenswert ist. Systemisch gesehen steht dieser erneuerbare Strom jedoch den anderen Produktions- und Konsumbereichen, die ebenfalls möglichst rasch mit 100 Prozent grüner Energie versorgt werden müssen, nicht zur Verfügung. Die stark expansiven Verbräuche digitaler Produkte und Dienstleistungen erschweren daher die Energiewende, da zur Zielerreichung von 100 Prozent erneuerbaren Energien insgesamt sinkende Verbräuche vonnöten sind.[13] Da ein schnelles Ende fossiler Brennstoffe – in Ländern wie Deutschland vorzugsweise bis zum Jahr 2035 – dringend geboten ist, um die globale Erwärmung unter einer gefährlichen Schwelle zu halten, wirken sich die wachsenden Stromverbräuche der Digitalisierung daher indirekt auf die Sicherung der wirtschaftlichen, sozialen und kulturellen Menschenrechte aus.

Um den Klimawandel und den Raubbau an Ökosystemen aufzuhalten, um den wachsenden Ressourcenverbrauch und die schädlichen Emissionen zu stoppen, gibt es für eine werteorientierte Gestaltung der Digitalisierung daher eine klare Schlussfolgerung: Nur wenn Informations- und Kommunikationstechnologien auch umgekehrt dafür eingesetzt werden, den überbordenden Energie- und Ressourcenverbrauch und die Emissionen der industriellen Zivilisation in allen Sektoren radikal zu verringern, wird die Digitalisierung einen Beitrag zur nachhaltigen Realisierung aller Menschenrechte leisten.

---

11 Vgl. The Shift Project: Lean ICT: Towards digital sobriety, Paris 2019. https://theshiftproject.org/wp-content/uploads/2019/03/Lean-ICT-Report_The-Shift-Project_2019.pdf (Stand: 19.03.2019).

12 Vgl. Lange, Steffen/Santarius, Tilman: Smarte grüne Welt? Digitalisierung zwischen Überwachung, Konsum und Nachhaltigkeit, München: oekom Verlag 2018.

13 Siehe z.B. die Annahmen für die deutsche Energiewende unter Bundesregierung: »Gesetz zur Digitalisierung der Energiewende«.

Bevor ich im übernächsten Abschnitt beispielhaft an zwei Sektoren genau dieser Frage nachgehe – welche Potenziale Digitalisierung für eine Senkung von Naturverbrauch und Emissionen mit sich bringt –, möchte ich zunächst noch auf den zweiten Aspekt von Gerechtigkeit eingehen: die Verteilungsgerechtigkeit.

Digitalisierung und Klimagerechtigkeit – vier Dimensionen

Ressourcenleichte Produktions- und Konsummuster sowie drastische Emissionsminderungen sind nicht nur für die Sicherung der absoluten Menschenrechte unabdingbar, sondern auch, um Verteilungsgerechtigkeit herzustellen. Im Diskurs über Nachhaltigkeit wird dies unter anderem durch Konzepte der ökologischen Gerechtigkeit oder – um hier einen spezifischeren Blick zu wählen – durch das Konzept der Klimagerechtigkeit angesprochen. Klimagerechtigkeit erkennt an, dass ein würdevolles Leben mit gesellschaftlicher Teilhabe nicht gänzlich ohne Emissionen zu haben ist. Es ist daher eine Frage der fairen Verteilung von Emissionsrechten, welche Menschen und Gesellschaften wie viel Emissionen emittieren dürfen. Grundsätzlich lassen sich vier Dimensionen der Klimagerechtigkeit unterscheiden: (1) die ungleiche Erzeugung und (2) die ungleichen Auswirkungen des Klimawandels sowie (3) die faire Lastenteilung und (4) die faire Chancenverteilung beim Klimaschutz.

(1) Die erste Dimension ist wohlbekannt im öffentlichen Diskurs. Heute emittieren die Industrieländer des globalen Nordens zwar weniger als die Hälfte aller weltweiten Treibhausgase. Werden aber die in der Atmosphäre akkumulierten Emissionen betrachtet – und für die Klimawirkung von beispielsweise CO_2 ist es unerheblich, ob eine Tonne des Gases aus einem Kohlekraftwerk heute oder bereits vor 50 Jahren emittiert wurde –, so entfallen rund Dreiviertel auf die Industrieländer. Diese und Menschen der transnationalen Konsumentenklasse in den Wohlstandsinseln des globalen Südens tragen damit nach wie vor die weit überwiegende Verantwortung für die globale Erwärmung. Pro Kopf zeigt sich das durch sehr unterschiedliche Emissionsbilanzen: Durchschnittlich ist eine US-Amerikanerin für 16 Tonnen, ein Deutscher für 9 Tonnen, eine Chinesin für 8 Tonnen, ein Inder für 2 Tonnen

oder eine Bangladescherin für 0,6 Tonnen CO_2-Emission pro Kopf und Jahr verantwortlich.[14]

Die Emissionsbilanzen stehen nur in einem indirekten, aber deutlichen Zusammenhang zur Verbreitungsdichte von digitalen Geräten und der Online-Nutzung. Beispielsweise zeigen sich fast ebenso große Unterschiede in der Verbreitungsdichte von Smartphones wie in den Pro-Kopf-Emissionen – mit mehr als Dreivierteln der Bevölkerung, die ein Smartphone besitzen, in den USA und Deutschland, 55 Prozent in China, 27 Prozent in Indien und 16 Prozent in Bangladesch.[15] Die Verbreitungsdichte digitaler Geräte ist beileibe nicht die wichtigste Determinante der CO_2-Emissionen pro Kopf – beides wird maßgeblich vom finanziellen Wohlstand sowie dem allgemeinen nationalen Produktions- und Konsumniveau beeinflusst. Doch wie Abbildung 1 zeigt, macht der Anteil digitaler Geräte in Ländern wie Deutschland mittlerweile rund 7 Prozent der konsumbedingten Pro-Kopf-Emissionen aus.

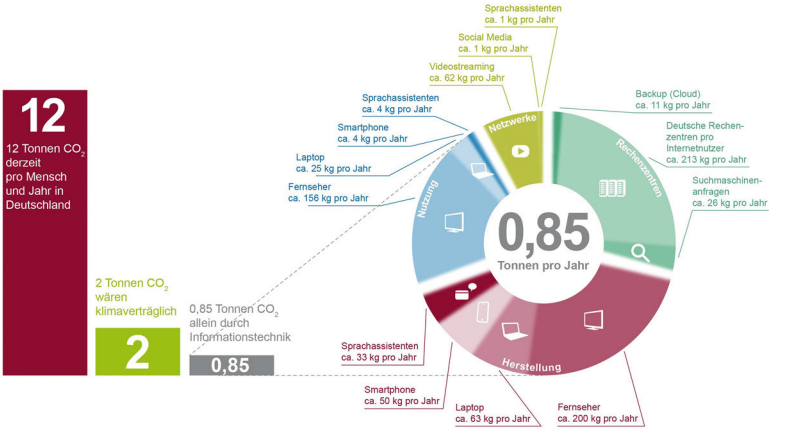
(2) Die zweite Dimension der Klimagerechtigkeit bezieht sich darauf, dass die Folgeschäden des Klimawandels Länder und Menschen weltweit höchst ungleich treffen. Ein Blick auf eine meteorologische Karte macht deutlich, welche Regionen durch zunehmende Extremwetterereignisse wie etwa Stürme und Überschwemmungen am meisten getroffen werden: Unregelmäßigkeiten im Monsun bedrohen in erster Linie die Länder Südostasiens; Überschwemmungen durch Sturmfluten oder angestiegene Flusswasserspiegel suchen vor allem die Bevölkerungen in den großen Deltagebieten der Erde heim, etwa in Bangladesch oder Indien; und der Anstieg des Meeresspiegels wird am stärksten die kleinen Inselstaaten treffen, etwa die unzähligen Eilande im Pazifik, oder auch Städte wie Mogadischu oder Dhaka, die auf Meeresspiegelniveau liegen. Ähnlich ungleich verteilt sind die Folgen für die

14 Vgl. European Commission. Joint Research Centre: Fossil CO2 and GHG emissions of all world countries. 2020 report. LU: Publications Office 2020.

15 Vgl. Newzoo: Global Mobile Market Report 2019 – Light Version. https://newzoo.com/insights/trend-reports/newzoo-global-mobile-market-report-2019-light-version/ (Stand: 27.01.2021).

16 Hinweis: Die Abbildung geht von konsumbedingten Emissionen pro Kopf aus und schließt daher Emissionen ein, die in anderen Ländern zur Herstellung von importierten Produkten entstehen. Daher werden die Pro-Kopf-Emissionen für Deutschland hier mit 12 Tonnen angegeben, gegenüber den rund 9 Tonnen Emissionen, die die territorial in Deutschland erfolgten Pro-Kopf-Emissionen ausweisen.

Abbildung 1: Anteil digitaler Geräte und Anwendungen am CO_2-Fußabdruck pro Kopf



Quelle: Gröger, Jens: »Der CO2-Fußabdruck unseres digitalen Lebensstils. Die Herstellung von Laptops, Fernsehern, Smartphones und Sprachassistenten verursacht den größten Teil der Treibhausemissionen«, in: Beitr. Standpunkte Aus Dem Ökoinstitut (2020). Die Zahlen beruhen auf Schätzungen und dienen zur Verdeutlichung der Größenordnung. Erklärung der Zahlen: https://blog.oeko.de/digitaler-co2-fussabdruck/. (CC BY-SA 2.0)[16]

Nahrungsmittelproduktion. Sie werden erstens ebenfalls durch Extremwetterbedingungen (Starkregen, Dürren), zweitens durch die Ausbreitung neuer Schädlinge in Regionen, in denen es diese bisher nicht gab, und drittens durch den allgemeinen globalen Temperaturanstieg beeinträchtigt. Für die meisten tropischen und subtropischen Regionen wird davon ausgegangen, dass die Erträge schon bei geringfügig höheren Temperaturen zurückgehen werden, weil die Pflanzen dort schon jetzt am Temperaturoptimum wachsen.

Was die Milderung beziehungsweise Anpassung an die Folgen (*climate change adaptation*) betrifft, hält Digitalisierung einige Chancen bereit. Digitale Werkzeuge für die Erdbeobachtung erleichtern es, Extremwetterbedingungen früh zu erkennen, Strategien für die Anpassung an den Klimawandel wissenschaftlich zu stützen und Erfahrungen aus den vielfältigen Anpassungsstrategien systematisch und rasch auszuwerten und zu verbreiten. Geografische Informationssysteme (GIS) leisten hier seit Längerem wichtige Beiträge. Zunehmend wird auch Sensorik zur Datenerhebung und zum ver-

besserten Management von Ökosystemen verwendet. Beispielsweise können digital-physische Systeme (Internet der Dinge) in der Forstwirtschaft dabei unterstützen, die Gesundheit von Spezies und Habitaten sowie die Holzproduktion zu beobachten, eine Bodenverschlechterung oder Dürren in Wäldern frühzeitig zu erkennen oder Waldbränden vorzubeugen. Auch im Bereich der Landwirtschaft werden große Hoffnungen auf sensorik- und datenbasierte Methoden gesetzt, mit denen gegebenenfalls der Einsatz von Pestiziden reduziert werden kann. Künftig dürften hier Anwendungen des maschinellen Lernens (künstliche Intelligenz) das Monitoring und die Entscheidungsfindung noch einmal verbessern – insbesondere wenn hierfür Datensätze aus den verschiedenen Weltregionen zusammengezogen und für Forschung und Management zugänglich gemacht werden, sodass eine Mustererkennung aus den Erfahrungen aller Klimaanpassungspraktiken erfolgen kann.[17]

(3) Die dritte Dimension nimmt Gerechtigkeit bei der Lastenverteilung in den Blick. Dabei wird davon ausgegangen, dass Klimapolitik zwar aus ökologischen und sozialen Gründen unbedingt notwendig ist, aber zunächst Geld kostet und daher ökonomische Belastungen mit sich bringt – jedenfalls gegenüber dem Status quo. Zwar bestehen in volkswirtschaftlicher Hinsicht wiederum wenig Zweifel, dass sich Klimaschutz »lohnt«, weil die langfristigen volkswirtschaftlichen Schäden die kurzfristigen Kosten für Klimaschutzmaßnahmen deutlich übersteigen werden. In den letzten Jahren betrugen die weltweiten, auf den Klimawandel zurückzuführenden Schäden aus Extremwetterbedingungen mehr als 100 Milliarden US-Dollar jährlich; bis 2050 antizipieren Szenarien, dass sich die Kosten auf 8 Billionen aufsummieren könnten, was dann rund 3 Prozent des weltweiten Bruttoinlandprodukts bedeuten würde.[18] Investitionen in Klimaschutz sowie eventuelle Einbußen des Bruttoinlandsprodukts aufgrund strenger Maßnahmen, darunter preisbeeinflussende wie Ökosteuern oder Emissionshandel, werden den Erwartungen gemäß deutlich geringer belastend sein.[19] Dennoch machen heutige Klimaschutz- und Klimaanpassungspolitiken Investitionen erforderlich, die zunächst bezahlt werden müssen und sich für die jeweiligen Akteure – seien

17 Vgl. Rolnick, David u.a.: »Tackling Climate Change with Machine Learning«, in: ArXiv190605433 Cs Stat 2019. http://arxiv.org/abs/1906.05433(Stand: 18.09.2019).

18 Vgl. Tol, Richard S.J.: »The Economic Impacts of Climate Change«, in: Review of Environmental Economics and Policy 12 (2018), S. 4-25.

19 Vgl. Stern, Nicholas H.: The economics of climate change. The Stern review, Cambridge, MA: Cambridge University press 2007.

es Unternehmen, Privatpersonen oder staatliche Institutionen – nicht unbedingt sichtbar »amortisieren« werden. Aus einer klimagerechten Perspektive stellt sich daher die Frage, wer diese Kosten eigentlich fairerweise tragen müsste. Zum Beispiel wurde vorgeschlagen, dass aufgrund ihrer großen historischen Verantwortung für die akkumulierten Treibhausgase in der Atmosphäre die Industrieländer auch einen erheblichen Anteil der Kosten übernehmen sollten, die in den Ländern des globalen Südens für Klimaschutz und -anpassung anfallen.[20] Nicht zuletzt daher gibt es im Rahmen der multilateralen Klimaverhandlungen Mechanismen für den Technologietransfer und für Finanztransfers, um Länder mit weniger Kapazitäten zu unterstützen.

Digitale Werkzeuge können auf doppeltem Wege zu einer fairen Lastenverteilung beitragen. Wie oben bereits ausgeführt, können sie erstens via verbessertem Monitoring und einer systematischen Auswertung von Politiken zur Klimaanpassung helfen, die Kosten der Schäden zu verringern. Und zweitens kann Digitalisierung die Kosten für Klimaschutzpolitiken vor allem durch Kosteneffizienzsteigerungen reduzieren. Grund für diese zweite Erwartung ist die Annahme, dass Digitalisierung den technischen Fortschritt sowie die wirtschaftliche Produktivität steigern kann. Laut explorativer Studien zum Beispiel der Global E-Sustainability Initiative kann Digitalisierung bis zum Jahr 2030 bis zu 20 Prozent der weltweiten CO_2-Emissionen einsparen helfen, zugleich aber 11 Billionen US-Dollar an ökonomischen Einsparungen und Wachstumseffekten hervorbringen.[21] Allerdings müssen digitale Produktivitätssteigerungen auch kritisch betrachtet werden: Die gleichzeitige Steigerung der K*arbonproduktivität* sowie der Kapital- und Arbeitsproduktivität können zu Rebound-Effekten (Einsparpotenziale von Effizienzsteigerungen werden durch erhöhten Konsum und Verbrauch nicht eingelöst) führen, die sich wiederum negativ auf die Erreichung von Nachhaltigkeitszielen auswirken.[22]

---

20 Siehe hierzu z.B. Baer, Paul u.a.: »Greenhouse Development Rights: towards an equitable framework for global climate policy«, in: Cambridge Review of International Affairs 21 (2008), S. 649-669.

21 Vgl. GeSI, Accenture: Smarter 2030. ICT Solutions for 21st Century Challenges, Brussels 2015; siehe auch GeSI, Deloitte: Digital with Purpose: Delivering a SMARTer2030, Brussels 2019; BITKOM, Accenture: Klimaeffekte der Digitalisierung. Studie zur Abschätzung des Beitrags digitaler Technologien zum Klimaschutz, Berlin: BITKOM 2021.

22 Vgl. Santarius, Tilman: Digitalization, Efficiency and the Rebound Effect. Blogpost vom 16. Februar 2018 auf https://www.degrowth.info/de/2017/02/digitalization-efficiency-and-the-rebound-effect/

(4) Die vierte Dimension der Klimagerechtigkeit zielt auf eine möglichst faire Verteilung der Chancen des Klimaschutzes, in diesem Fall insbesondere der ökonomischen Chancen. Diese Chancen stellen sich nicht nur volkswirtschaftlich in der Verringerung von Schäden und der Einsparung von Kosten dar, sondern konkret auch betriebswirtschaftlich für jene Akteure, die Klimaschutztechnologien entwickeln und vermarkten. Weltweit stiegen die Exporte von Umweltschutztechnologien von 2002 bis 2015 um durchschnittlich 8,4 Prozent pro Jahr und damit deutlich stärker als das allgemeine Welthandelsvolumen und auch das globale Bruttoinlandsprodukt. Betrachtet man jedoch, welche Länder (und Unternehmen) hier die zentralen Nutznießer sind, beschränkt sich dies auf eine Hand voll Industrieländer sowie einige sehr wenige ausgesuchte Schwellenländer – darunter insbesondere China, aber zum Beispiel auch Indonesien, Malaysia und Mexiko. Deutschland nimmt einen Welthandelsanteil von 13,6 Prozent ein und ist damit nach China der zweitgrößte Exporteur weltweit, dessen Anteil sich seit 2002 mehr als verdreifacht hat.[23]

Während die Potenziale der Digitalisierung für Kostensenkungen zu einer faireren Lastenverteilung beitragen können (siehe oben), müssen die daraus erwachsenden ökonomischen Vorteile vor dem Hintergrund der vierten Dimension der Klimagerechtigkeit trotzdem kritisch reflektiert werden. Denn auch die digitalen Lösungen für den Klimaschutz in den Bereichen Mobilitäts- und Energietransformation, *smarte Landwirtschaft* (z.B. Precision Farming) oder auch im Bereich Wohnen (z.B. Smarthome-Systeme) werden derzeit vor allem in den High-Tech-Zentren der Welt entwickelt. Der Großteil jener Länder im globalen Süden, die vor allem unter den ungleichen Auswirkungen des Klimawandels leiden, hat damit wenig Aussicht auf einen fairen Anteil der ökonomischen Chancen aus digitalen Klimaschutz-Technologien. Es steht gar zu befürchten, dass die Technologie- und Finanztransfers, die aus Gründen der (3) fairen Lastenverteilung in erster Linie jenen Ländern des globalen Südens dienen sollten, die wenig zum Klimawandel beigetragen haben, über den Import technologischer Lösungen aus den High-Tech- und Hauptverursacher-Ländern des globalen Nordens letzteren mehr nutzen als ersteren. Daher bleibt als Fazit: Wenn Anwendungen für Klimaschutz und Klimaanpassung digitaler werden und die Entwicklung dieser Technologien vor allem in den wohlhabenden Regionen der Welt stattfindet, wird Digitalisierung die ungleiche Chancenverteilung eher noch verschärfen.

23 Vgl. Umweltbundesamt: Umweltwirtschaft und grüne Zukunftsmärkte, Dessau 2020.

In der Gesamtschau des Konzepts der Klimagerechtigkeit wird deutlich, dass Digitalisierung in allen Dimensionen eine Rolle spielen kann und sie sowohl Chancen als auch Risiken birgt. Die Chancen liegen vor allem in Kostensenkungen, besserem Monitoring, dem Austausch von Informationen (und Fähigkeiten) sowie neuen Steuerungsmöglichkeiten, zum Beispiel durch künstliche Intelligenz. Die Risiken liegen insbesondere in den Klima- und Menschenrechts-Implikationen der materiellen Basis (Hardware) der Digitalisierung, weiterem Wachstumsdruck (etwa durch Rebound-Effekte) und einer ungleichen Verteilung von Chancen durch die Entwicklung von klimabezogenen digitalen Technologien. Um diesen Risiken entgegenzuwirken und die Chancen zu nutzen, ist verstärkte politische Gestaltung vonnöten. Dies wird im weiteren Verlauf des Artikels ausgeführt.

Digitale Lösungen zur Senkung von Naturverbrauch und Emissionen – Beispiele Mobilität und Konsum

Ungeachtet dieser Herausforderungen aus Sicht der Klimagerechtigkeit soll abschließend untersucht werden, inwiefern digitale Werkzeuge tatsächlich dazu beitragen können, Naturverbrauch und Emissionen zu verringern. Wie schon erwähnt, bieten sich in praktisch allen Sektoren – beim Konsum, in der Mobilität, bei der Energieversorgung, im Haushalt, in der Industrie etc. – Potenziale und Risiken. Beispielhaft und nur kursorisch sollen hier daher einige Aspekte der Bereiche Mobilität und Konsum betrachtet werden.

Die Nachhaltigkeitsziele in der Mobilitätswende sind vielfältig, lassen sich aber auf folgende Kernpunkte verengen: Es geht um den Wechsel vom privaten Pkw-Besitz zu nutzungsgeteilten und öffentlichen (Massen-)Verkehrsmitteln, die möglichst mit grünem Strom (oder anderen erneuerbaren Energieträgern) betrieben werden, sowie um eine kluge, digitalgestützte Raum- und Mobilitätsplanung, um Verkehrsströme insgesamt zu verringern – insbesondere den Flugverkehr. Die Digitalisierung bietet für diese Ziele etliche Chancen: Eine konsequente Nutzung von Video-Konferenzen kann viele Dienstreisen überflüssig machen. Die Nutzung öffentlicher Verkehrsträger – Busse, Sammeltaxen, Bahnen etc. – sowie das Sharing von Fahrrädern, Autos oder Mitfahrgelegenheiten ist dank der Digitalisierung bereits sehr viel einfacher, günstiger und bequemer geworden – auch wenn Car-Sharing alleine, insbesondere die flexiblen Free-Floating-Modelle (Fahrzeug kann innerhalb eines fest definierten Nutzungsgebiets auf jedem freien Parkplatz abgestellt wer-

den) in Innenstädten, kaum zu Verkehrsvermeidung führt. In Zukunft kann Digitalisierung weitere wertvolle Beiträge leisten, wenn integrierte »Mobility-as-a-Service«-Plattformen entstehen, die multimodale Mobilität (über mehrere Verkehrsträger hinweg) per Mausklick und *on-the-go* ermöglichen. Dann können Nutzer*innen schnell und günstig mehrere öffentliche Verkehrsträger miteinander kombinieren – etwa von zu Hause ein Leihrad zur nächsten öffentlichen Haltestelle nehmen, dort per ÖPNV durch die Stadt fahren und sich schließlich für die letzte Strecke einen Roller mieten.

Allerdings birgt Digitalisierung im Mobilitätsbereich auch Risiken. Denn die Vision für einen multimodalen, öffentlichen Verkehr ist weder die einzige noch die dominante in der gegenwärtigen Debatte über digitale Mobilitätsstrategien. Große IT- und Automobilkonzerne stellen stattdessen in Aussicht, in selbstfahrenden Autos von Robotern chauffiert zu werden – ein attraktives Narrativ, das die ökologisch und sozial verhängnisvolle »Liebe zum Automobil« in der Gesellschaft neu entfachen könnte. Währenddessen treibt das Bundesministerium für Verkehr und digitale Infrastruktur den Ausbau des 5G-Mobilfunkstandards und das »Testfeld digitale Autobahn« voran, um datenintensiven Assistenzsystemen im Straßenverkehr zum Durchbruch zu verhelfen. Diese Art von Effizienz- und Komfortsteigerungen birgt jedoch die Gefahr erheblicher Rebound-Effekte, die die Einsparpotenziale konterkarieren können.

Ähnlich lassen sich Chancen und Risiken der Digitalisierung für eine Konsumwende feststellen. Aus Nachhaltigkeitssicht wäre es einerseits notwendig, das Konsumniveau zu senken, zumindest in den reichen Hochverbrauchsländern, sowie andererseits von konventionellen zu nachhaltiger erzeugten Produkten und Dienstleistungen zu wechseln. Digitale Werkzeuge bieten Chancen, um beides zu fördern: Gebrauchthandels-Plattformen (Ebay & Co) machen es leicht, auf Neukauf zu verzichten. Über Peer-to-Peer-Sharing lassen sich Rasenmäher, Autos, Bohrmaschinen, aber auch Nachbarschaftshilfe teilen. Und der Einkauf von nachhaltigen Waren – ob FSC-zertifizierte Möbel oder faire Kleidung – ist im Prinzip genauso leicht per Mausklick möglich wie der Erwerb der nicht-nachhaltigen Massen-Produkte. Doch diese Potenziale werden durch einen mächtigen Gegentrend unterlaufen. Die allzeitige Verfügbarkeit von Online-Shopping-Optionen, die ständige Optimierung personalisierter Werbung und ein omnipräsentes Marketing auf Suchmaschinen und in sozialen Medien treiben die Umsätze des E-Commerce kontinuierlich in die Höhe. Und auch in diesem Bereich bergen Zeit- und Komfortgewinne durch Online-Shopping das Risiko von Rebound-Effekten, die sich in einem

gestiegenen Konsumniveau niederschlagen.[24] Bedauerlicherweise ist das Geschäftsfeld der großen Plattformanbieter wie Facebook, Google, Amazon und andere darauf ausgerichtet, den hohen und nicht nachhaltigen Massenkonsum mittels digitaler Optimierung von Werbung noch weiter anzukurbeln, anstatt das Sharing und die Vermarktung alternativer Produkte voranzubringen.

Politiken für eine nachhaltigkeitsorientierte Gestaltung der Digitalisierung

Wie oben beschrieben, wirken sich große ökologische Fußabdrücke aus der Herstellung digitaler Geräte und Infrastrukturen direkt auf die Existenzrechte und indirekt auf die Klimagerechtigkeit aus. Ein wichtiger, und doch oft übersehener Ansatz für eine nachhaltigere Gestaltung der Digitalisierung sind daher das Design und die Standards für nachhaltige Herstellungsbedingungen. Zentral ist die Entwicklung einer Design-Richtlinie für IT-Geräte, zum Beispiel anknüpfend an bestehende Design-Richtlinien auf EU-Ebene. Darin könnten Standards gesetzt werden, dass Geräte möglichst schadstoffarm und energiesparend hergestellt werden, zudem mit erneuerbarer Energie. Ferner sollten Geräte grundsätzlich modular aufgebaut und reparierbar konzipiert werden. Auch könnte eine Ausdehnung der Herstellergarantien vorgeschrieben werden wie auch die Anforderung, dass Hersteller grundsätzlich bis zum Ende der Lebensdauer von Geräten Softwareupdates bereitstellen müssen. Damit würde der Berg des digitalen Elektroschrotts pro Jahr langsamer anwachsen, während eine Regulierung von Recyclingquoten vorschreiben könnte, möglichst viele knappe Rohstoffe in den Produktionskreislauf zurückzuführen.

Ferner könnte als Richtlinie eine Politik des »one person, one device« erwogen werden. Eine solche Politik kann zum einen dazu beitragen, die materielle Basis der Digitalisierung und ihre Folgen für Existenzrechte auf einem möglichst niedrigen Niveau zu halten. Zum anderen kann sie als Richtschnur

24 Vgl. Santarius, Tilman: »Auf dem Weg in die vernetzte (Verbraucher-)Zukunft – Widersprüche der Digitalisierung für den nachhaltigen Konsum«, in: Blättl-Mink, Birgit/Kenning, Peter (Hg.): Paradoxien des Verbraucherverhaltens. Dokumentation der Jahreskonferenz 2017 des Netzwerks Verbraucherforschung, Wiesbaden: Springer Gabler 2019, S. 101-111.

dienen, die digitale Kluft zwischen Nord und Süd zu verringern und eine fairere Verteilung der Chancen und Risiken der Digitalisierung zu erzielen. Mit dem Prinzip des »one person, one device« würden nicht nur die politischen und bürgerlichen Menschenrechte für Erdenbürger*innen verbessert, die derzeit noch gar keinen Internet-Zugang genießen, sondern es würden zugleich die schädlichen Nebeneffekte eines *digitalen Hochverbrauchs* insbesondere der reichen Erdenbürger*innen auf die Existenzrechte weltweit reduziert.

Mit Blick auf die steigenden Stromverbräuche bei der Nutzung digitaler Geräte, die für die kommenden Jahre erwartet werden und die sich ebenfalls indirekt auf die Realisierung der Existenzrechte sowie direkt auf die Realisierungschancen der Energiewende auswirken, könnten Energiestandards für Rechenzentren und Endgeräte festgeschrieben werden. Zum einen könnten dies Effizienzstandards sein, die im Zeitverlauf dynamisch verschärft werden – ähnlich des Top-Runner-Ansatzes, bei dem der beste technische Standard heute schon wenige Jahre später zum Mindeststandard für die ganze Branche gemacht wird. Doch neben Effizienzstandards sollten auch *Suffizienzstandards* erwogen werden; beispielsweise Labels, die den absoluten (und nicht nur relativen) Energieverbrauch von Geräten angeben, oder Anforderungen an eine Mindest-Auslastung von Rechenzentren sowie Bedingungen für den Neubau von Rechenzentren, die eine Nutzung der Abwärme als Ressource für andere Prozesse (Fernwärme, gewerbliche Prozesse) vorschreiben.

Darüber hinaus wird eine nachhaltigkeitsorientierte Digitalpolitik die Effizienzpotenziale der Digitalisierung zu heben versuchen – aber zugleich mit klugen Maßnahmen flankieren, um sicherzustellen, dass die Einsparpotenziale bei Energie und Ressourcen nicht durch Nachfragewachstum (wie Rebound-Effekte) wieder aufgefressen werden. Zum einen kann hier mit ökonomischen Instrumenten eine *Globalsteuerung* angestrebt werden. So kann eine »digital-ökologische Steuerreform«[25] Rahmenbedingungen für die gesamte Wirtschaft setzen, sodass Strom- und Spritverbräuche kontinuierlich teurer werden, während gleichzeitig umweltfreundlichere Alternativen und der Faktor Arbeit durch die Einnahmen entlastet werden. Zum anderen kann eine *sektorspezifische Feinsteuerung* erfolgen: Im Verkehrsbereich sollte die Entwicklung von »Mobility-as-a-Service«-Plattformen mit öffentlichen Mitteln unterstützt und zudem eine Daten-Governance aufgebaut werden,

25 Lange, Steffen/Santarius, Tilman: Smarte grüne Welt? Digitalisierung zwischen Überwachung, Konsum und Nachhaltigkeit, München: oekom Verlag 2018.

die einer transformativen Lenkung von Verkehrsströmen vom Individualverkehr zum öffentlichen und nutzungsgeteilten Verkehr dient. Da hierdurch jedoch der ÖPNV digital optimiert und das Sharing von Verkehrsträgern kostengünstiger und einfacher werden und deren Effizienz gehoben wird, sollte parallel der motorisierte und gegebenenfalls bald automatisierte Individualverkehr durch aktive Politiken unattraktiver gemacht werden, etwa durch Parkraumverteuerung, Straßenberuhigung, Mautgebühren und anderes, um Rebound-Effekten vorzubeugen. Im Bereich Konsum und E-Commerce sollte vor allem das Tracking von Online-Kaufentscheidungen und die Personalisierung von Werbung eingehegt werden. Da die Vermarktung von Daten für Zwecke Dritter derzeit nicht ausreichend geregelt wird, bedarf es einer konsequenten Weiterentwicklung der europäischen Datenschutz-Grundverordnung (DSGVO), um neue Rechtsvorschriften zum Prinzip der Datensparsamkeit und des Kopplungsverbots einzuführen und Vollzugsdefizite zu verringern. Ferner sollte eine selektive Beschränkung von Online-Werbung in Betracht gezogen werden: Äquivalent zum Verbot von Werbung in öffentlichen Räumen wie Schulen könnten werbefreie Räume im Internet errichtet werden, vor allem auf Suchmaschinen und in sozialen Medien. Diese Maßnahmen würden nicht nur ganz direkt bürgerliche und politische Menschenrechte sicherstellen, sondern indirekt auch zur Verbesserung der wirtschaftlichen Menschenrechte und der Existenzrechte beitragen. Denn eine auf Überwachungskapitalismus basierende Personalisierung von Werbung steigert effektiv den Konsum[26] und trägt damit zur Übernutzung knapper Ressourcen und der Belastungsgrenzen des Planeten bei.

Ferner kann öffentliche Forschungspolitik und -förderung die Entwicklung von nachhaltigkeits- oder klimaschutzorientierten digitalen Technologien voranbringen. Gefördert werden sollten beispielsweise die Entwicklung von Anwendungen und Infrastrukturen für smarte dezentrale Stromnetze

26 Vgl. Santarius, Tilman: »Auf dem Weg in die vernetzte (Verbraucher-)Zukunft – Widersprüche der Digitalisierung für den nachhaltigen Konsum«, in: Blättel-Mink, Birgit/Kenning, Peter (Hg.): Paradoxien des Verbraucherverhaltens: Dokumentation der Jahreskonferenz 2017 des Netzwerks Verbraucherforschung, Wiesbaden: Springer Gabler 2019, S. 101-111; Frick, Vivian/Matthies, Ellen: »Everything is just a click away. Online shopping efficiency and consumption levels in three consumption domains«, in: Sustain. Prod. Consum. 23 (2020), S. 212-223; Frick, Vivian u.a.: »Do online environments promote sufficiency or overconsumption? Online advertisement and social media effects on clothing, digital devices, and air travel consumption«, in: J. Consum. Behav. 2020.

(z.B. *micro grids*); suffiziente Energiemanagementsysteme zur Steuerung von Heizungsanlagen; grüne Apps, die nachhaltigen Konsum erleichtern; E-Commerce-Plattformen, die lokalen und regionalen Anbietern einen Vorteil gegenüber den globalen Shopping-Plattformen verschaffen oder Peer-to-Peer-Sharing-Plattformen, die eine regionale Vernetzung von Produzent*innen und Konsument*innen unterstützen. Hierzu können nationale oder kommunale Regierungen Inkubatoren-Programme (Gründerzentren) und Accelerator-Camps (Beschleunigungsprogramme) etablieren oder auch Vernetzungs-Plattformen für den Austausch und eine kollaborative Entwicklung von Projekten bieten. Zudem können offene IT-Produkte auf Basis offener Hard- und Software gefördert werden, indem eine gezielte Vergabe öffentlicher Aufträge ihre Priorisierung erlaubt. Staatliche Aufträge können ferner hohe Standards für Datenschutz, ein möglichst ökologisches Produktdesign der digitalen Geräte (Green IT) und einen minimalen Energieverbrauch der Geräte im Betrieb fordern.

Es ist erfreulich festzustellen, dass wenigstens einige dieser Politiken für eine nachhaltigkeitsorientierte Digitalisierung bereits von politischen Akteuren angestoßen wurden. 2019 hat das Bundesumweltministerium ein Eckpunktepapier sowie 2020 eine umfangreiche »Umweltpolitische Digitalagenda« vorgelegt, die nun etliche konkrete Politiken und Maßnahmen zur Gestaltung einer nachhaltigeren Digitalisierung plant.[27] Zugleich wurde im European Green Deal der EU-Kommission angekündigt, die Themen Digitalisierung und Klimaschutz prioritär zu behandeln, und im Dezember 2020 wurde eine europäische Agenda für eine nachhaltige Digitalisierung durch Beschlüsse des EU-Ministerrats skizziert.[28] Es bleibt abzuwarten, inwiefern diese Politiken in den nächsten Jahren tatsächlich und mit ambitionierten Zielen und Standards umgesetzt werden und ob Regierungen anderer Länder ähnliche Agenden entwickeln.

27 Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit: Umwelt in die Algorithmen! – Eckpunkte für eine umweltpolitische Digitalagenda des BMU, Berlin: BMU 2019; siehe kritisch dazu Kern, Florian/Santarius, Tilman: »Digitalisierung als Treiber einer sozial-ökologischen Transformation?«, in: Ökologisch Wirtschaften 33 (2020), S. 8-9.

28 Rat der Europäischen Union: Digitalisierung zum Wohle der Umwelt. Schlussfolgerungen des Rats der Europäischen Union. 2021.

2.3 Demokratie, Zugang und Souveränität

2.3.1 Zugang

Digitale Öffentlichkeit, Aufmerksamkeit als Ware und die deliberative Demokratie

Christian Stöcker

Kurz nachdem in den Morgenstunden des ersten Weihnachtsfeiertags 2020 in Nashville, Tennessee, ein Wohnmobil explodiert war, veröffentlichte eine für die Lokalzeitung *The Tennessean* arbeitende Reporterin[1] eine bemerkenswerte Beobachtung: Der zu diesem Zeitpunkt bereits als Täter identifizierte Anthony Quinn Warner, der bei der Explosion selbst ums Leben gekommen war, habe »praktisch keinen Online-Fußabdruck hinterlassen«, schrieb die Journalistin Natalie Allison auf Twitter.[2]

Bemerkenswert ist diese Beobachtung aus zwei Gründen: Zum einen, weil es im Jahr 2020 augenscheinlich bereits als absolut selbstverständlich galt, dass ein Bewohner einer westlichen Industrienation im Normalfall einen solchen »Online-Fußabdruck« hinterlassen würde. Und zum anderen, weil gerade die Männer, die mit spektakulären Gewalttaten auf sich aufmerksam machten, zu diesem Zeitpunkt sonst häufig nicht nur beiläufig entstandene, sondern sehr bewusst platzierte »Fußabdrücke« im Netz hinterließen, oft als »Manifeste« deklariert. Egal, ob sie ihre Gewalttaten in Norwegen, in Halle, Hanau oder Christchurch, Neuseeland, begingen.

Das neue, digital-mediale Ökosystem hat nahezu alle Bewohner*innen industrialisierter Nationen auch zu Inhalteproduzent*innen werden lassen, wenn auch in sehr unterschiedlichem Ausmaß. Manche dieser Inhalte sind

1 »Anthony Quinn Warner, self-employed computer guru ID'd as lone Nashville bomber, killed in blast«, Nashville Tennessean 2020, https://www.tennessean.com/story/news/crime/2020/12/27/anthony-quinn-warner-confirmed-person-interest-nashville-explosion/4052711001/

2 Ellison, Natalie: »Tweet von Natalie Allison«, 28.12.2020, https://twitter.com/natalie_allison/status/1343349692982304771?s=20

mit Grundprinzipien wie Menschenrechte, Menschenwürde oder auch nur mit elementaren Qualitätsansprüchen an öffentlich verfügbare Information kaum oder gar nicht vereinbar. Andere sehen aus wie Werbung, werden aber als Unterhaltung konsumiert. Wieder andere sind die Keimzellen neuer sozialer Bewegungen.

Die veränderte kommunikativ-mediale Landschaft der Gegenwart beeinflusst auch die Art und Weise, wie demokratische Gesellschaften Themen verhandeln, wie Willensbildung erfolgt, wie politische und gesellschaftliche Diskurse ablaufen. Die kommerziellen Plattformen, auf denen oder über die vermittelt private wie öffentliche Kommunikation und der neue, gigantische Graubereich dazwischen heute stattfinden, arbeiten nach anderen Regeln als die alte Welt der Massenmedien. Immer deutlicher zeigt sich, dass die Mechanismen der Inhaltesortierung und Aufmerksamkeitsverteilung unter Umständen die Diskurse verschärfen. Sie scheinen gesellschaftliche Polarisierung zu fördern und, ohne dass das immer intendiert wäre, Echokammern für extreme und manchmal abseitige Ideologien und Gedankenwelten zu schaffen. Die liberalen Demokratien der Gegenwart und Zukunft werden sich dieser Veränderung weit intensiver und proaktiver widmen müssen als bisher, wenn die digitale Öffentlichkeit als konstruktiver und produktiver Ort der demokratischen Willensbildung funktionieren soll.

Der Aufmerksamkeitsmarkt sind wir

Der von dem deutschen Stadtplaner Georg Franck schon Anfang der 1990er Jahre geprägte Begriff der »Ökonomie der Aufmerksamkeit«[3] hat im Zeitalter der allgegenwärtigen digitalen Medien, dem Zeitalter der nahezu vollständigen Mediatisierung des Alltags, überragende Relevanz erreicht. Franck betrachtete die Aufmerksamkeitsökonomie als Konkurrenz zur klassischen Geldökonomie, hielt aber auch bereits 1993 fest: »Auflagenhöhen und Einschaltquoten messen die Aufmerksamkeit, die das Medium als Medium einnimmt. Sie messen auch seinen finanziellen Erfolg.«[4]

Heute erscheint eine strikte Unterteilung in Geld- und Aufmerksamkeitsökonomie auf den ersten Blick geradezu widersinnig: Mehrere der wertvolls-

3 Franck, Georg: »Ökonomie der Aufmerksamkeit«, MERKUR 47/534-535 (1993), S. 748-761.

4 Ebd.

ten börsennotierten Unternehmen der Welt machen ihre Umsätze maßgeblich mit dem Verkauf von Aufmerksamkeit, genauer: mit dem Verkauf und der Kanalisierung der Aufmerksamkeitszeit ihrer Nutzer*innen, allen voran Google, Facebook und deren Tochterunternehmen wie Youtube oder Instagram. Die Tatsache, dass dieses globale Geschäft so immens lukrativ ist, ist der vermutlich wichtigste Grund für die rapide Veränderung des Mediensystems in den vergangenen etwa 20 Jahren. Die »Aufmerksamkeitshändler«, wie Tim Wu, der Buchautor und frühere Berater von US-Präsident Barack Obama, die Plattformgiganten von heute nennt,[5] haben gelernt, einen nachwachsenden, aber dennoch begrenzten Rohstoff in hocheffizienter Weise zu fördern und zu Geld zu machen.

Dabei ist ein filigranes, nahezu beliebig abstufbares System der Aufmerksamkeitsvermarktung entstanden. Es kann beispielsweise sogenannten Mirko-Influencer*innen ein individuelles, auf persönlichen Aufmerksamkeitsangeboten basierendes Einkommen sichern. Als Mikro-Influencer*innen gelten gängigen Branchendefinitionen zufolge Menschen, die in sozialen Netzwerken wie der Facebook-Tochter Instagram oder auf der aus China stammenden Plattform TikTok 5000 bis 100.000 Follower, also Abonnent*innen, vorweisen können. Sie haben oft eine engagierte Fangemeinde und gelten in den Marketingabteilungen von Unternehmen, die sogenannte Kooperationen mit diesen Social-Media-Persönlichkeiten zu Vermarktungszwecken eingehen, als besonders authentische Markenbotschafter*innen.[6] Es handelt sich um ein Wachstumssegment: Einem Branchenbericht zufolge verdreifachte sich die Anzahl der Mikro-Influencer*innen, die derartige Kooperationen mit großen Unternehmen eingingen, von 2016 bis 2020.[7]

5 Wu, Tim: The attention merchants: the epic scramble to get inside our heads, First edition Aufl., New York: Alfred A. Knopf 2016.

6 Vgl. »Micro Influencer Definition | OnlineMarketing.de Lexikon«, OnlineMarketing.de https://onlinemarketing.de/lexikon/definition-micro-influencer

7 Vgl. »The State of Influencer Marketing 2020: Benchmark Report«, Influencer Marketing Hub https://influencermarketinghub.com/influencer-marketing-benchmark-report-2020/.

Gleiche und Gleichere in der Geld- und Aufmerksamkeitsökonomie

Es gibt aber nicht nur rein kommerziell motivierte Influencer*innen. Der Markt derer, die auf den neuen Plattformen um Aufmerksamkeit buhlen, ist deutlich breiter und umfasst auch Influencer*innen, also Beeinflusser*innen, mit anderen als kommerziellen Interessen. Manche sind wohlmeinende Aktivist*innen wie Greta Thunberg, andere Verschwörungstheoretiker*innen mit oder ohne Geschäftsmodell – der US-Amerikaner Alex Jones, Betreiber von »Infowars«, eines Angebots für US-Verschwörungstheoretiker*innen, verkauft zweifelhafte Nahrungsergänzungsmittel und andere Produkte an sein Publikum. Es gibt aber auch islamistische, rechtsextreme, esoterische ebenso wie ernsthaft an Bildungs- oder Hobbythemen interessierte Influencer*innen ohne direktes Monetarisierungsziel. Sie publizieren Fotos, Videos, Texte und Podcasts, sie pflegen ihre jeweiligen Communities, manche versuchen, diese zu aktivieren, andere, ihr Publikum zu (des-)informieren oder von irgendeiner Ideologie zu überzeugen. Diese neue, verwirrende, teils im Sinne der Partizipation begrüßenswerte, teils aber auch extrem problematische Vielfalt der Anbieter ist die Kehrseite der zum Ernten von Aufmerksamkeit optimierten Plattformen. Beide bedingen und befruchten einander. Die einen liefern den Zugang zum Publikum, die anderen den Content. Beide Seiten profitieren, auch wenn hier eine große Asymmetrie zugunsten der Plattformen und ihrer Anteilseigner herrscht.

Zumindest bei den kommerziell motivierten Influencer*innen besteht, ähnlich wie bei klassischen ganz oder teilweise werbefinanzierten Medien, eine enge Verknüpfung zwischen Aufmerksamkeits- und Geldökonomie. Die erfolgreichsten unter ihnen setzen zweistellige Millionenbeträge im Jahr um.[8] Die Tatsache, dass der internetöffentliche Konsum von Produkten, attraktiv präsentierten Hinweisen auf Reiseziele oder Restaurants oder mit für das Publikum unterhaltsamen Kommentaren unterlegte, aufgezeichnete oder live gestreamte Videospielsitzungen heute derartiges Unternehmertum ermöglichen, ist eine direkte Folge der ungleich größeren Aufmerksamkeitsverteiler, über die diese Inhalte veröffentlicht werden: die großen Internetplattformen. Die global reichweitenstärksten Internetangebote sind

8 Vgl. Berg, Madeline: »The Highest-Paid YouTube Stars of 2019: The Kids Are Killing It«, Forbeshttps://www.forbes.com/sites/maddieberg/2019/12/18/the-highest-paid-youtube-stars-of-2019-the-kids-are-killing-it/

fast ausnahmslos Angebote von kommerziellen Anbietern,[9] und das Gleiche gilt für die Rangliste der reichweitenstärksten Angebote in Deutschland.[10]

Debatten darüber, ob die Infrastruktur und die Öffentlichkeit herstellenden Dienste nicht öffentliche Güter sein sollten, als solche behandelt werden sollten oder es öffentlich gestützte Alternativen geben sollte, die nicht nur der Logik der Aufmerksamkeitsökonomie folgen, sind derzeit trotz alledem fast randständige Phänomene.

Die individuelle Monetarisierbarkeit von Aufmerksamkeit hat die Geld- und die Aufmerksamkeitsökonomie also noch stärker zusammenwachsen lassen, als das noch in der Zeit der Fall war, als Franck den Begriff prägte. Gleichzeitig ist die andere, nicht primär monetäre Motivation durch die »Währung Aufmerksamkeit«[11] immer noch präsent: Nicht nur kommerziell motivierte Influencer*innen buhlen um die Zeit und oft genug auch die Emotionen des Publikums. »Die Aufmerksamkeit anderer Menschen ist die unwiderstehlichste aller Drogen«, schrieb Franck. »Ihr Bezug sticht jedes andere Einkommen aus.«[12]

Tatsächlich ist es heute aber nicht nur die »Sucht« nach der belohnenden Wirkung, die die aufmerksamkeitshungrigen Akteur*innen von heute antreibt. Neben der gewissermaßen intrinsischen und der monetären Motivation werden manche von ihnen von höchst ehrenwerten, andere von düsteren, menschenverachtenden Motiven geleitet.

Die von der Schwedin Greta Thunberg ins Leben gerufene, von Kindern, Jugendlichen und jungen Erwachsenen getragene Klimaschutzbewegung »Fridays for Future« kämpft um die Aufmerksamkeit der Welt der Erwachsenen, damit die Menschheit damit aufhört, ihren eigenen Planeten für sich selbst unbewohnbar zu machen. Aber auch Massenmörder wie der Rechtsterrorist von Christchurch, der seine Morde live ins Netz streamte, oder die Attentäter vom 13. November 2015 in Paris hatten das Ziel, globale Aufmerksamkeit zu erreichen. Die Terroristen von Paris etwa hatten eigentlich vor, ihren Angriff auf die Stadt mit Bombenexplosionen in einem vollbesetzten Fußballstadion während eines deutsch-französischen Länderspiels zu beginnen, um von Anfang an globale mediale Aufmerksamkeit auf ihre Untaten

9 Vgl. »Alexa – Top sites«, ohne Datum, https://www.alexa.com/topsites/

10 Vgl. »Alexa – Top Sites in Germany – Alexa«, ohne Datum, https://www.alexa.com/topsites/countries/DE

11 Franck, Georg: »Die neue Währung: Aufmerksamkeit.«, MERKUR 43/486 (1989), S. 688-701.

12 Franck: »Ökonomie der Aufmerksamkeit«.

zu ziehen. Auch andere große Terrorakte der vergangenen Jahre waren als menschenverachtende, sich über Stunden hinziehende Live-Ereignisse inszeniert,[13] mittlerweile wird dieses Muster zur Norm.[14]

Die Täter kalkulierten augenscheinlich oft auch ein, dass ihre Taten durch die tragbaren Medienproduktionsgeräte, die fast jede*r heute bei sich hat, und über die Always-on-Medienplattformen im Netz nahezu in Echtzeit in die Welt übertragen werden können, von einer dezentralen Schar von zu Reporter*innen gewordenen Augenzeug*innen.

Eine andere direkte Folge der neuen Mechanismen: Der Präsident einer führenden Industrienation wickelte einen großen Teil seiner öffentlichen Politik und Wähler*innenansprache und -mobilisierung über soziale Netzwerke ab, bis auch er auf Basis des privaten Hausrechts, der Allgemeinen Geschäftsbedingungen, vor die Tür gesetzt, gesperrt wurde. Auch dieser Präsident agierte auf dem gleichen Markt, wie die oben genannten Akteur*innen. Donald Trump war bis zur Sperrung seiner Accounts gewissermaßen Influencer-in-Chief. Nach der Sperrung bezog er sich auf das in der Verfassung garantierte Recht *freedom of speech*. Die sperrenden Dienste wiederum pochten auf ihre Freiheit als private Anbieter, ihre Hausregeln durchzusetzen.

Die genannten Beispiele zeigen, dass das nicht monetär motivierte Streben nach Aufmerksamkeit sich pauschalen normativen Kategorisierungen entzieht: Welches Ziel die Akteur*innen der Aufmerksamkeitsökonomie letztendlich verfolgen, ist entkoppelt von den Marktplätzen, auf denen sie mit allen übrigen, auch den kommerziell oder vom Streben nach Ruhm, Einfluss oder anderen Zielen motivierten Akteur*innen der Aufmerksamkeitsökonomie konkurrieren.

Wir sind nicht auf dem Marktplatz, wir sind der Marktplatz

Das verbindende Element sind in allen genannten Fällen eben diese Marktplätze. Sie wurden konstruiert, um bestimmte Zwecke für die Nutzer*innen zu realisieren und deren Aufmerksamkeit gleichzeitig für die Betreiber der

13 Vgl. Stöcker, Christian: »Orlando-Massaker, Paris-Anschläge: Der Live-Terror kommt«, DER SPIEGEL, 2016, https://www.spiegel.de/netzwelt/netzpolitik/orlando-massaker-paris-anschlaege-der-live-terror-kommt-a-1098005.html.

14 Vgl. Stöcker, Christian: »Halle: In diesen Online-Biotopen gedeihen die Terror-Influencer«, DER SPIEGEL, 2019, https://www.spiegel.de/wissenschaft/mensch/halle-in-diesen-online-biotopen-gedeihen-die-terror-influencer-a-1291160.html

Marktplätze monetarisierbar zu machen. Sie unterscheiden sich jedoch in den Mechanismen, die zum Ernten und zur Bündelung der Aufmerksamkeit eingesetzt werden.

Wie diese Mechanismen genau aussehen und wie die Ziele operationalisiert werden, ist im Einzelfall unterschiedlich. Gemeinsam ist den kommerziellen Plattformen aber eines: Ihre primären Zielsetzungen sind nicht gesellschaftlicher, sondern wirtschaftlicher Natur. Die Spielflächen, auf denen sich die deliberative Öffentlichkeit nun manifestiert, werden unter dem Gesichtspunkt der Profitmaximierung gestaltet und betrieben. Werte und Ziele, wie sie etwa der deutschen Medienregulierung zugrunde liegen (siehe weiter unten), spielen keine oder zumindest eine stark untergeordnete Rolle. Gleichzeitig ist die Teilnahme an dieser neuen kommunikativen Sphäre an Eintrittsbedingungen geknüpft, die wiederum primär kommerziellen Zwecken dienen. Die Betreiber der großen Plattformen sammeln sämtlich mehr Daten über ihre Nutzer*innen, als dies zur Optimierung der Dienste selbst notwendig wäre. Sie tun das, weil sich Aufmerksamkeitspakete, die in zielgruppenspezifischen Bündeln zusammengepackt sind, besonders gut monetarisieren lassen. Gleichzeitig versuchen sie Investitionen, die negative Auswirkungen ihrer Systeme vermeiden oder wenigstens eindämmen sollen, so weit als möglich zu unterlassen, weil sie die Gewinne schmälern – direkt durch die Investitionen etwa in menschliche Content-Moderation und unter Umständen indirekt, weil zum Beispiel bestimmte aufmerksamkeitsstarke Inhalte ausgeblendet werden müssten. Die deliberative Demokratie informiert sich, debattiert und unterhält sich mittlerweile mindestens zum Teil an Orten, die dafür nicht gemacht sind. Und das hat sehr reale, bereits klar erkennbare Konsequenzen.

Eine Suchmaschine wie Google erschließt eine gigantische Zahl von Informationsquellen für ihre Nutzer*innen – und monetarisiert deren Aufmerksamkeit und daraus ableitbare Informationen über Konsumverhalten, am effektivsten vermutlich immer dann, wenn diese Nutzer*innen tatsächlich gerade auf der Suche nach kommerziell relevanten Informationen sind. Aber eben auch sonst, egal, ob sich Nutzer*innen gerade für den Holocaust, Kritik an Impfungen oder Verschwörungstheorien interessieren.

Ein soziales Netzwerk wie Facebook bietet seinen Nutzer*innen eine einfache, komfortable und im Idealfall unterhaltsame Möglichkeit, den eigenen Freundes- und Bekanntenkreis zu pflegen – und monetarisiert deren Aufmerksamkeit, indem es einerseits die im Netzwerk verbrachte Zeit an sich per Werbeanzeige käuflich macht, und es andererseits Unternehmen erlaubt, in

diesem doch ursprünglich für private Kontakte gedachten Umfeld Kundenbeziehungen aufzubauen und zu pflegen. Und Kunde ist im weitesten Sinne zu verstehen. Microtargeting und Dark Ads sind auch Instrumente, um individuelle oder kollektive Willensbildungsprozesse zu beeinflussen, beispielsweise demokratische Wahlen, wie uns der Fall Cambridge Analytica vor Augen geführt hat. In der Logik von Aufmerksamkeitsbrokern ist auch die Aufmerksamkeit von Wähler*innen vermarktbar. Mit Twitter und anderen sozialen Netzwerken teilt Facebook einen Mechanismus der Aufmerksamkeitsbündelung, der sich von dem unterscheidet, den etwa Suchmaschinen einsetzen: durch die einfach zu handhabenden Sharing-Funktionen wird Viralität ermöglicht, weiter angeheizt durch algorithmische Sortiersysteme, die den vielversprechendsten Kandidaten für maximalen Aufmerksamkeitswert ein noch größeres Publikum verschaffen sollen.

Auf diesen Plattformen, die einem relativ scharf definierten, klar umrissenen ursprünglichen Zweck dienen, haben sich emergente Phänomene der Aufmerksamkeitsökonomie entwickelt, die sich die genannten Mechanismen der Plattformen zunutze machen, um Aufmerksamkeit zu binden und zu monetarisieren. Social-Media-Influencer*innen sind ein Beispiel für diese emergenten Phänomene, dezentrale, lose Terrornetzwerke wie das des sogenannten Islamischen Staats oder die wachsende Zahl digital sozialisierter und radikalisierter Rechtsterroristen von Norwegen bis Neuseeland sind weitere.[15] Aber auch Hashtag-basierte soziale Bewegungen von #MeToo bis #FridaysforFuture sind ohne die zu gänzlich anderen Zwecken konzipierten neuen Plattformen zur Aufmerksamkeitsvermarktung der digitalen Gegenwart nicht denkbar, ebenso wie mittlerweile internationalisierte neue Verschwörungserzählungen wie »QAnon«.[16]

Suchende Lichtkegel in der Medienwelt

Man kann sich diese neue Medienwelt wie eine gewaltige Landschaft vorstellen, deren Oberfläche beständig von Suchscheinwerfern mit sich permanent

15 Vgl. Stöcker, Christian: »Anschlag in Neuseeland: Monster, die sich für Helden halten«, DER SPIEGEL, 2019, https://www.spiegel.de/wissenschaft/mensch/anschlag-in-neuseeland-monster-die-sich-fuer-helden-halten-a-1258159.html

16 Kozlowska, Hanna: »Facebook is a perfect place for conspiracy theories like QAnon to evolve«, Quartz, 2019, https://qz.com/1348635/facebook-is-a-perfect-home-for-conspiracy-theories-like-qanon/

veränderndem Lichtkegel abgetastet wird. Jeder Lichtstrahl setzt sich aus der Aufmerksamkeit von manchmal Dutzenden, manchmal Tausenden und zuweilen Millionen von Nutzer*innen zusammen, gesammelt und gebündelt von den Unternehmen, die die großen Plattformen betreiben.

Die Zahl der Lichtkegel ist viel größer als noch im vordigitalen Zeitalter, doch der Radius einzelner Kegel ist oft viel kleiner: Die Aufmerksamkeit des Publikums verteilt sich über eine ungleich größere Menge an Inhalten als früher. Jürgen Habermas formulierte es in einem 2008 erschienenen Essay so: »Dieses Publikum zerfällt im virtuellen Raum in eine riesige Anzahl von zersplitterten, durch Spezialinteressen zusammengehaltenen Zufallsgruppen. Auf diese Weise scheinen die bestehenden nationalen Öffentlichkeiten eher unterminiert zu werden.«[17] Die von den Scheinwerferkegeln bestrichene Landschaft selbst aber wird sekündlich größer und größer. Die Aufmerksamkeit des Publikums ist auf teils filigrane Weise über die ständig rasant weiterwachsende Gesamtmenge der potenziellen Aufmerksamkeitsgegenstände verteilt, ständig in Bewegung.

Neue Zentren und Ziele für die Lichtkegel entstehen, andere vergehen. Manche Teile der Landschaft werden für einen kurzen Moment hell erleuchtet und verschwinden dann wieder im Dunkeln. Anderswo wachsen Lichtkegel langsam immer weiter an, weitere schrumpfen nach und nach, bis sie schließlich nicht mehr zu sehen sind. Die Landschaft selbst besteht aus den Hervorbringungen von Gaming-, Mode-, Spielzeug-, Kosmetik-, Reise- oder Koch-Influencer*innen, aus Lexikoneinträgen und wissenschaftlichen Fachveröffentlichungen, aus kurzen Nachrichten und langen Reportagen, aus Videoclips über Extremsportarten, dressierte Tiere oder seltsame Hobbys, aus Bombenbauanleitungen, aus Holocaustleugner-Websites, aus Kurz- und Spielfilmen, Konzertaufnahmen und Punk-Singles, aus Klassikern der Weltliteratur und Pornografie, aus religiösen Texten, künstlerisch wertvollen Fotografien, den Katalogen ganzer Museen, aus Protestnoten, Pamphleten und den Manifesten von Massenmördern.

Wie eingangs erwähnt: Mittlerweile gilt es als außergewöhnlich, wenn jemand bei seinem Tod *keinen* »Online-Fußabdruck« hinterlässt. In vielen Ländern rund um den Globus ist es zu einem selbstverständlichen Teil der Existenz geworden, die Menge der im Internet verfügbaren digitalen Inhalte auch persönlich weiter zu vergrößern, auf welche Weise auch immer.

17 Habermas, Jürgen: Ach, Europa: Kleine Politische Schriften XI, Originalausgabe Aufl., Frankfurt a.M.: Suhrkamp 2008.

In diesem neuen, hochgradig vernetzten, von hoher Geschwindigkeit, Multimedialität und Emotion geprägten Ökosystem sind sowohl traditionelle Medienunternehmen als auch andere klassische Akteur*innen professionalisierter öffentlicher Kommunikation zum Teil noch immer auf der Suche nach ihrem Platz, ihrer Funktion und Rolle – und oft genug auch auf der Suche nach einem funktionierenden Geschäftsmodell.

Das klassische Modell der Tageszeitung etwa, das auf einer hybriden Finanzierung aus Vertriebserlösen und Aufmerksamkeitsvermarktung über Werbung und Kleinanzeigen basierte, hat sich bislang größtenteils nicht in befriedigender Weise in diese neue Medienwelt übertragen lassen. Die neuen Aufmerksamkeitsvermarkter sind so viel mächtiger und effizienter, das Angebot an potenziellen Werbeflächen so viel größer als das, was traditionelle Verlagshäuser anzubieten haben, dass das alte Geschäftsmodell nicht mehr richtig funktioniert. Folgerichtig schrumpfen sowohl Auflagen als auch Anzeigenerlöse immer weiter. Gleichzeitig können die auf traditionellen Nachrichtenfaktoren[18] basierenden Auswahl- und Relevanzkriterien redaktionell arbeitender Angebote zuweilen nicht mit den für Aufmerksamkeitsbindung optimierten Konkurrenzangeboten der algorithmisch kuratierten Plattformen mithalten.

Die neue, plattformbasierte digitale Aufmerksamkeitsökonomie ist dabei kein statisches System, sondern selbst im permanenten Wandel begriffen. Die Plattformbetreiber passen kontinuierlich ihre Benutzeroberflächen an, es gibt Wechselwirkungen zwischen neuen Gerätetypen und -klassen für den Zugang zur digitalen Medienwelt, neue Konkurrenten wie TikTok (Social Media) oder Disney+ (Video-Streaming). Es gibt Trends, Moden und längerfristige Entwicklungen wie die hin zu privaten Messenger-Systemen, die für viele die großen Allround-Social-Media-Plattformen wie Facebook zumindest teilweise abgelöst haben. Die Plattformen sind untereinander wiederum vernetzt und verzahnt: Eine Google-Suche kann zu einem Facebook-Post oder Instagram-Foto führen, ein bei Facebook geposteter Link auf einen Nachrichtenartikel in einem klassischen redaktionellen Medium verweisen – oder auf das neueste Video eines Verschwörungstheoretikers bei Youtube. Im Jahr 2020 wurden im Zuge der Corona-Pandemie im Messenger Telegram

18 Vgl. Galtung, Johan und Mari Holmboe Ruge: »The Structure of Foreign News«, Journal of Peace Research 2/1 (1965), S. 64-91.

abonnierbare Kanäle von Verschwörungs-Influencer*innen[19] und Rechtsextremen[20] zu einer neuen Quelle, aus der sich wiederum Youtube-Videos, Facebook-Posts und andere Social-Media-Inhalte speisten.

Einige Konstanten oder besser: einige vermutlich dauerhaft haltbare Grundprinzipien lassen sich mittlerweile trotz des in einem ständigen Veränderungsprozess begriffenen neuen medialen Ökosystems ableiten:

(1) Die Gesamtmenge der verfügbaren Information – dieser Begriff ist hier wertfrei im Sinne der Definition von Shannon und Weaver[21] zu verstehen, also ohne Bezug auf Bedeutung oder gar Qualität – wird weiterhin stetig steigen. Dabei spielt auch eine Rolle, dass durch die ständig wachsenden technischen Möglichkeiten und das zunehmende Vorhandensein digitaler Breitbandzugänge auch die Zahl der potenziellen und tatsächlichen Anbieter von Information zumindest bis auf Weiteres kontinuierlich wachsen wird.[22]
(2) Die Menge der verfügbaren menschlichen Aufmerksamkeitszeit ist in jedem Fall endlich, auch wenn sie aus Sicht der Plattformbetreiber vermutlich durch Marketing, weitere Optimierung von Benutzeroberflächen, den Gewinn von Marktanteilen und die Erschließung gänzlich neuer Märkte, etwa in Entwicklungs- und Schwellenländern, vorerst noch ausgebaut werden kann.
(3) Die Verteilung der finiten Menge an menschlicher Aufmerksamkeitszeit auf eine ständig wachsende Menge verfügbarer Information (wiederum im wertneutralen Sinne von Shannon und Weaver) wird aller Wahrscheinlichkeit nach weiterhin mindestens teilweise von automatisierten Entscheidungssystemen (Automated Decision Making, ADM-Systemen) ge-

19 Vgl. Stöcker, Christian: »Corona-Verschwörungstheorien: Detlef, Ken und Attila wissen Genaueres«, DER SPIEGEL, 2020, https://www.spiegel.de/wissenschaft/mensch/corona-verschwoerungstheorien-detlef-ken-und-attila-wissen-genaueres-kolumne-a-e10ce3d3-1826-467d-8d2a-204f304b1378

20 Vgl. Stöcker, Christian: »Corona und QAnon: Das Unbehagen der deutschen Nazis«, DER SPIEGEL, 2020, https://www.spiegel.de/wissenschaft/mensch/corona-und-qanon-das-unbehagen-der-deutschen-nazis-a-98a0f18b-cb82-4543-aeda-1d455152c2ea

21 Shannon, Claude E. und Warren Weaver: The mathematical theory of communication, Urbana: University of Illinois Press 1975.

22 Vgl. Hilbert, M. und P. Lopez: »The World's Technological Capacity to Store, Communicate, and Compute Information«, Science 332/6025 (01.04.2011), S. 60-65.

steuert werden,[23] einfach deshalb, weil die Kuratierung der ständig rapide wachsenden Gesamtmenge an Information anders nicht mehr zu handhaben ist – jedenfalls nicht auf für die Plattformbetreiber lukrative Weise. Zusätzlich werden Diensteanbieter auch durch die staatliche Zuschreibung von gesellschaftlicher Verantwortung dazu gedrängt, Technologien zu nutzen, die nahezu in Echtzeit und automatisiert Inhalte kuratieren oder zum Verschwinden bringen – man denke etwa an die automatisierten Pornografie-Filter, die Youtube einsetzt. Das heißt, dass die Plattformbetreiber ihre Maschinen auch entscheiden lassen, bestimmte Inhalte nicht öffentlich zugänglich zu machen.

(4) Neben der algorithmisch, durch ADM-Systeme kuratierten Inhaltezuordnung zu einzelnen Nutzer*innen werden weiterhin von Menschen, also redaktionell kuratierte Informations- und Unterhaltungsangebote Bestand haben. Diese Angebote müssen sich auf einem umkämpften Markt jedoch gegen die ADM-kuratierten Angebote behaupten und gleichzeitig ihre eigene Monetarisierung sicherstellen, ohne auf die Skaleneffekte bauen zu können, die den gewaltigen ADM-kuratierten Systemen einen Wettbewerbsvorteil verschaffen. In Zukunft wird die Angebotsflut durch automatisiert erstellte Inhalte womöglich noch schneller anwachsen.

(5) Das ursprüngliche Bestreben mancher Plattformbetreiber, möglichst vollständige Öffentlichkeit auch privater Kommunikation und Information zur Norm zu erheben,[24] kann als gescheitert gelten. Gerade jüngere und versiertere Nutzer*innen digitaler Kommunikationsmedien weichen für große Teile ihrer auf diesem Weg abgewickelten privaten Kommunikation mittlerweile auf Ende-zu-Ende-verschlüsselte Messenger-Dienste wie WhatsApp, Signal oder Threema aus. Diese »privaten Öffentlichkeiten«, wie die Internetforscherin danah boyd dieses Phänomen schon 2008 genannt hat,[25] sind weiterhin persistent und duplizierbar (etwa in Form von Screenshots oder Kopien von Chatverläufen), aber nicht ohne Weiteres durchsuchbar und auch nicht von außen einzusehen. Sie entziehen sich

23 Vgl. Lischka, Konrad und Christian Stöcker: »Digitale Öffentlichkeit«, Bertelsmann Stiftung 2017.

24 Vgl. Stöcker, Christian: »Facebook: Warum kehrt Mark Zuckerberg von seinem Theorem ab?«, DER SPIEGEL, 2019, https://www.spiegel.de/wissenschaft/medizin/facebook-warum-kehrt-mark-zuckerberg-von-seinem-theorem-ab-a-1256929.html

25 boyd, danah: »Taken Out of Context: American Teen Sociality in Networked Publics«, Dissertation, University of California-Berkeley, School of Information 2008, https://www.ssrn.com/abstract=1344756

damit auch der algorithmischen Kuratierung und Sortierung. Zum zentralen Ordnungsprinzip wird wieder die Chronologie der Kommunikationsvorgänge. Hinzu kommt die zunehmende Teilöffentlichkeit von Kanälen von Messengerdiensten wie Telegram, die von tausenden Menschen abonniert werden. Der Gesetzgeber hat hier noch keinen regulativen Zugriff gefunden, da sich diese im neu entstandenen Graubereich zwischen privater und öffentlicher Kommunikation bewegen.

(6) Zumindest solange die Geschäftsmodelle der ADM-basierten Aufmerksamkeitsverteiler auf der Monetarisierung von Aufmerksamkeitszeit durch Werbung fußen, wird ein nicht auflösbarer Widerspruch zwischen den Kuratierungsentscheidungen der ADM-Systeme und klassischen Kriterien für inhaltliche Qualität wie Wahrhaftigkeit, Angemessenheit, Jugendschutz, Ausgewogenheit, Schutz der Menschenwürde, Förderung des gesellschaftlichen Zusammenhalts oder des Gemeinwohls bestehen bleiben. Die Optimierungsziele der Plattformbetreiber orientieren sich letztlich an ihren kurz- und langfristigen Umsatzzielen.

Stationäre versus fliegende Händler

Der letzte Punkt macht deutlich, wo sich das in ständigem Wandel begriffene digitale Mediensystem mit Blick auf seine Leitprinzipien stark von der nach dem Zweiten Weltkrieg in Deutschland etablierten Medienordnung unterscheidet. Exemplarisch lässt sich das nachzeichnen anhand der im deutschen Rundfunkstaatsvertrag niedergelegten Aufgaben des öffentlich-rechtlichen Rundfunks (II. Abschnitt, Paragraph 11, Absatz 1 und 2)[26], die hier stellvertretend für die im demokratischen Prozess ausgehandelten Ziele der Medienordnung an sich herangezogen werden sollen:

> »(1) Auftrag der öffentlich-rechtlichen Rundfunkanstalten ist, durch die Herstellung und Verbreitung ihrer Angebote als Medium und Faktor des Prozesses freier individueller und öffentlicher Meinungsbildung zu wirken und dadurch die demokratischen, sozialen und kulturellen Bedürfnisse der Gesellschaft zu erfüllen. Die öffentlich-rechtlichen Rundfunkanstalten haben in

26 »Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag) vom 31. August 1991, zuletzt geändert durch den Zwanzigsten Rundfunkänderungsstaatsvertrag vom 8. bis16. Dezember 2016«, ohne Datum.

> ihren Angeboten einen umfassenden Überblick über das internationale, europäische, nationale und regionale Geschehen in allen wesentlichen Lebensbereichen zu geben. Sie sollen hierdurch die internationale Verständigung, die europäische Integration und den gesellschaftlichen Zusammenhalt in Bund und Ländern fördern. Ihre Angebote haben der Bildung, Information, Beratung und Unterhaltung zu dienen. Sie haben Beiträge insbesondere zur Kultur anzubieten. Auch Unterhaltung soll einem öffentlich-rechtlichen Angebotsprofil entsprechen.
> (2) Die öffentlich-rechtlichen Rundfunkanstalten haben bei der Erfüllung ihres Auftrags die Grundsätze der Objektivität und Unparteilichkeit der Berichterstattung, die Meinungsvielfalt sowie die Ausgewogenheit ihrer Angebote zu berücksichtigen.«

Auf den ersten Blick wird deutlich, dass zumindest Teile der hier formulierten Ziele sich theoretisch auch mithilfe algorithmisch kuratierter digitaler Informationsplattformen verfolgen lassen, beziehungsweise dass diese Plattformen heute längst dazu eingesetzt werden: Zweifellos erfüllen Google, Facebook, Instagram, Youtube, TikTok, aber auch Anbieter kostenpflichtiger Video- oder Musik-, Hörbuch-, vermehrt auch Games- und Podcast-Streaming-Dienste »soziale und kulturelle Bedürfnisse«, und all diese Angebote werden zweifellos auch zum Zweck der »Bildung, Information, Beratung und Unterhaltung« genutzt. Auch auf die Meinungsbildung haben derartige Plattformen bereits heute einen gewichtigen, wenn auch, gesamtgesellschaftlich betrachtet, nach wie vor keinen überragenden Einfluss, wie der »Reuters Digital News Report«[27] Jahr für Jahr zeigt.

Gleichzeitig gibt es immer mehr Belege dafür, dass im Rundfunkstaatsvertrag als Zielvorgaben formulierte Grundsätze wie Objektivität und Ausgewogenheit sich in den automatisierten Kuratierungsentscheidungen etwa von Google, Facebook und Youtube oft gar nicht oder nicht in angemessener Weise niederschlagen.[28] An Vielfalt herrscht zwar kein Mangel, doch diese Vielfalt umfasst häufig auch höchst problematische, teils gefährliche, teils grob irreführende, teils justiziable Inhalte. Auch erscheint mindestens fraglich, ob das Ziel eines »umfassenden Überblicks über das internationale, europäische, nationale und regionale Geschehen in allen wesentlichen Lebensbereichen«

27 Reuters Institute digital news report, https://www.digitalnewsreport.org

28 Vgl. Stöcker, Christian: »How Facebook and Google accidentally created a perfect ecosystem for targeted disinformation«, in: Grimme, Christian und Mike Preuss (Hg.): Conference Proceedings Misdoom 2019, Lecture Notes in Computer Science, in press.

sich nur auf Basis der automatisierten, durch die Angabe persönlicher Präferenzen der Nutzer*innen modifizierten Kuratierungsentscheidungen solcher Plattformen in der alltäglichen Praxis erreichen lässt. Eine deliberative Demokratie, deren Informationen ausschließlich auf mit monetären Optimierungszielen ausgestatteten Informationsplattformen beruht, gerät über kurz oder lang in Schwierigkeiten. Klare Anzeichen dieser Entwicklung sind schon jetzt nicht mehr zu übersehen, von Corona-Leugner*innen in Deutschland bis hin zu gewaltbereiten Anhänger*innen des Ex-Präsidenten und aggressiven Verschwörungstheoretiker*innen in den USA. Der Sturm auf das US-Kapitol am 6. Januar 2021 wurde nachweislich auf diversen Internetplattformen geplant und vorbereitet.

Exemplarisch soll an dieser Stelle kurz anhand der drei wichtigsten, reichweitenstärksten unter den großen Plattformen dargelegt werden, warum das so ist: Facebook, Google und die Google-Tochter Youtube.

Facebook

Das zentrale Optimierungsziel von Facebook, gewissermaßen das als Näherung für Aufmerksamkeitsbindung eingesetzte Maß, ist »Engagement«. Damit ist die Kombination von innerhalb der Plattform möglichen Formen der Interaktion mit einem gegebenen Inhalt gemeint; zusätzlich erfasst Facebook eine Vielzahl weiterer Messgrößen, um Kuratierungsentscheidungen innerhalb des sogenannten Newsfeeds zu treffen:

(1) Klicks auf den »gefällt mir«-Button (»Likes«) oder andere Ein-Klick-Reaktionen wie Emojis, Shares, also Weiterreichungen des Inhalts innerhalb der Plattform, sowie Kommentare,[29] die Beziehung zwischen dem »Sender« und dem »Empfänger« des jeweiligen Inhalts, vorangegangene Interaktionen des Empfängers mit anderen Inhalten, Interaktionen anderer Nutzer*innen mit dem jeweiligen Inhalt und diverse andere Kriterien. Erfasst werden dabei auch Maße wie die Scrollgeschwindigkeit etwa bei der Nutzung der Smartphone-App von Facebook oder der Webseite.

29 Vgl. Stöcker, Christian und Konrad Lischka: »Wie algorithmische Prozesse Öffentlichkeit strukturieren«, in: (Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft, Fraunhofer Focus, hg. von Resa Mohabbat Kar, Basanta EP Thapa und Peter Parycek, Berlin 2018, S. 28.

Solche und weitere Kriterien, auf deren Basis Facebooks System permanent automatisierte Kuratierungs- also letztlich individualisierte Relevanzentscheidungen fällt, treten jedoch in Wechselwirkung zu anderen Faktoren. Dazu gehören unter anderem Folgende:

(1) Personen mit laut Selbstauskunft extremen oder radikalen politischen Einstellungen sind, zumindest in Deutschland, tendenziell aktiver in den sozialen Medien als andere, politisch moderate Nutzer*innen: Sie erzeugen also überproportional viel »Engagement«[30].
(2) Facebooks Benutzeroberfläche ist für maximales Engagement und damit gleichzeitig für möglichst geringe kognitive Anstrengung optimiert, was einen Informationsverarbeitungsmodus begünstigt, der wiederum anfällig für kognitive Verzerrungen und emotionale Reaktionen ist.[31]
(3) Emotionalisierende Inhalte erzeugen auf sozial-medialen Plattformen tendenziell mehr »Engagement«, was mittlerweile vielfach empirisch nachgewiesen werden konnte.[32]
(4) Gerade Akteure, die etwa Desinformation und Propaganda verbreiten möchten, können sich diese Faktoren gezielt zunutze machen, also ihre Botschaften beliebig emotionalisierend gestalten, ohne dabei Rücksicht auf Quellen oder Wahrhaftigkeit nehmen zu müssen.

Gemeinsam treten diese Faktoren in eine teils unheilvolle Wechselwirkung: Emotionalisierende Inhalte, besonders aktive Nutzer*innen aus dem Bereich politischer Extreme, eine Oberfläche, die so gestaltet ist, dass sie möglichst niederschwellige, gedankenlose Interaktion begünstigt und damit kognitiven Verzerrungen Vorschub leistet, treffen auf ein Kuratierungssystem, das entsprechenden Inhalten, die aufgrund dieser Faktoren besonders hohes »Engagement« erzeugen, wiederum zusätzliche Reichweite und damit »Engagement«-Möglichkeiten verschafft.

30 Vgl. Stöcker: »How Facebook and Google accidentally created a perfect ecosystem for targeted disinformation«.
31 Vgl. Lischka/Stöcker: »Digitale Öffentlichkeit«.
32 Vgl. Stöcker, Christian: »Bedeutung von Emotionen in den Sozialen Medien, Emotionalisierung durch Soziale Medien: Emotion bringt Reichweite?«, in: Besand, Anja, Bernd Overwien und Peter Zorn (Hg.): Politische Bildung mit Gefühl, Bd. 10299, Schriftenreihe der Bundeszentrale für politische Bildung, Bonn: Bundeszentrale für politische Bildung 2019.

Es gibt mittlerweile eine Vielzahl gut dokumentierter Beispiele dafür, was diese komplexe, aber unbestreitbare Wechselwirkung unter Umständen zur Folge haben kann. So ist Facebook zu einem Biotop geworden für die Propaganda von Impfgegner*innen,[33] für irreführende Informationen über das Zika-Virus,[34] die von der US-Bundespolizei FBI als terroristische Gefahr eingestufte QAnon-Verschwörungserzählung[35] und selbstverständlich auch für die Verschwörungsthesen von Corona-Leugner*innen im Jahr 2020.[36]

Google

Auch Google, mit weitem Abstand die dominante Suchmaschine in Deutschland und vielen anderen Märkten, hat ein Problem mit Des- und Misinformation auf hohen Ergebnisrängen. Während Google selbst keine detaillierten Informationen über die konkreten Kriterien seines Ranking-Algorithmus veröffentlicht (mit wenigen Ausnahmen[37]), gibt es professionelle Anbieter von Suchmaschinenoptimierung für Webseiten-Betreiber, die entsprechende Kriterien ableiten und zugänglich machen.[38]

Zu den »Nutzer*innen-Signalen«, die Google unter anderem auswertet, gehört demnach:

(1) Die sogenannte Click-Through-Rate, also die Häufigkeit, mit der auf einen bestimmten Link auf einer Ergebnisseite geklickt wird,
(2) der Anteil der Nutzer*innen, die nach einem Klick auf einen Ergebnislink sofort wieder zur Trefferseite zurückkehren und

33 Vgl. Wong, Julia Carrie: »Anti-vaxx propaganda has gone viral on Facebook. Pinterest has a cure«, The Guardian, 21.02.2019, https://www.theguardian.com/technology/2019/feb/20/pinterest-anti-vaxx-propaganda-search-facebook.

34 Vgl. Sharma, Megha u.a.: »Zika virus pandemic—analysis of Facebook as a social media health information platform«, American Journal of Infection Control 45/3 (03.2017), S. 301-302.

35 Vgl. Kozlowska: »Facebook is a perfect place for conspiracy theories like QAnon to evolve«; Wilson, Jason: »Conspiracy theories like QAnon could fuel ›extremist‹ violence, FBI says«, The Guardian, 01.08.2019, https://www.theguardian.com/us-news/2019/aug/01/conspiracy-theories-fbi-qanon-extremism

36 Vgl. Stöcker: »Corona-Verschwörungstheorien«.

37 Vgl. Garb, Rachel: »More transparency in customized search results«, 30.07.2008, https://googleblog.blogspot.de/2008/07/more-transparency-in-customized-search.html.

38 Vgl. Dean, Brian: »Google's 200 Ranking Factors: The Complete List«, 05.11.2016, http://backlinko.com/google-ranking-factors

(3) die sogenannte Dwell Time, also die Zeit, die ein/e Nutzer*in auf der jeweiligen Seite verbringt, nachdem er oder sie einen Ergebnislink angeklickt hat. Längere Verweildauern werden als Signal für der Suchanfrage angemessene Ergebnisse gewertet.

Diese Kriterien, und vermutlich Hunderte weitere, werden mit den Urteilen der sogenannten Quality Rater, die Google beschäftigt,[39] verrechnet, um schließlich für Milliarden von Suchanfragen pro Tag zu entscheiden, wie die Ergebnisse sortiert werden. In vielen Fällen funktioniert dieses System so gut, dass es Google in zahlreichen Ländern rund um die Welt die Marktführerschaft beschert hat. In anderen Fällen fördern auf diese Weise erzeugte Ergebnisseiten Desinformation oder sogar justiziable Inhalte zutage.

Noch im Jahr 2016 lieferte eine Google-Suche auch in Deutschland unter Umständen unter den ersten Treffern zu bestimmten Suchanfragen Links zu Webseiten, auf denen der Holocaust geleugnet wurde.[40] Auch bei Google wurden Impfgegner-Webseiten auf diese Weise einem erweiterten Publikum zugänglich gemacht.[41] Click-Through-Rate und Dwell Time sind bei bestimmten Suchanfragen, die ein in diesem Bereich möglicherweise verunsichertes Publikum anziehen, offenbar zuweilen sehr schlechte Ratgeber, wenn es um echte Relevanz oder gar Qualität geht.

Youtube

Bei Youtube ist das zentrale Optimierungsziel die Gesamt-Sehdauer, über mehrere aufeinanderfolgende Videos hinweg, wie ein Entwickler bereits 2012 verriet.[42] 2016 erschien eine Fachveröffentlichung von Youtube-Entwickler*innen, der zufolge an dieser Optimierungsaufgabe mittler-

39 Vgl. Google: »General Guidelines«, 14.03.2017, https://static.googleusercontent.com/media/www.google.com/de//insidesearch/howsearchworks/assets/searchqualityevaluatorguidelines.pdf

40 Vgl. Mierau, Caspar Clemens: »Fake News zum Holocaust sind noch immer Top-Treffer auf Google – Motherboard«, 15.12.2016, https://motherboard.vice.com/de/article/holocaust-leugnungen-google

41 Vgl. Stöcker, Christian: »Impfgegner: Tödliche Dummheit – «, DER SPIEGEL, 2019, https://www.spiegel.de/wissenschaft/medizin/impfgegner-toedliche-dummheit-a-1255983.html

42 Vgl. Meyerson, Eric: »YouTube Now: Why We Focus on Watch Time«, YouTube Creators' Blog, 2012, https://youtube-creators.googleblog.com/2012/08/youtube-now-why-we-focus-on-watch-time.html

weile in zentraler Weise künstliche neuronale Netze für das maschinelle Lernen eingesetzt werden.[43] Bereits im Jahr 2015 führte Youtube den sogenannten Autoplay-Mechanismus ein, der, wenn der/die Nutzer*in nicht explizit widerspricht, dafür sorgt, dass nach dem Ende jedes Videos automatisch das nächste, algorithmisch vorgeschlagene Video anläuft. Dieses Empfehlungssystem ist so erfolgreich, dass schon im Jahr 2018 laut einem Youtube-Manager 70 Prozent aller bei Youtube verbrachter Sehdauer auf algorithmisch empfohlene Clips entfiel.[44]

Auch dieses Optimierungsverfahren kann unerwünschte Nebeneffekte erzeugen, ja, sie sind aufgrund konzeptioneller Grundlagen derartiger Empfehlungssystems sogar unvermeidbar.[45] Automatisierte Empfehlungssysteme werden immer einen bestimmten Anteil vom Kontext her unangemessener Empfehlungen aussprechen, ein bestimmter Anteil der Nutzer*innen wird diesen unangemessenen Empfehlungen folgen und sie ansehen und damit wiederum Signale erzeugen, die dafür sorgen, dass weitere Nutzer*innen die gleichen unangemessenen Empfehlungen erhalten.

Drei Beispiele für unerwünschte Konsequenzen dieser Empfehlungsprinzipien:

(1) 2016 enthüllte der ehemalige Youtube-Entwickler Guillaume Chaslot, dass automatisch generierte Empfehlungen für die Suchbegriffe »Trump« und »Clinton« im Vorfeld der US-Wahl einen starken Pro-Trump-Bias aufwiesen. Ein großer Teil der auf diesem Weg empfohlenen Videos enthalte zudem gesellschaftliche Spaltung befördernde oder inhaltlich falsche Anteile.[46]

---

43 Vgl. Covington, Paul, Jay Adams und Emre Sargin: »Deep Neural Networks for YouTube Recommendations«, in: Proceedings of the 10th ACM Conference on Recommender Systems – RecSys ›16, the 10th ACM Conference, Boston, Massachusetts, USA: ACM Press, 2016, http://dl.acm.org/citation.cfm?doid=2959100.2959190

44 Vgl. Solsman, Joan E.: »Ever get caught in an unexpected hourlong YouTube binge? Thank YouTube AI for that«, CNET, ohne Datum, https://www.cnet.com/news/youtube-ces-2018-neal-mohan/

45 Vgl. Stöcker, Christian und Mike Preuss: »Riding the Wave of Misclassification: How we End Up with Extreme YouTube Content«, HCII2020, Kopenhagen, 2020.

46 Chaslot, Guillaume: »YouTube's A.I. was divisive in the US presidential election«, Medium, 06.01.2018, https://medium.com/the-graph/youtubes-ai-is-neutral-towards-clicks-but-is-biased-towards-people-and-ideas-3a2f643dea9a

(2) Im Jahr 2017 zeigten ein unabhängiger Autor[47] und im Anschluss mehrere Nachrichtenangebote, dass der Empfehlungsalgorithmus der Videoplattform Nutzer*innen zu Clips hinlenkte, die »Parodien« von bekannten Kinder-Cartoon-Sendungen wie »Peppa Wutz« oder »Paw Patrol« darstellen sollten. Diese »Parodien« enthielten beispielsweise dem britischen *The Guardian* zufolge Szenen von »bekannten Cartoon-Figuren in gewalttätigen oder sexualisierten Situationen, während andere Clips andere verstörende Bilder enthielten«[48].

(3) Im Jahr 2019 stießen drei Wissenschaftler, die eigentlich politische Inhalte aus Brasilien bei Youtube untersuchen wollten, auf ein Netzwerk aus »sexuell suggestiven Kanälen«. Bei näherer Betrachtung zeigten diese Kanäle teilweise Clips »minderjähriger Frauen« oder erwachsener Frauen, die Kinderkleidung trugen. Die folgenden Empfehlungen wiederum führten dann zu »Kanälen mit Videos von kleinen Kindern«, manche davon in Badekleidung, andere bei gymnastischen Übungen. »Das verbindende Element war, dass die Kinder leicht bekleidet waren«, so die Wissenschaftler in einem online veröffentlichten Arbeitspapier.[49] Der *New York Times* zufolge[50] waren einige dieser Clips binnen Tagen hunderttausende Male abgespielt worden.[51]

(4) Eine Vielzahl weiterer Beispiele aus diversen Bereichen ist bereits publiziert, etwa aus dem Gebiet der Berichterstattung über den menschengemachten Klimawandel, wo ein Forscher feststellte, dass »eine Mehrheit der Videos in der Stichprobe eine Weltsicht vertritt, die dem wis-

47 Bridle, James: »Something is wrong on the internet«, Medium, 21.06.2018, https://medium.com/@jamesbridle/something-is-wrong-on-the-internet-c39c471271d2

48 Maheshwari, Sapna: »On YouTube Kids, Startling Videos Slip Past Filters«, The New York Times, 04.11.2017, https://www.nytimes.com/2017/11/04/business/media/youtube-kids-paw-patrol.html;Naughton, John: »How Peppa Pig knock-offs bring home the bacon for Google | John Naughton«, The Guardian, 12.11.2017, https://www.theguardian.com/commentisfree/2017/nov/12/content-google-youtube-kids-not-always-suitable-for-children-peppa-pig-brings-home-bacon

49 Kaiser, Jonas und Adrian Rauchfleisch: »The implications of venturing down the rabbit hole«, Internet Policy Review, 2019, https://policyreview.info/articles/news/implications-venturing-down-rabbit-hole/1406

50 Fisher, Max und Amanda Taub: »On YouTube's Digital Playground, an Open Gate for Pedophiles«, The New York Times, 03.06.2019, https://www.nytimes.com/2019/06/03/world/americas/youtube-pedophiles.html

51 Vgl. Kaiser/Rauchfleisch: »The implications of venturing down the rabbit hole«.

senschaftlichen Konsens widerspricht«[52], oder im Bereich der Verschwörungserzählungen.[53] Die erfolgreichsten Videos von Verschwörungstheoretiker*innen in der Stichprobe einer Studie mit einer Gesamtzahl über 9000 empfohlenen Clips waren jeweils mehrere zehn Millionen Mal angesehen worden.

Wie können wir mediale Kollateralschäden eindämmen?

Aus den oben aufgelisteten Beispielen von drei exemplarischen, besonders reichweitenstarken Plattformen geht klar hervor, dass die ADM-Systeme, mit denen die Plattformbetreiber ihre jeweiligen Monetarisierungziele zu erreichen versuchen, unter bestimmten Umständen Inhalten Reichweite verschaffen, die entweder justiziabel, auf andere Weise, etwa unter Jugendschutzgesichtspunkten, problematisch oder der Qualität des demokratischen Diskurses in einer offenen Gesellschaft abträglich sind. Diese unerwünschten Nebeneffekte, die auf komplexen Wechselwirkungen der psychologischen und soziologischen Eigenschaften des Publikums, der Optimierungsziele der Plattformen, der Interessen bestimmter Akteure im neuen Medien-Ökosystem und den Eigenarten algorithmischer Empfehlungssysteme basieren, sind keine Ausrutscher, sondern systematische, zwangsläufige Effekte.

Die gewaltige Masse und die permanente, rasante Zunahme von verfügbaren Inhalten macht die zu leistende Aufgabe immer schwieriger: Von den Plattformbetreibern wird erwartet, dass sie Urheberrechts-, Persönlichkeitsrechts-, Jugendschutz- und strafrechtlich relevante Verstöße schnell ahnden und dabei nicht in unzulässiger Weise in Grundrechte wie die Meinungsfreiheit eingreifen. Das deutsche Netzwerkdurchsetzungsgesetz war ein Versuch, die Plattformen auf dem Umweg über die Androhung hoher Strafen bei Verstößen dazu zu bringen, mehr Geld in menschliche Moderator*innen zu investieren, damit gemeldete Verstöße schneller und mit höherer Trefferquote sanktioniert werden. Im Sommer 2020 beschloss

52 Allgaier, Joachim: »Science and Environmental Communication on YouTube: Strategically Distorted Communications in Online Videos on Climate Change and Climate Engineering«, Frontiers in Communication 4 (2019), S. 36.

53 Vgl. Albright, Jonathan: »Untrue-Tube: Monetizing Misery and Disinformation«, Medium, 02.03.2018, https://medium.com/@d1gi/untrue-tube-monetizing-misery-and-disinformation-388c4786cc3d

die Große Koalition Nachbesserungen, die etwa vorsahen, dass die Plattformen gemeldete, von ihnen dann als strafbar erkannte Inhalte anschließend an das Bundeskriminalamt weitermelden müssen. Doch die Ergänzung des Gesetzes stieß auf verfassungsrechtliche Bedenken und soll nun noch einmal überprüft werden. Doch neben solchen Ex-post-Eingriffen werden auch Ex-ante-Verfahren oder mehr Befugnisse für Aufsichtsgremien, Institutionen oder gar Behörden diskutiert: So sieht der neue deutsche Medienstaatsvertrag in seinem 2020 finalisierten, noch auf EU-Rechts-Konformität zu prüfende Entwurf Vorgaben zur Transparenz und Diskriminierungsfreiheit vor. Die sogenannten Informationsintermediäre, also vor allem die Betreiber von Suchmaschinen, Videoplattformen und sozialen Netzwerken, sollen künftig verständlich darlegen, nach welchen Kriterien Inhalte sortiert und ausgewählt werden.[54] Eine tatsächliche Offenlegung von Sortieralgorithmen wird derzeit nicht in Betracht gezogen.

Ein weiteres Problem betrifft einen Bereich, in dem die Entscheidungen noch weniger klar sind: Wenn es nicht um strafrechtlich oder anderweitig justiziable Inhalte geht, sondern um die Qualität von Information oder die Bewertung von Desinformation. Als Twitter das Konto des zu dem Zeitpunkt noch amtierenden Präsidenten Donald Trump nach dem Sturm auf das Kapitol im Januar 2021 schließlich löschte, unter Verweis auf gefährliche, zu Gewalt aufstachelnde Desinformation hinsichtlich des US-Wahlergebnisses, gab es eine hitzige Debatte, in die sich sogar Bundeskanzlerin Angela Merkel einschaltete: Sollten Plattformen wirklich die Macht haben, Staatsoberhäuptern von einem Tag auf den anderen den Zugang zu einem Millionenpublikum zu entziehen?

Dass die Problematik und die noch zu treffenden Regulierungsentscheidungen vielfältig sind, zeigt auch ein aktueller Fall aus Deutschland: Im Dezember 2020 erklärte der Präsident der Landesmedienanstalt Hamburg/Schleswig-Holstein, Thomas Fuchs, im Interview mit der *Tageszeitung (taz)*, man prüfe derzeit eine Kooperation zwischen Google und dem Bundesgesundheitsministerium.[55] Der Grund: »Bei der Internetsuche nach

54 Vgl. »Der neue Medienstaatsvertrag: Ein erster Überblick«, Bird & Bird, ohne Datum, https://www.twobirds.com/de/news/articles/2019/germany/der-neue-medienstaatsvertrag.

55 Rath, Christian: »Kritik an Kooperation mit Ministerium: ›Google bevorzugt den Staat‹«, Die Tageszeitung: taz, 21.12.2020, https://taz.de/!5735113/

mindestens 160 Krankheiten – von Asthma bis Windpocken – wird seit November der Inhalt des Portals *gesund.bund.de,* das vom Ministerium finanziert wird, von Google bevorzugt angezeigt.« Es bestehe der Verdacht, so Fuchs, »dass dadurch private journalistische Anbieter unzulässig benachteiligt werden«.[56]

Das Beispiel zeigt: Auch wenn Informationsintermediäre Anbieter bevorzugen, die in einem bestimmten Bereich auf den ersten Blick vielleicht tatsächlich hochwertige Informationen anzubieten haben, nicht zuletzt mit dem Ziel, Verbreitern von Desinformation Aufmerksamkeit zu entziehen, kann das auf den zweiten Blick problematische Konstellationen ergeben.

Eine über Mediengattungen und -kanäle hinweg konzipierte künftige Medienregulierung, wie sie etwa mit dem Digital Services Act[57] der Europäischen Union zumindest in Ansätzen angestrebt wird, sollte diesen Problemen in fundamentaler Weise Rechnung tragen. Aus den bisher verfügbaren Informationen über das geplante EU-Gesetz geht hervor, dass darin zumindest einige der oben angesprochenen Problemstellungen durchaus berücksichtigt zu werden scheinen. Insbesondere verspricht die Europäische Kommission im Kontext dieses Kapitels folgende relevanten Änderungen:[58]

(1) »Maßnahmen zur Bekämpfung illegaler Waren, Dienstleistungen oder Inhalte im Internet mit einem Mechanismus, der Nutzerinnen und Nutzern das Kennzeichnen solcher Inhalte erlaubt und Plattformen die Zusammenarbeit mit ›vertrauenswürdigen Hinweisgebern‹ ermöglicht (Anm. d. Verf.: Gemeint ist eine priorisierte Bearbeitung von Hinweisen auf problematische Inhalte oder Ähnliches von bestimmten Stellen.)
(2) Wirksame Schutzvorkehrungen für die Nutzer mit der Möglichkeit, Entscheidungen der Plattformen zur Moderation von Inhalten anzufechten (Anm. d. Verf: Es geht hier um die Möglichkeit, einen zu Unrecht gelöschten Inhalt anschließend wieder hochladen zu dürfen. Offen bleibt, wie solche Lösungen etwa im Falle von Livestreams tatsächlich ausreichend schnell und für die Betroffenen befriedigend umgesetzt werden können.)

56 Ebd.
57 Vgl. »Gesetz über digitale Dienste: mehr Sicherheit und Verantwortung im Online-Umfeld«, EU-Kommission – European Commission, Text, ohne Datum, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_de
58 Ebd.

(3) Erhöhung der Transparenz von Online-Plattformen in unterschiedlichen Bereichen, unter anderem bei für Vorschläge verwendeten Algorithmen
(4) Verpflichtungen für sehr große Plattformen, den Missbrauch ihrer Systeme zu verhindern, indem sie risikobasierte Maßnahmen ergreifen und ihr Risikomanagementsystem von unabhängiger Seite prüfen lassen
(5) Zugriff für die Forschung auf die Kerndaten größerer Plattformen, um das Fortschreiten von Online-Risiken nachvollziehen zu können
(6) Eine Beaufsichtigungsstruktur, die der Komplexität des Online-Raums gerecht wird: Die Hauptrolle kommt den Mitgliedstaaten zu – sie werden dabei von einem neuen Europäischen Gremium für digitale Dienste unterstützt. Bei sehr großen Plattformen übernimmt die Kommission eine erweiterte Überwachung und Durchsetzung.«

Insbesondere eine kontinuierliche, unabhängige Überwachung auch des Risikomanagements der Plattformen durch Forscher*innen und entsprechende Aufsichtsbehörden sowie der Zugriff auf Plattformdaten zur unabhängigen Kontrolle der Auswirkungen der eingesetzten ADM-Systeme erscheint unabdingbar. Bisher wirken die korrigierenden Eingriffe der Plattformbetreiber, die sich lange gegen jede Form der inhaltlichen Verantwortung gesträubt haben, in der Regel sehr reaktiv und ad hoc. Mit dem fundamentalen, systemischen Problem, das sich aus den oben ausgeführten Mechanismen, aus dem zwangsläufigen Widerspruch zwischen Monetarisierungs- und gesellschaftlichen Interessen ergibt, haben sich die Plattformen aus eigenem Antrieb bislang nicht befasst.

Die Antwort der Plattformbetreiber lautet bis jetzt meist: Die durch autonome technische Systeme verursachten Probleme sollen durch weitere autonome, technische, von ihnen selbst gestaltete und gesteuerte Aufsichtssysteme beigelegt werden. Ein solches Vorgehen würde aber nur noch mehr Macht in die Hände der Plattformbetreiber geben. Zudem berücksichtigen technische Konzepte wie Upload-Filter gegen urheberrechtlich geschützte Inhalte oder auf maschinellem Lernen basierende Systeme zur schnelleren Erkennung von Hassrede oder anderen problematischen Inhalten jeweils nur Teilprobleme und gehen nicht das grundlegende Problem der Aufmerksamkeitsökonomie der Gegenwart an: Die Tatsache, dass eine auf die Maximierung von Aufmerksamkeitszeit gerichtete Gestaltung von Medienplattformen ohne Rücksicht auf inhaltliche Kriterien, Qualität, Angemessenheit, Vielfalt, gesellschaftliche Relevanz oder gar Faktizität zwangsläufig dazu führen wird, dass problematische, mindestens aber zu einer wachsenden gesellschaftlichen Po-

larisierung beitragende Inhalte ein besonders großes Publikum finden werden.

Gelänge es der Europäischen Union, diesem Problem mit stringenter, robuster und auch mit entsprechenden Durchsetzungsressourcen unterfütterter Gesetzgebung wirksam zu begegnen, könnte eine derartige Gesetzgebung vorbildhaft auch für andere Weltgegenden wirken. Die Probleme, die aus den oben beschriebenen veränderten Rahmenbedingungen für die deliberative Demokratie, für den Grundrechtsschutz, die Meinungsfreiheit, für Persönlichkeits-, Urheber- und andere Rechte entstehen, sind oftmals fundamental, komplex und nicht mit einfachen, aus der Vergangenheit adaptierten Lösungen zu behandeln. Es gilt, eine neue Balance zu schaffen zwischen den wirtschaftlichen Interessen von Aufmerksamkeitsvermarktern, Inhalteanbietern, Publikum und demokratischer Öffentlichkeit. Die Vermarktung von Aufmerksamkeit auf Basis digitaler und automatisierter Sortierung oft kostenlos zur Verfügung gestellter Inhalte hat sich für die Informationsintermediäre als enorm lukratives Geschäftsmodell erwiesen. Es ist an der Zeit, sie umfassender als bisher an den gesellschaftlichen Kosten, die ihre Geschäftsmodelle verursachen, zu beteiligen, sie stärker bei der Prävention solcher Kollateralschäden in die Pflicht zu nehmen und ihnen deutlich klarere, robust durchsetzbare Vorgaben zu machen, was die Berücksichtigung von Optimierungszielen angeht, die jenseits ihres Börsenwertes liegen.

2.3.2 Digitale Souveränität

Von der Karriere eines einenden und doch problematischen Konzepts

Julia Pohle und Thorsten Thiel

Anfang März 2021 forderte Kanzlerin Angela Merkel und ihre Amtskolleginnen aus Dänemark, Finnland und Estland in einem öffentlichen Brief von der EU-Kommissionschefin »eine Offensive zur Stärkung der digitalen Souveränität der EU«.[1] Dieser so prominente wie ungewöhnliche gemeinsame Aufruf von vier europäischen Regierungschefinnen führt vor Augen, was für eine steile Karriere die Idee der *digitalen Souveränität* in den letzten Jahren hingelegt hat. Der Begriff ist in Deutschland und Europa insbesondere in den letzten fünf Jahren zu einem zentralen politischen Konzept aufgestiegen. Er findet sich im Programm für die deutsche EU-Ratspräsidentschaft, die das Ziel verfolgte, »digitale Souveränität als Leitmotiv der europäischen Digitalpolitik [zu] etablieren«[2]; er steht im Zentrum unzähliger Policy- und Positionspapiere, die sich um so unterschiedliche Themen drehen wie künstliche

1 Merkel, Angela/Kallas, Kaja/Frederiksen, Mette/Marin, Sanna: Appell von vier Regierungschefinnen an die EU: »Europa muss seine digitale Souveränität stärken«, in: Handelsblatt, 02.03.2021, https://www.handelsblatt.com/meinung/gastbeitraege/digitalisierung-appell-von-vier-regierungschefinnen-an-die-eu-europa-muss-seine-digitale-souveraenitaet-staerken/26962398.html

2 Auswärtiges Amt: Gemeinsam. Europa wieder stark machen. Programm der deutschen EU-Ratspräsidentschaft, Berlin 2020, S. 8.

Intelligenz,[3] Öffentlichkeit[4] oder Geopolitik;[5] er soll mit dem im Bundesinnenministerium anzusiedelnden Zentrum für Digitale Souveränität (ZenDiS) gar institutionell festgeschrieben werden.[6] Dass der Begriff von staatlichen Akteur*innen propagiert wird, ist wenig überraschend. Aber dass er auch offensiv von Wirtschaft[7] und Zivilgesellschaft[8] umarmt wird, sollte schon etwas mehr stutzig machen. Auch im parteipolitischen Spektrum zeigt sich der Begriff überall anschlussfähig: Er kann liberale Positionen auszeichnen oder auch im Diskurs um öffentliche Sicherheit fallen, er wird mit Ideen wie Open-Source-Software verknüpft oder auch für industriepolitische Argumentationen herangezogen. Selbst im sonst so nüchternen rechtswissenschaftlichen Diskurs wird ein Aufstieg des Konzepts digitaler Souveränität zum verfassungsstaatlichen Leitbild konstatiert.[9]

Wie kommt das und was heißt das? Ziel dieses Beitrages ist es, den sich entwickelnden Diskurs zur digitalen Souveränität kritisch zu analysieren und danach zu fragen, wie sich die zunehmende Ineinssetzung von Souveränität, Demokratie und europäischen Werten vollzogen hat – und inwiefern sie überzeugt. Ohne die strukturellen und politisch-ökonomischen Beweggründe für

3 Vgl. Bundesministerium für Wirtschaft und Energie BMWi: Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen, Fokusgruppe »Digitale Souveränität in einer vernetzten Gesellschaft«, Nürnberg, 2018.

4 Vgl. Kagermann, Henning/Wilhelm, Ulrich: European Public Sphere. Gestaltung der digitalen Souveränität Europas, München: acatech 2020.

5 Vgl. Steiner, Falk/Grzymek, Viktoria: Digital Sovereignty in the EU, Berlin: Bertelsmann Stiftung 2020.

6 Vgl. Punz, Matthias: Was das BMI zu digitaler Souveränität plant, in: Tagesspiegel Background, 28.10.2020, https://background.tagesspiegel.de/digitalisierung/was-das-bmi-zu-digitaler-souveraenitaet-plant

7 Vgl. BITKOM: Digitale Souveränität: Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa, Berlin. 2015; ZVEI, Die Elektroindustrie: Technological Sovereignty Industrial Resilience and European Competences. The Electrical Industry's View on Europe's Recovery Post-Covid-19 and Future Industrial Strategy, Brüssel 2020.; Reisch, Lucia/Büchel, Daniela: Digitale Souveränität, Gutachten des Sachverständigenrats für Verbraucherfragen, Berlin 2017.

8 Vgl. Gesellschaft für Informatik: Schlüsselaspekte Digitaler Souveränität (Arbeitspapier), Berlin, 2020; Reda, Julia: Edit Policy – Wo bleibt Europas Open Technology Fund?, in: netzpolitik.org, 13.10.2020, https://netzpolitik.org/2020/wo-bleibt-europas-open-technology-fund/

9 Vgl. Peuker, Enrico: Verfassungswandel durch Digitalisierung, Tübingen: Mohr Siebeck 2020.

die Forderungen nach mehr Selbstbestimmung im Digitalen zu negieren, sollen Verkürzungen in der mit dem Begriff verbundenen Argumentation aufgezeigt werden. Zu diesem Zweck rekonstruieren wir zunächst die wechselhafte Begriffsgeschichte (digitaler) Souveränität, bevor wir detaillierter auf die gegenwärtige Verwendung im deutschen und europäischen Diskurs eingehen. Abschließend erörtern wir aus einer normativ-demokratietheoretischen Perspektive, wieso die gegenwärtige Verwendungsweise gerade seitens progressiv-emanzipatorischer Kräfte ein Kurzschluss ist, und skizzieren, wie die zentralen Werte von Demokratie und Gemeinwohl insbesondere von progressiven Akteur*innen besser vorgetragen werden können.

Souveränität und die Herausforderung einer digital vernetzten Welt

Ideengeschichtlich ist Souveränität ein staatsbezogenes Konzept. Der Begriff leitet sich vom lateinischen Wort *superanus* ab, was »darüber befindlich« oder »überlegen« bedeutet, und wanderte als politischer Terminus in der Neuzeit aus dem Französischen (*souveraineté*) ins Deutsche ein. Das traditionelle Verständnis von Souveränität, wie es von Jean Bodin und Thomas Hobbes formuliert wurde, postuliert im Kern eine Zentralisierung von Macht als Antwort auf die Unwägbarkeiten pluralistischer Gesellschaften. Souveränität soll Gestaltungsmacht und Stabilität erzeugen, indem sie Kapazitäten bündelt und eine Hierarchie von Zuständigkeiten und Kontrollmöglichkeiten etabliert.

Im Laufe der Zeit entfernte sich das Konzept jedoch von seinen absolutistischen Wurzeln. Die Zentralisierung von Macht wurde um eine stärkere demokratische Rückbindung ergänzt. Zudem wurde Souveränität strikter unterschieden in Bezug auf eine äußere Dimension, die Anerkennung der Unabhängigkeit eines Staates, und eine innere Dimension, die selbstbestimmte staatliche Gestaltung der Ordnung. Im Begriff der Volkssouveränität umfasst diese dann auch das Selbstbestimmungsrecht der Bürger*innen eines Staates mitsamt deren individuellen Rechten gegenüber dem Staat.[10] Diese Vorstellung von Souveränität blieb in all ihren Facetten stets eng – wenngleich

10 Zum Konzept der Souveränität und seiner Entwicklung vgl. Grimm, Dieter: Souveränität: Herkunft und Zukunft eines Schlüsselbegriffs, Berlin: Berlin University Press 2009; Nootens, Geneviève: Popular Sovereignty in the West: Polities, Contention, and Ideas, New York: Routledge 2013.

meist implizit – mit einer geografisch-territorialen Bestimmung verknüpft.[11] Ab Mitte des 20. Jahrhunderts führte dies jedoch dazu, dass der Begriff sich überlebt zu haben schien. So setzte sich in der Nachkriegszeit – versinnbildlicht im Aufstieg neuer Steuerungsideale wie der neoliberalen Vorstellung des Marktes oder dem kybernetischen Denken – der Aufstieg eines Denkens in Netzwerken immer stärker durch, das eine politische Steuerung versprach, die die Vielfalt und Dynamik moderner Gesellschaften gerecht wird.[12] Spätestens mit dem Ende des Kalten Krieges und den Ideen globalen Regierens und europäischer Integration schien sich die Netzwerkgesellschaft auch politisch als postsouveräne Realität behauptet zu haben.[13]

Zu dieser Entwicklung passt die gesamte Frühgeschichte des Internets bis weit in die 1990er Jahre hinein.[14] Diese war von großer Skepsis gegenüber jedweder Form staatlicher Überordnung geprägt, und dies ungeachtet der Tatsache, dass staatliche Infrastruktur und Investitionen die entscheidenden Bedingungen dafür waren, dass die zugrunde liegenden Technologien entstehen und sich durchsetzen konnten.[15] Am deutlichsten kommt diese Denkrichtung, die als *Cyber-Exzeptionalismus* bezeichnet wird, in den Worten John Perry Barlows zum Ausdruck, mit denen seine 1996 beim Weltwirtschaftsforum in Davos verkündete *Declaration of the Independence of Cyberspace* beginnt:

---

11 Vgl. Lambach, Daniel: The Territorialization of Cyberspace, in: International Studies Review 22:3, 2020, 482-506.

12 Vgl. August, Vincent: Hierarchie, Markt, Netzwerk: Stabilitätsmodelle spätmoderner Demokratien, in: Hausteiner, Eva Marlene/Strassenberger, Grit/Wassermann, Felix (Hg.): Politische Stabilität: Ordnungsversprechen, Demokratiegefährdung, Kampfbegriff, Baden-Baden: Nomos 2020, 96-119; August, Vincent: Technologisches Regieren. Der Aufstieg des Netzwerk-Denkens in der Krise der Moderne, Bielefeld: transcript 2020.

13 Vgl. MacCormick, Neil: Questioning Sovereignty: Law, State, and Nation in the European Commonwealth, Oxford, NY: Oxford University Press 1999.

14 Eine ausführlichere Diskussion der historischen Entwicklung des Diskurses haben wir an anderer Stelle vorgelegt: Pohle, Julia/Thiel, Thorsten: Digitale Vernetzung und Souveränität: Genealogie eines Spannungsverhältnisses, in: Borucki, Isabelle/Schünemann, Wolf-Jürgen (Hg.): Internet und Staat: Perspektiven auf eine komplizierte Beziehung, Baden-Baden: Nomos 2019, 57-80 ; Thiel, Thorsten: Souveränität in der digitalen Konstellation: Dynamisierung und Kontestation, in: Hofmann, Jeanette et al.: Politik in der digitalen Gesellschaft, Bielefeld: transcript 2019.

15 Vgl. Mazzucato, Mariana: The entrepreneurial state, London: Anthem Press 2011.

> »Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.«[16]

Barlow und viele seiner Mitstreiter*innen waren überzeugt, dass Gesellschaften dank digitaler Netzwerke mittel- bis langfristig auf zentralisierte Infrastrukturen verzichten könnten und stattdessen die Möglichkeit kultivieren sollten, flexibel und gleichberechtigt bedarfsgerechte und spontane Assoziationen zu bilden.[17] Diese würden erlauben, sich von staatlicher Souveränität und mit dieser assoziierten Fehlentwicklungen wie Ineffizienz, statische Hierarchien, konfliktive Machtungleichgewichte und erzwungene Homogenität zu verabschieden.[18]

Die reale Entwicklung des Internets zeigte aber, dass dieses deutlich kompatibler mit der Ausübung souveräner Kontrolle ist als von den Cyber-Exzeptionalist*innen angenommen wurde. Insbesondere die Vorstellung einer Unregierbarkeit des Internets führt in die Irre. Dies wird am Beispiel autoritär regierter Staaten deutlich – zunächst vor allem China, wenig später dann auch Russland und viele weitere Länder –, die die offene Kommunikationsarchitektur als Bedrohung wahrnahmen und mit dem Aufbau eigener Kontrollmöglichkeiten und Dienste begegneten.[19] Viele dieser Maßnahmen

16 Barlow, John Perry: A Declaration of the Independence of Cyberspace, in: https://www.eff.org/cyberspace-independence1996.

17 Vgl. Benkler, Yochai: The Wealth of Networks: How Social Production Transforms Markets and Freedom, New Haven: Yale University Press 2006.

18 Ideologisch ist der ursprüngliche Cyber-Exzeptionalismus in einer liberal-pragmatischen Sicht auf die Welt verortet, die ein individualistisches Konzept von Gleichheit und Freiheit des Einzelnen absolut setzt und die sowohl mit libertären ökonomischen Positionen als auch mit Argumenten der Gegenkultur harmoniert, vgl.: Turner, Fred: From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism, Chicago: University of Chicago Press 2006. Diese auch als »Californian ideology« bezeichnete Sichtweise hat sich im Laufe Zeit auch im Silicon Valley immer wieder verändert und ist in ihrer heutigen Inkarnation nochmal stärker ökonomisch-libertär geprägt, vgl.: Daub, Adrian: Was das Valley Denken nennt – Über die Ideologie der Tech-Branche, Berlin: Suhrkamp 2020.

19 Vgl. Creemers, Rogier: China's Conception of Cyber Sovereignty: Rhetoric and Realization, in: Broeders, Dennis/van den Berg, Bibi (Hg.): Governing Cyberspace: Behaviour, Diplomacy and Power, Lanham: Rowman & Littlefield 2020, 107-145; Maréchal, Nathalie: Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy, in: Media and Communication 5:1 2017, 29-41; Thussu,

wurden anfangs belächelt, erwiesen sich aber zunehmend als erfolgreich und letztlich oft herrschaftsstabilisierend.[20] Doch auch liberale und demokratische Staaten begannen frühzeitig, Kapazitäten zu erweitern, um digitale Kommunikation nationalstaatlichen Vorgaben zugänglich zu machen.[21] Obwohl in der Anwendungsschicht des Internets Lokalisierung und Identifizierung voraussetzungsvoll sind, lassen sich digitale Infrastrukturen doch sehr gut auf staatliche Bedürfnisse von Ortung und Kontrolle hin einrichten. Verstärkt wird dies durch die umfassende Kommerzialisierung digitaler Kommunikation und die Entwicklung und Durchsetzung von Geschäftsmodellen, die auf Geschlossenheit und der intensiven Produktion und Nutzung von Daten beruhen.[22] Hier entstehen zahlreiche Anreize zur Identifizierung und Kontrolle, wodurch die Anonymität der Nutzer*innen umfassend schwindet.[23] Nationalstaatliche Prozesse der Rechtssetzung und -durchsetzung sind daher deutlich effektiver als im Diskurs der 1990er Jahre angenommen. Ebenso hat es sich – zumindest für die starken Staaten des Westens – als weniger schwierig erwiesen, mit rechtlichen Instrumenten global vernetzten Strukturen beizukommen, als Cyber-Exzeptionalist*innen vermuteten.[24] Das Internet ist kein rechtsfreier Raum – und ist es auch nie gewesen.

Obwohl die Vorstellung eines technisch erzeugten und autarken virtuellen Raums weiterhin fasziniert – man denke etwa an die Diskussion um Bitcoin und andere Blockchain-Phänomene[25] –, ist sie als Beschreibung einer sozio-

---

Daya Kishan/Nordenstreng, Kaarle: BRICS Media: Reshaping the Global Communication Order?, New York: Routledge 2020.

20 Vgl. Morozov, Evgeny: The Net Delusion: The dark side of Internet freedom, New York: PublicAffairs 2012.

21 Vgl. Goldsmith, Jack/Wu, Tim: Who Controls the Internet? Illusions of a Borderless World, New York: Oxford University Press 2006; Eriksson, Johan/Giacomello, Giampiero: Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State«, in: International Studies Review 11:1 2009, 205-230; DeNardis, Laura: Hidden Levers of Internet Control, in: Information, Communication & Society 15:5 2012, 720-738.

22 Vgl. Zuboff, Shoshana: The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, New York: PublicAffairs 2019.

23 Vgl. Thiel, Thorsten: Anonymität und der digitale Strukturwandel der Öffentlichkeit, in: Zeitschrift für Menschenrechte 10:1 2016, 9-24.

24 Eine komplexe Darstellung, wie die heutige dichte normative Regulierung funktioniert, findet sich bei Kettemann, Matthias C.: The Normative Order of the Internet: A Theory of Rule and Regulation Online, Oxford, NY: Oxford University Press 2020.

25 Vgl. Pistor, Katharina: Statehood in the digital age, in: Constellations 27:1 2020, 3-18.

technischen Realität heute weitgehend diskreditiert, zumal sie auch als Utopie viel von ihrer Anziehungskraft verloren hat: Die einfache Gleichsetzung von Vernetzung und Emanzipation trägt nicht länger.[26] Vielmehr hat die Entwicklung des kommerzialisierten Internets mit seinen Plattformen und Monopolen, aber auch die zunehmend polarisierte und toxische Diskurskultur der Aufmerksamkeitsökonomie vor Augen geführt, dass staatliche Regulierung in vielerlei Hinsicht notwendig für kollektiv-emanzipatorische Prozesse ist. Dies hat gerade in der europäischen Diskussion zu der Annahme geführt, dass starke Staatlichkeit in digitalen Fragen eine Art Vorbedingung für das Überleben der Demokratie sei.[27]

Die erste Dekade der 2000er Jahre lässt sich dabei rückblickend als die Übergangsphase interpretieren, in der der Souveränitätsbegriff auch im Hinblick auf das Internet wieder zunehmend an Popularität gewinnt, zunächst aber vor allem in klassischen Themenfeldern wie staatliche Autonomie, wirtschaftliche Konkurrenz und Sicherheit.[28] Die heutige Omnipräsenz des Begriffes ist jedoch erst das Ergebnis der Dekade nach 2010. Um die Dynamik dieser Phase zu verstehen, lohnt es sich, zwei Ebenen zu unterscheiden.

Die erste Ebene umfasst die Ereignisgeschichte, die von zwei Zäsuren geprägt ist: die Enthüllungen Edward Snowdens über die Praktiken geheimdienstlicher Überwachung durch die NSA und ihre Partnerdienste im Sommer 2013 und das doppelte politische Erdbeben des Brexit-Referendums und der Trump-Wahl im Jahr 2016. Die Snowden-Enthüllungen führten vor Augen, dass die Ordnung des Internets nicht eine freiheitlich-föderale ist, sondern dass eine klare Hegemonialposition existiert, die zudem die privatwirtschaftliche Sphäre überwölbt und aktiv ausnutzt. Die politischen Schocks des Jahres 2016 dagegen verdeutlichten – zumindest in der kontinentaleuropäischen Interpretation –, wie sehr eine Regulierung politischer Öffentlichkeit sowie ein aktiver Umgang mit Desinformation und Datensammlung für den Schutz demokratischer Prozesse nötig sind. Zusammengenommen bewirkten diese

26 Vgl. Pfeffer, Matthias/Nemitz, Paul Entstehung des Internets: Anarchie und Macht im Cyberspace«, in: Frankfurter Allgemein Zeitung (28.12.2020), 18.

27 Vgl. etwa schon früh die FAZ-Debatte um den sogenannten technologischen Totalitarismus: Schirrmacher, Frank, Hg.: Technologischer Totalitarismus: Eine Debatte, Frankfurt a.M.: Suhrkamp 2015.

28 Vgl. Dunn Cavelty, Myriam/Mauer, Victor (Hg.): Power and Security in the Information Age: Investigating the Role of the State in Cyberspace, Farnham (UK): Ashgate 2007, 151-163.

Ereignisse und ihre politischen Folgen, dass der vorherige Fokus auf die externe Dimension von Souveränität – also Souveränität als zwischenstaatliche Handlungsfähigkeit und Anerkennung von Einflusssphären – erweitert werden muss. Auch im Hinblick auf das Digitale muss die interne Dimension von Souveränität – also die Vorstellung von Souveränität als Bedingung für demokratische Selbstbestimmung – einbezogen werden.

Die zweite Ebene ist die allgemeine Bewusstwerdung der tiefgreifenden Transformation, die Digitalität für Gesellschaft und individuelle Lebensentwürfe bedeutet: die digitale Konstellation.[29] Dieses Umdenken kommt etwa darin zum Ausdruck, dass heute die Digitalisierung den begrifflichen Bezugspunkt von Souveränität darstellt, und nicht mehr die technische Infrastruktur des Internets oder dessen metaphorische Imagination als Cyberspace. Digitalisierung ist ein umfassenderes Konzept, das stärker kompetitive als kollaborative Assoziationen hervorruft und das nicht mehr auf eine raumzeitliche Trennung (online/offline) verweist, sondern einen Zustandswechsel impliziert – von einer analogen Welt in eine digitale. In der digitalen Konstellation sind nicht nur Kommunikationen, sondern etwa auch Gegenstände oder Prozesse stets so codiert, dass sie in digitaler Logik zu prozessieren sind, das heißt, dass sie Möglichkeiten algorithmischer Berechnung, Prognose und Automatisierung schaffen, also in Echtzeit geformt und gegebenenfalls individualisiert konfiguriert werden können.[30]

Die alles umfassende Digitalität unserer Gesellschaften bringt aber – zumindest in der Gegenwart, wo sie sich noch neu und herausfordernd anfühlt – die mit ihr einhergehenden Abhängigkeiten viel stärker ins Bewusstsein. Drei

29 Der Begriff der digitalen Konstellation verweist – anders etwa als Begriffe wie das digitale Zeitalter – darauf, dass technologische und gesellschaftliche Entwicklung am besten als wechselseitig und ko-konstitutiv interpretiert werden: Berg, Sebastian/Rakowski, Niklas/Thiel, Thorsten: Die digitale Konstellation. Eine Positionsbestimmung, in: Zeitschrift für Politikwissenschaft 30:2, 171-191, 2020. Was Digitalität mit Gesellschaft macht, ist nicht in den technologischen Möglichkeiten begründet, sondern wird durch die kontingente, oft auch bereichsbezogenene soziotechnische Entwicklung begründet. Die heutige digitale Konstellation ist dabei etwa entscheidend durch den Plattformkapitalismus geprägt, der wiederum neben seiner technologischen Konfiguration vor allem durch ökonomische und rechtliche Faktoren bestimmt ist: Cohen, Julie E.: Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford, NY: Oxford University Press 2019.

30 Wie tiefgreifend diese gesellschaftliche Veränderung ist, beschreibt etwa: Floridi, Luciano: The Fourth Revolution: How the Infosphere is Reshaping Human Reality, Oxford, NY: Oxford University Press 2014.

Quellen der Abhängigkeiten sind dabei für den Diskurs zu digitaler Souveränität ausschlaggebend: Erstens die Abhängigkeit von digitalen Infrastrukturen, wonach unsere Gesellschaften auf einen materiellen und immateriellen technologischen Unterbau angewiesen sind. Von Serverfarmen bis Softwarepatenten fußt die digitale Gesellschaft darauf, dass technologische Apparate und Protokolle, die zuverlässig und sicher zu sein haben, ineinandergreifen. Zweitens die Abhängigkeit von privaten Akteur*innen, insbesondere den großen Plattformunternehmen. Diese treten als Quasi-Souveräne auf, da sie etwa im Hinblick auf Größe und wirtschaftliche Macht ebenbürtig mit den Staaten erscheinen und ihre Geschäftsmodelle, zum Beispiel das Kuratieren von Öffentlichkeit oder das Erzeugen proprietärer Märkte, staatsähnlicher sind als frühere Erlösmodelle.[31] Drittens schließlich die Abhängigkeit in der geopolitischen Dimension, wie sie sich vor allem in der Rivalität einer amerikanischen und einer chinesischen Einflusssphäre zeigt. Hier geht es um den faktisch ungleichen Einfluss von Staaten und Regionen auf die technologische Entwicklung. Alle drei Abhängigkeiten werden in Europa öffentlich und politisch debattiert und begründen die gegenwärtigen Forderungen nach digitaler Souveränität.

Forderungen nach digitaler Souveränität in Deutschland und Europa

Der deutsche und der europäische Diskurs um digitale Souveränität weisen vielerlei Unterschiede auf zu denen in anderen Weltteilen, insbesondere in illiberalen Staaten. Eine grundlegende Differenz besteht darin, dass in Europa die Erhaltung und Stärkung der digitalen Souveränität als effektives Mittel angesehen wird, um im Zuge der digitalen Transformation liberale und demokratische Werte sowie die individuelle Selbstverwirklichung gleichermaßen zu realisieren. Nach europäischem Verständnis soll digitale Souveränität staatliche Macht nicht zementieren, eine gegenseitige Abhängigkeit wird akzeptiert, Nicht-Einmischung zumindest nicht absolut gesetzt. Zudem wird die zentrale Stellung der Bürger*innen in der politischen Entscheidungsstruktur betont. Der Diskurs um digitale Souveränität ist in Europa umfassender, aber auch diffuser als in hybriden oder autoritären Staaten,

31 Vgl. Staab, Philipp: Digitaler Kapitalismus: Markt und Herrschaft in der Ökonomie der Unknappheit, Frankfurt a.M.: Suhrkamp Verlag 2019.

was wiederum zu Unsicherheiten führt, wie die teilweise sehr unterschiedlichen Forderungen und Vorstellungen in politische, wirtschaftliche und technologische Praktiken umgesetzt werden könnten oder sollten. Es ist diese Ausdehnung und gleichzeitige Unfokussiertheit der deutschen und europäischen Debatte, die wir im Folgenden detaillierter aufschlüsseln wollen.[32]

Der Diskurs zur digitalen Souveränität in Deutschland

Unter den Ländern der Europäischen Union prägt Deutschland die Debatte um digitale Souveränität am stärksten. Anders als in anderen demokratischen Ländern, etwa Frankreich oder Indien, wurden in Deutschland erst verhältnismäßig spät Forderungen nach nationalstaatlicher Autonomie im Digitalen aufgestellt, wobei das Jahr 2013 mit den Snowden-Enthüllungen als deutlicher Katalysator wirkte. Dabei weist die deutsche Debatte drei Spezifika auf: erstens eine interne Ausdifferenzierung und Diffusion des Konzepts, zweitens eine Abkehr von einem allein hierarchisch-staatsbezogenen Souveränitätsverständnis und drittens eine stark normativ geprägte Argumentationsstrategie, die bisher aber nur zögerlich auch außereuropäisch kommuniziert wird.

Nicht zuletzt als Reaktion auf die gefühlte digitale Übermacht ausländischer Geheimdienste und Technologiekonzerne konzentrierten sich Politiker*innen und gesellschaftliche Akteur*innen nach 2013 vorerst auf Fragen der Sicherheit digitaler Infrastrukturen und die damit verbundene Unabhängigkeit von US-amerikanischen (und später auch von chinesischen) Anbietern. Dabei ging es primär um die Forderung, die IT-Infrastruktur und die Daten des Staates und staatlicher Einrichtungen zu schützen. Die vorgeschlagenen sicherheits- und innenpolitischen Maßnahmen betreffen etwa die Förderung vertrauenswürdiger IT-Produkte, den Einsatz nationaler IT-Sicherheitstechnologien sowie den Ausbau der Kapazitäten zur Cyber-Abwehr des Bundesamts für Sicherheit in der Informationstechnik. Seit Kurzem steht zudem die digitale Souveränität der öffentlichen Verwaltung

32 Eine vertiefte Untersuchung der Debatte um digitale Souveränität sowie der damit verbundenen Maßnahmen zur Stärkung der staatlichen, wirtschaftlichen und individuellen Selbstbestimmung bietet: Pohle, Julia: Digitale Souveränität: Ein neues digitalpolitisches Schlüsselkonzept in Deutschland und Europa, Berlin: Konrad-Adenauer-Stiftung 2020; . Vgl. außerdem: Misterek, Fokko : Digitale Souveränität: Technikutopien und Gestaltungsansprüche demokratischer Politik, Köln: MPIfG Discussion Paper 17/11 2017, Peuker, Enrico: Verfassungswandel durch Digitalisierung.

im Vordergrund, bei der es darum geht, Abhängigkeiten von proprietären Softwareanbietern zu verringern, indem Alternativen identifiziert und Wechselmöglichkeiten durch offene Schnittstellen und Standards unterstützt werden.[33]

Darüber hinaus nehmen auch wirtschafts- und industriepolitische Maßnahmen eine zentrale Stellung in der Debatte um digitale Souveränität ein. Diese zielen darauf, die Wettbewerbsfähigkeit und Unabhängigkeit des Wirtschafts- und Technologiestandorts Deutschland zu fördern, etwa durch den Aufbau von Schlüsselkompetenzen und -technologien in den Bereichen der Software- und Hardware-Entwicklung, der Cyber-Security, Big Data und Smart Data sowie Cloud-Diensten.[34] Einschlägiges Beispiel hierfür ist das insbesondere vom Bundeswirtschaftsministerium vorangetriebene europäische Cloud-Projekt GAIA-X, mit dem eine offene, sichere und vertrauenswürdige Plattform für Cloud-Anbieter als europäische Alternative zu den US-amerikanischen Providern geschaffen werden soll.[35]

Auffällig im deutschen Diskurs ist, dass dieser in hohem Maße die Nutzer*innen digitaler Technologien und Anwendungen in den Vordergrund stellt.[36] So wird die Forderung nach Souveränität oft in den Kontext

33 Vgl. BMI Bundesministerium des Inneren: BMI intensiviert Aktivitäten zur Stärkung der digitalen Souveränität in der öffentlichen Verwaltung (Pressemitteilung, 19.09.2019), https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/09/digitale-souveraenitaet-oeff-verwltg.html?nn=9390260; IT-Planungsrat und IT-Rat: Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung, Eckpunkte – Ziel und Handlungsfelder (31.03.2020), https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/32_Umlaufverfahren_Eckpunktepapier/Entscheidungsniederschrift_Umlaufverfahren_Eckpunktepapier.pdf?__blob=publicationFile&v=3

34 Vgl. Bundesministerium für Wirtschaft und Energie BMWi: Digitale Strategie 2025, https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-strategie-2025.html;BITKOM: Digitale Souveränität: Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa.

35 Vgl. Bundesministerium für Wirtschaft und Energie BMWi: Dossier GAIA-X: Eine vernetzte Datenstruktur für ein europäisches digitales Ökosystem, https://www.bmwi.de/Redaktion/DE/Dossier/gaia-x.html

36 In der Antwort auf eine Kleine Anfrage hielt die Bundesregierung im Dezember 2020 fest – dabei eine Formulierung aus einem Diskussionspapier des Kompetenzzentrums Öffentliche IT (Goldacker, Gabriele: Digitale Souveränität, Berlin: Kompetenzzentrum Öffentliche IT. 2017) übernehmend –, dass sie digitale Souveränität definiert als »die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können« Deutscher Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordne-

individueller Selbstbestimmung gerückt, etwa im Sinne einer »Verbrauchersouveränität« oder »Bürgersouveränität«. Entsprechend soll digitale Souveränität unter anderem auch durch bildungs- und verbraucherpolitische Maßnahmen befördert werden. Ebenso werden die Stärkung von Digitalkompetenz, Nutzer*innenrechten und Transparenz oder ein verbraucherorientierter Datenschutz, der sich an den Prinzipien des Privacy by Design beziehungsweise Privacy by Default orientiert, mit Souveränitätsargumenten begründet.[37] In Anlehnung an das im Zusammenhang mit dem Datenschutz in Deutschland entwickelte Konzept der »informationellen Selbstbestimmung« soll daher »digitale Selbstbestimmung« als Leitkonzept kultiviert werden.[38]

Statt allein die Unabhängigkeit und Autorität des Staates im Digitalen zu betonen, gilt im deutschen Diskurs also digitale Souveränität als Voraussetzung dafür, den Prozess der digitalen Transformation mitzugestalten und im digitalen Raum selbstbestimmt handeln zu können. Und dies bezieht sich gleichermaßen auf den Staat als zentralen demokratischen Akteur wie auch auf die Bürger*innen als individuelle Nutzer*innen und Konsument*innen. Im Mittelpunkt stehen folglich die kollektive Souveränität als Handlungs- und Gestaltungsfähigkeit des Staates sowie die individuelle Souveränität, verstanden als Autonomie und selbstbestimmte Handlungsfähigkeit des Individuums in einer vernetzten Welt. Zugleich wird versucht, Souveränität nicht exkludierend herzustellen, sondern eher über Regelakzeptanz und -befolgung zu verankern. Die Nutzung von Technologien und Anbietern aus dem Ausland wird nicht verboten, vielmehr sollen sie einer strikten Regelkontrolle unterworfen werden. So wurden beispielsweise amerikanische Großunternehmen von Palantir bis Amazon zum europäischen Cloud-Projekt GAIA-X zugelassen. Zudem wird in Deutschland weniger restriktiv und stärker prozedural

---

ten Joana Cotar, Uwe Schulz, Dr. Michael Espendiller und der Fraktion der AfD, Drucksache 19/24896.)

37 Vgl. Reisch, Lucia/Büchel, Daniela: Digitale Souveränität, Gutachten des Sachverständigenrats für Verbraucherfragen; Glasze, Georg/Dammann, Finn: Von der ›globalen Informationsgesellschaft‹ zum ›Schengenraum für Daten‹ – Raumkonzepte in der Regierung der ›digitalen Transformation‹ in Deutschland, in: Döbler, Thomas/Pentzold, Christian/Katzenbach, Christian (Hg.): Räume digitaler Kommunikation. Lokalität – Imagination – Virtualisierung, Köln: Herbert von Halem Verlag 2021.

38 Vgl. Mertz, Marcel et al.: Digitale Selbstbestimmung, Köln: Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres) 2016.

mit der Netzwerktechnologie von Huawei umgegangen als in anderen europäischen Ländern.

Um digitale Souveränität von Individuen zu erreichen und zu bewahren, sind jedoch andere Voraussetzungen zu erfüllen und Konsequenzen zu berücksichtigen als bei einem Staat oder einer Volkswirtschaft. Politik, Verwaltung und Gesellschaft stehen hier deshalb auch vor anderen Herausforderungen. Was diesbezüglich konkret zu tun sei, ist umstritten. Nahezu alle Diskursstränge verbindet aber, dass der Begriff der digitalen Souveränität als eine Zielvorstellung angeführt wird.[39] Digitale Souveränität wird gefordert, um Maßnahmen zu rechtfertigen, nicht aber, um eine institutionelle Struktur auszuarbeiten und ihr Zustandekommen zu rechtfertigen.

Der Begriff wird insofern stark normativ verwendet: Mehr Souveränität im Digitalen wird mit der Verwirklichung von Demokratie und europäischen Werten gleichgesetzt und die Vereinbarkeit von Souveränität mit Grund- und Bürgerrechten von vornherein als begründet angesehen. Besonders häufig werden dabei Datenschutz und Privatsphäre als zentrale Elemente digitaler Souveränität benannt, da diese individuelle Autonomie erst ermöglichen. Aber auch Prinzipien wie die Würde des Menschen, Freiheit, Rechtsstaatlichkeit, Gleichbehandlung, Diversität, Toleranz und Wertschätzung werden durch die Souveränitätsrhetorik vereinnahmt.[40] Kontrastiert werden diese Werte von Akteur*innen in Politik, Wirtschaft und Zivilgesellschaft mit den Modellen einer Digitalökonomie, wie sie in den USA (libertär) oder China (autoritär) als verwirklicht gelten.

Das dritte Spezifikum der deutschen Debatte ist, dass die Politik, einschließlich der Bundesregierung, den Begriff der digitalen Souveränität im Inland zwar intensiv bemüht und auch in Europa offensiv artikuliert, aber deutlich zögerlicher dabei ist, digitale Souveränität als allgemeines Prinzip in multilateralen Foren auf außereuropäischer Ebene zu propagieren. Das deutsche Programm für die EU-Ratspräsidentschaft vom Juli 2020, in dem die Stärkung der digitalen Souveränität Europas als ein zentrales Anliegen for-

39 Vgl. Bendiek, Annegret/Neyer, Jürgen: Europas digitale Souveränität. Bedingungen und Herausforderungen internationaler politischer Handlungsfähigkeit, in: Oswald, Michael/Borucki, Isabelle (Hg.): Demokratietheorie im Zeitalter der Frühdigitalisierung, Wiesbaden: Springer VS 2020, 103-125. 2020.

40 Vgl. Bundesministerium für Wirtschaft und Energie BMWi: Digitale Strategie 2025, https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-strategie-2025.html

muliert wurde,[41] kann als die strategische und gleichzeitig sehr prominente Fortführung des im Inland begonnenen Diskurses auf europäischer Ebene interpretiert werden. Die Zurückhaltung, den Begriff auch jenseits von Europa zu artikulieren, scheint darin begründet, dass digitale Souveränität in diesem Kontext weniger demokratisch als vielmehr nationalstaatlich-isolationistisch wahrgenommen wird. Es besteht die implizite Sorge, dass die Verwendung des Souveränitätsbegriffes autoritären Ländern und damit den vermeintlichen Gegnern eines freien, offenen Internets in die Hände spielt, von denen man die eigene Vorstellung der digitalen Souveränität ja gerade abzusetzen versucht. So bezog sich die Bundeskanzlerin in ihrer Eröffnungsrede des von den Vereinten Nationen organisierten und von Deutschland 2019 erstmals ausgerichteten Internet Governance Forums (IGF) zwar auf die Idee der digitalen Souveränität. Gleichzeitig grenzte sie ihr Verständnis aber explizit ab von Abschottung sowie von »Protektionismus oder Vorgabe von staatlichen Stellen, was an Informationen verbreitet werden kann – also Zensur«. Stattdessen sei es, so betonte sie, »gerade auch Ausdruck der Souveränität, für ein gemeinsames, freies, offenes und sicheres globales Internet einzutreten«.[42]

Die Debatte um digitale Souveränität auf europäischer Ebene

Bereits vor Beginn der EU-Ratspräsidentschaft Deutschlands 2020 war die Wirkung des deutschen Diskurses zur digitalen Souveränität auf der europäischen Ebene deutlich sichtbar. Deutschland und Frankreich sind in diesem Politikfeld, wie so häufig in der EU, zentrale Motoren.[43] Allerdings wird der Souveränitätsbegriff in Bezug auf Fragen der Digitalisierung von europäischen Akteur*innen, insbesondere der Europäischen Kommission, aber nicht nur insgesamt weniger, sondern auch weniger umfassend verwendet als in der deutschen Debatte. Drei Charakteristika prägen den europäischen Diskurs: erstens ein tendenzieller Verzicht auf die direkte Verwendung des

41 711Auswärtiges Amt: Gemeinsam. Europa wieder stark machen. Programm der deutschen EU-Ratspräsidentschaft, Berlin 2020, S. 8.

42 Merkel, Angela: Rede zur Eröffnung des 14. Internet Governance Forums (26.11.2019), https://www.bundeskanzlerin.de/bkin-de/aktuelles/rede-von-bundeskanzlerin-angela-merkel-zur-eroeffnung-des-14-internet-governance-forums-26-november-2019-in-berlin-1698264

43 Für das französische Verständnis und dessen Einbettung in den europäischen Diskurs vgl.: Heidenreich, Felix: Digitale Souveränität. Macrons Digitalisierungspolitik als Blaupause für die EU? In: Merkur, 74:4 2020, 77-84.

Souveränitätsbegriffes beziehungsweise dessen Fokussierung auf infrastrukturelle und medienrechtliche Aspekte sowie auf das Thema des digitalen Binnenmarktes, zweitens eine eher Kontinuität als Visionen betonende Rückbeziehung auf bestehende europäische Rahmen- und Arbeitsprogramme und drittens ein Rechtfertigungsdiskurs, der im Vergleich zum deutschen Diskurs weniger auf das Individuum konzentriert ist.

Tatsächlich wird auf EU-Ebene der Begriff digitale Souveränität bisher eher durch Begrifflichkeiten wie »strategische Autonomie« und »technologische Souveränität« ersetzt.[44] Jedoch weist insbesondere das Konzept der strategischen Autonomie, das 2016 in der Globalen Strategie für die Außen- und Sicherheitspolitik der EU eingeführt wurde, vielfältige Überlappungen mit der aktuellen Verwendung des Souveränitätsbegriffes auf, betont aber deutlich stärker die Bedeutung multilateraler Beziehungen und Partnerschaften.[45] Strategische Autonomie kann damit auch als ein Mittel gesehen werden, (staatliche und wirtschaftliche) Souveränität auszubauen. Der Unterschied besteht darin, dass die Idee der strategischen Autonomie im Kontext eines militärisch-sicherheitspolitischen Diskurses geprägt wurde und somit eher auf Themen der Sicherheit und Verteidigung eingeht.[46] Weil strategische Autonomie nicht explizit auf Technik beziehungsweise auf digitale Vernetzung und Technologie ausgerichtet ist, sondern gerade einmal Fragen der Cybersicherheit umfasst, wurde vereinzelt auch der Begriff der »digitalen strategischen Autonomie« eingebracht. Die damit verbundenen Forderungen beschränken sich oftmals auf die Stärkung der Sicherheit digitaler Infrastrukturen und Technologien. Sofern die Förderung anderer europäischer Kernanliegen thematisiert wird, steht vor allem die Etablierung eines wettbewerbsfähigen europäischen Technologiesektors oder der Aufbau strategischer Allianzen im Vordergrund.[47]

---

44 Vgl. Bauer, Matthias/Erixon, Fredrik: Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls, Brüssel: European Center for International Political Economy (ECIPE) 2020.

45 European External Action Service EEAS: Gemeinsame Vision, gemeinsames Handeln: Ein stärkeres Europa. Eine Globale Strategie für die Außen- und Sicherheitspolitik der Europäischen Union, Brüssel 2016, 3; Lippert, Barbara et al.: European Strategic Autonomy. Actors, Issues, Conflicts of Interests, Berlin: Stiftung Wissenschaft und Politik 2019.

46 Vgl. Timmers, Paul: Strategic Autonomy and Cybersecurity, Brüssel: EU Cyber Direct – Supporting the EU Cyber Diplomacy 2019, 2ff.

47 Vgl. Eurosmart: 10-Point Manifesto for European Digital Strategic Autonomy, Brussels 2019.Ganz aktuell ist der Versuch einiger Autoren, den Begriff der digitalen strategi-

Technologische Souveränität – im Englischen auch in der Kurzform *tech sovereignty* – ist noch etwas näher an der deutschen Vorstellung von digitaler Souveränität als das Konzept der strategischen Autonomie. Um technologische Souveränität zu erreichen, setzt die EU-Kommission vor allem auf Wettbewerbsförderung (z.B. im Bereich künstliche Intelligenz), Infrastrukturaufbau (z.B. durch die Förderung von Breitband- und 5G-Netzen) und die Entwicklung wirtschaftlicher und technologischer Schlüsselkompetenzen.[48] Das deckt sich zu großen Teilen mit der Strategie zum Aufbau eines europäischen digitalen Binnenmarkts, die die Europäische Kommission bereits seit der Einführung der Digitalen Agenda 2010 verfolgt.[49]

Der Souveränitätsbegriff wird im europäischen Diskurs damit insgesamt deutlich enger gefasst als in Deutschland. Auffallend ist, dass in ihm der individuellen Souveränität weniger Relevanz zugewiesen wird. So fordert zwar auch die EU-Kommission, Digitalkompetenzen zu stärken und mit digitalen Technologien bewusster umzugehen. Sie erhofft sich dies jedoch eher als abgeleitete Wirkung aus einer neuen bedeutsameren Rolle der EU in der globalen digitalen Ökonomie.[50] Als primäre Merkmale europäischer Digitalpolitik gelten hingegen wirtschaftliche Stärke und die Bereitstellung einer Infrastruktur, die diese ausbaut und schützt. Diese sollen durch gezielte Wettbewerbsförderung erreicht werden, weniger durch Protektionismus.[51] Die verschiedenen wirtschafts- und sicherheitspolitischen Ziele und Maßnahmen, die auf EU-Ebene in den letzten Jahren im Zusammenhang mit dem Begriff der technologischen Souveränität verfolgt wurden, stellen dabei keine substanziellen Neuerungen zu existierenden digitalpolitischen Programmen der EU-Kommission dar. Die Weiterentwicklung der letzten Jahre ist eher als eine Anpassung an neue Technologien zu sehen, etwa im Bereich künstliche

---

schen Autonomie auch im deutschen Diskurs zu etablieren und sich damit von einem Verständnis von digitaler Souveränität abzugrenzen, das auch die Handlungsfähigkeit von Unternehmen und Individuen umfasst. Vgl. dazu Kar, Resa Mohabbat/Thapa, Basanta E P: Digitale Souveränität als strategische Autonomie – Umgang mit Abhängigkeiten im digitalen Staat, Berlin: Kompetenzzentrum Öffentliche IT 2020, 10.

48 Europäische Kommission: Shaping Europe's Digital Future, in: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

49 Peuker sieht den Aufbau des Digitalen Binnenmarkts daher als Kernelement der europäischen Strategie für digitale Souveränität, vgl. Peuker, Enrico: Verfassungswandel durch Digitalisierung, 2020, 200ff.

50 Vgl. von der Leyen, Ursula: Gestaltung der digitalen Zukunft Europas (19.02.2020), in: https://ec.europa.eu/commission/presscorner/detail/de/ac_20_260

51 Vgl. Peuker, Enrico: Verfassungswandel durch Digitalisierung, 2020, 204.

Intelligenz oder Quantencomputing.[52] Gleichzeitig betont die Kommission die Notwendigkeit, existierende digitale Angebote und Anbieter zu regulieren, und setzt die Schaffung rechtlicher Rahmenbedingungen zunehmend als strategisches Instrument ein.[53]

In diesem Sinne läutete die Europäische Kommission im März 2021 »Europas digitale Dekade« ein und legte mit einem »digitalen Kompass« klare Zielvorgaben vor, die bis 2030 umgesetzt werden sollen.[54] Der Kompass, der darauf abzielt die »Rechte und Werte der EU […] im Mittelpunkt des auf den Menschen ausgerichteten europäischen Weges der Digitalisierung« zu stellen, beruht weitgehend auf der bestehenden Digitalstrategie der Kommission vom Februar 2020, ergänzt diese aber um einige Elemente. Interessant ist dabei vor allem die Schaffung eines Rahmens für Digitalgrundsätze, der »in einer breiten gesellschaftlichen Debatte erörtert« und in einer »feierlichen interinstitutionellen Erklärung des Europäischen Parlaments, des Rates und der Kommission verankert« werden soll. Konkrete Vorschläge wie eine solche Deliberation über das »Ziel der EU […], digital souverän zu sein« aussehen könnte, bleiben jedoch aus.

Während der Diskurs um digitale europäische Souveränität also von einer gewissen Konstanz mit älteren europäischen Politiken geprägt ist, lässt sich in Bezug auf die diskursive Rechtfertigung dieser Politiken in jüngerer Zeit eine neue Gewichtung feststellen. Wirtschafts- und geopolitische Spannungen werden viel offensiver mit der formulierten Notwendigkeit einer wettbewerbsorientierten, technologischen Souveränität verknüpft. Europa zu stär-

52 Europäische Kommission: White Paper on Artificial Intelligence: a European approach to excellence and trust (19.02.2020), in: https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

53 Das bekannteste Beispiel in diesem Bereich ist die europäische Datenschutz-Grundverordnung (DSGVO), aber auch neuere und noch in der Verabschiedung befindliche Initiativen wie der Digital Service Act (DSA) und Digital Markets Act (DMA) hoffen auf einen *Brussels Effect* (Bradford, Anu: The Brussels Effect: How the European Union Rules the World, Oxford, NY: Oxford University Press 2020.) und etablieren gezielt Regulierungshoheit als zweiten Pfeiler neben strategischer Autonomie: Christakis, Theodore: ›European Digital Sovereignty‹: Successfully Navigating Between the ›Brussels Effect‹ and Europe's Quest for Strategic Autonomy, Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute, Studies on Digital Governance 2020.

54 Europäische Kommission: Europas digitale Dekade: ein digital gestärktes Europa bis 2030 (09.03.2021), in: https://ec.europa.eu/commission/presscorner/detail/de/ip_21_983

ken ist demnach nicht nur Selbstzweck, sondern eine Frage der Verteidigung europäischer Werte. Nicht umsonst definierte Ursula von der Leyen bei ihrem Antritt als Kommissionspräsidentin technologische Souveränität als »die Fähigkeit, über die Europa verfügen muss, um im Einklang mit den eigenen Werten und Regeln eigene Entscheidungen treffen zu können«.[55] Als Teil der für den europäischen Binnenmarkt zentralen Normen werden hier traditionell der Datenschutz und die von der EU garantierten Individualrechte genannt.[56] Die Anpreisung europäischer Werte kann dabei, wie auch im deutschen Diskurs, als Versuch gesehen werden, sich gegenüber den von den Konkurrenten USA und China verfolgten Wirtschafts- und Industriepolitiken abzugrenzen, unter dem Vorwand einer europäischen Sozial- und Verbraucherpolitik.[57] So forderte der deutsche EU-Abgeordnete Axel Voss (CDU) beispielsweise einen »europäische[n] (dritte[n]) Weg der Digitalisierung, der im Gegensatz zum US-amerikanischen oder chinesischen Ansatz menschenzentriert, wertorientiert und auf dem Konzept der Sozialen Marktwirtschaft basiert«.[58]

Souveränitätsforderungen werden im deutschen wie europäischen Kontext somit stark normativ aufgeladen und mit Verweisen auf spezifische Werte und Institutionen begründet. Der europäische Diskurs ist dabei aber deutlich weniger als der deutsche auf die Handlungs- und Entscheidungsfähigkeit der einzelnen Bürger*innen ausgerichtet. Vielmehr wird die Stärke der europäischen Staatengemeinschaft als Garant gesehen, die Souveränität der einzelnen Länder sowie die Individualrechte ihrer Bürger*innen zu bewahren.[59]

Digitale Souveränität: Eine Problematisierung

Bisher haben wir die langen Linien des Souveränitätsdiskurses in Bezug auf digitale Vernetzung sowie die aktuelle Ausprägung des deutschen und euro-

55 von der Leyen, Ursula: Gestaltung der digitalen Zukunft Europas (19.02.2020).

56 Vgl. Reding, Vivienne: Digital Sovereignty: Europe at a Crossroads, Brüssel: European Investment Bank Institute, European Debates Series 2016, 3.

57 So auch in: Steiner, Falk/Grzymek, Viktoria: Digital Sovereignty in the EU, 4.

58 Voss, Axel: Manifest Digitale Souveränität: In der EU-Digitalpoltik radikal umdenken (20.01.2020), in: https://www.axel-voss-europa.de/2020/01/20/in-der-eu-digitalpoltik-radikal-umdenken/

59 Vgl. Peuker, Enrico: Verfassungswandel durch Digitalisierung, 2020, 204.

päischen Verständnisses von digitaler Souveränität nachvollzogen. Dabei ist deutlich geworden, dass die aktuelle Prominenz des Begriffes auf zwei miteinander zusammenhängende Aspekte zurückzuführen ist: Zum einen wird die digitale Konstellation unserer Gegenwart als ein Zustand zunehmender Abhängigkeit bei gleichzeitiger großer Unsicherheit erfahren. Die tiefgreifende Durchdringung unseres Alltags mit digitalen Medien und ein damit einhergehendes öffentliches Bewusstsein für die damit verbundenen Risiken und den invasiven Plattformkapitalismus haben eine große Skepsis gegenüber einer als unreguliert wahrgenommenen Digitalisierung hervorgerufen. Auf diese verspricht digitale Souveränität eine Antwort zu geben. Zum anderen aber hat der Souveränitätsbegriff selbst eine Umwidmung erfahren. Er wird – zumindest im deutschen und europäischen Kontext – gegenwärtig fast durchgehend synonym verwendet mit Selbstbestimmung und Autonomie, Demokratie und Grundrechten und dient daher als *stand-in* für die viel beschworenen europäischen Werte.

Zum Ende dieses Textes wollen wir nun die begrifflich-rekonstruktive Ebene verlassen und stattdessen noch einmal darauf eingehen, inwiefern digitale Souveränität als progressives Konzept zu überzeugen vermag. Die Prominenz des Begriffes macht ihn zu einer starken normativen Projektionsfläche. Umso wichtiger ist es, zu sezieren, wie der Begriff wirkt und ob es Alternativen zu ihm gibt. Es ist nicht die Diagnose, die infrage steht: Eindeutig bedarf es heute demokratischer Institutionen, die fähig sind, durch verbindliche Regelsetzung auf die sich verändernden Möglichkeiten, den gesellschaftlichen Diskurs zu formen, einzugehen und somit Ungleichheiten und Manipulationspotenziale entgegenzuwirken. Zu hinterfragen ist aber, was durch den Begriff digitale Souveränität als Alternative imaginiert wird. Drei Aspekte machen es nach unserer Einschätzung ratsam – gerade seitens progressiv-emanzipatorisch orientierter Akteur*innen – zu überdenken, ob man die aktuelle Konjunktur des Begriffes weiter verstärken soll.

Zunächst ist zu fragen: Passt digitale Souveränität für das europäische Projekt? Wie oben gezeigt, wird der Begriff auf der Ebene europäischer Politik weniger und begrenzter genutzt als in Deutschland. Grund dafür mag auch sein, dass das europäische Projekt nicht zuletzt aus der Idee geboren wurde, nationalstaatliche Souveränität zu überwinden. Versuche, eine europäische Souveränität oberhalb der europäischen Nationalstaaten zu propagieren, haben teils große Krisen im Prozess der europäischen Integration ausgelöst. Die intensive Nutzung des Konzepts digitaler Souveränität gerade auf deutscher Seite liegt zwar nahe, da von der Exportpolitik über das ausgeprägte

ordnungspolitische Element bis hin zu Besonderheiten wie dem starken öffentlich-rechtlichen Sektor die digitale Souveränität Europas klar deutschen Interessen sowie dem deutschen Selbstverständnis als europäisch denkende Macht entspricht. Doch in dieser deutschen Prägung liegt auch ein Risiko, nämlich dass das Projekt – wie andere deutsche Ideen zu Binnenmarkt oder der Finanzarchitektur – weniger als Demokratisierungs-, denn als Hegemonialprojekt wahrgenommen wird. Das Verwischen der Grenze zwischen Nationalstaat und Europa – wie es in deutschen Positionspapieren anhaltend praktiziert wird[60] – lässt sich durchaus als Interessenpolitik einer ohnehin sehr dominanten Macht wahrnehmen.[61] In seiner Penetranz offenbart es einen tendenziell staatspolitisch verengten Blick auf die digitale Konstellation. Die Konstruktion einer Frontstellung beziehungsweise einer Alternative zu zwei anderen geopolitischen Mächten, China und den USA, die hinsichtlich ihrer Werte und ihres Politikverständnisses als verschieden ausgeflaggt werden, funktioniert zwar besser als frühere Versuche einer europäischen Identitätsbildung. Sie bleibt aber etwas, wofür das europäische Projekt eigentlich nicht stehen sollte.

Zweitens: Passt der Begriff zu den propagierten Zielen? Wie bereits gezeigt, wurde der Souveränitätsbegriff in seinem ursprünglichen Kontext in Reaktion auf durch Pluralität erzeugte Konflikte und Unsicherheiten etabliert. Souveränität sollte diese befrieden und entscheiden. Obwohl die Totalität und Personalität des souveränen Anspruchs heute verloren ist, bleibt Souveränität ein Begriff, der auf eine gewisse Einheitlichkeit zielt und Durchsetzungsmacht imaginiert. Dies lässt sich etwa an dem von Christoph Meinel veröffentlichten Text »Deutschland gibt seine Souveränität am Router ab« zeigen, in dem dieser einen in vielerlei Hinsicht erstmal progressiven Souveränitätsbegriff vertritt, der jedwede absolutistische oder auch nur staatszentrierte Vorstellung verwirft.[62] Digitale Souveränität wird nach Meinel durch die Nutzung und Weiterentwicklung von Open-Source-Software erlangt. Souveränität wird von ihm als Instrument gesehen, Offenheit zu ermöglichen und zu managen, indem sie entlang von Werten orientiert wird.

60 Als Beispiel: Kagermann, Henning/Wilhelm, Ulrich: European Public Sphere. Gestaltung der digitalen Souveränität Europas, 2020.

61 Vgl. Tamma, Paola: Europe wants ›strategic autonomy‹ – it just has to decide what that means (15.10.2020), in: https://www.politico.eu/article/europe-trade-wants-strategic-autonomy-decide-what-means/

62 Meinel, Christoph: Deutschland gibt seine Souveränität am Router ab, in: Frankfurter Allgemeine Zeitung (05.10.2020), 21.

An den Stellen, wo der Text aber explizit auf die politische Ebene eingeht, ändert sich plötzlich der Ton und eine andere Vorstellung von Souveränität und ihrer Funktion wird deutlich. Meinel problematisiert hier demokratische Prozesse und Institutionen und beschreibt diese als eher hinderlich für das technische Konzept digitaler Souveränität. Hier zeigt sich exemplarisch, dass der Souveränitätsbegriff – gerade weil er so diffus und doch zielgerichtet verwendet wird – oft viel zu sehr vom als wünschenswert unterstellten Ergebnis her gedacht ist und weniger als ein demokratischer Prozess. Souveränität lässt sich begrifflich höchstens temporär von Handlungsmacht und einem Denken in stabilen Kollektiven abkoppeln. Es ist daher kein Zufall, dass der Begriff und die Logik der Souveränität auch in rechtspopulistischen Diskursen so präsent ist.[63] In seiner 2020 erschienenen Streitschrift *Sovereignty, RIP* schreibt Don Herzog daher pointiert, dass wir für alle Leistungen, die wir uns von Souveränität erhoffen, längst bessere, weil demokratische Alternativen entwickelt wurden, haben.[64]

An diesen Punkt schließt unmittelbar unser dritter Einwand an: Souveränität setzt in hohem Maße Kontrolle und Kontrollmöglichkeiten voraus. Im Kontext digitaler Gesellschaften heißt dies, dass Souveränitätsforderungen fast immer auch auf das Schaffen und Rechtfertigen neuer Eingriffs- und Beobachtungsbefugnisse hinauslaufen. Bereits der erste Schub des Souveränitätsdiskurses vor 2010 hat wie ein Katalysator auf die Zahl und Möglichkeiten der Eingriffspunkte für Staaten und private Dritte in digitale Netzwerke und ihre gesellschaftliche Nutzung gewirkt.[65] Und auch der gegenwärtige Diskurs um digitale Souveränität wird begleitet von immer expliziteren Bemühungen, Datenverkehr und Kommunikationsinfrastrukturen für staatliche Institutionen leichter zugänglich zu machen. Das prägnanteste Beispiel hierfür ist die Forderung nach Durchgriffsmöglichkeiten und Überwachungsbefugnissen im Bereich der Kommunikation. Zwar wird diese Forderung im europäischen Raum selten explizit mit Souveränität begründet, weil Souveränität gegenwärtig auch zu stark mit individueller Selbstbestimmung und Datenschutz verknüpft ist. Doch die in diesem Diskurs vorgetragenen Argumente sind in ähnlicher Weise auf die Abhängigkeiten und auf die (behauptete)

63 Vgl. Heidenreich, Felix: Die Rhetorik Der Souveränität: Zu Einem Zentralen Topos in Der Grammatik Populistischer Emotionalisierung, in: Zeitschrift für Politik, 65:1 2018, 45-59.

64 Herzog, Don: Sovereignty, RIP, New Haven: Yale University Press 2020.

65 Vgl. DeNardis, Laura: Hidden Levers of Internet Control, 2012.

Unsicherheit und Rechtlosigkeit einer nicht souverän kontrollierten Ordnung bezogen. Kontrollinfrastrukturen zu errichten ist dem Souveränitätsdenken daher sehr viel näher als die (potenzielle) Demokratisierung der souveränen Kontrollinstanzen. Die Zentralisierung politischer Macht beim Souverän wird vorrangig vor der Frage behandelt, wie in pluralen Gesellschaften eine demokratische Willensbildung gelingen kann.

Die kommende Dekade wird in Bezug auf die digitale Transformation fraglos im Zeichen des Kampfes um den Erhalt und die Weiterentwicklung der freiheitlichen Demokratien stehen. Dass dieser Prozess begonnen wurde und die technologische Entwicklung in ihrer soziopolitischen Dimension erkannt ist und angegangen wird, ist nicht zuletzt auch ein Verdienst der Debatte um digitale Souveränität. Der Begriff der digitalen Souveränität hat es wie kein anderer in den vergangenen fünf Jahren vermocht, Akteure aus Politik, Wirtschaft und Zivilgesellschaft zusammenzubringen und eine aktive europäische politische Regulierung von Fehlentwicklungen im Kontext der digitalen Transformation anzustoßen. Das Potenzial des Begriffes zu einen ist aber trügerisch. Gerade progressive Akteur*innen, die hoffen, mit dem Begriff eine stärkere Gemeinwohlorientierung und Demokratisierung der digitalen Transformation zu erreichen, laufen Gefahr, enttäuscht zu werden. Wer sich für eine demokratische und offene Digitalisierung engagiert, sollte nicht zu sehr auf einen Begriff setzen, der Zentralisierung und Machtdurchsetzung prämiert, sondern viel stärker offensiv einfordern, dass Möglichkeiten der Mitbestimmung und Teilhabe institutionell festgeschrieben werden. Viele derzeit mitverhandelte Ideen – wie offene Infrastrukturen, eine andere, stärker von öffentlichen Zielen her gedachte Datennutzung sowie deren Kontrolle – lassen sich auch ohne den Verweis auf das Ziel digitaler Souveränität begründen, viele sogar besser umsetzen, wenn sie eben nicht begrenzt auf einen bestimmten politischen Bezugsraum gedacht werden. Die sozialen und politischen Kämpfe der kommenden Jahre sollten sich daher vom Begriff der Souveränität wieder lösen und unmittelbar Demokratie, Mitbestimmung und Gemeinwohlorientierung als Zukunftshorizont benennen.

III. Von der Verantwortungsdiffusion zur Governance

3.1 Mehrebenensystem
Digitalpolitik von technischen Standards über staatliche Normen bis zum digitalen Völkerrecht

Matthias C. Kettemann

Zur Verortung der Digitalpolitik

Zunächst müssen wir Digitalpolitik lokalisieren. Wo wird Digitalpolitik betrieben? Die einfachere Frage wäre inzwischen: Wo nicht? Digitalisierung ist phänomenologisch so breit und diffus geworden wie die Globalisierung. Ähnlich begrifflich konturlos, häufig missverstanden, manchmal dämonisiert. Das Buch, in dem dieser Beitrag erscheint, zeigt die Vielfalt der Digitalisierung, aber auch ihre Wirkkraft auf gesellschaftliche Realitäten und Werte. Die Beiträge in diesem Buch betonen die Gestaltungsnotwendigkeit der Digitalisierung, die Bedeutung des *Primats des Rechts*. Hier knüpft dieser Beitrag an und zeigt auf, wie vielfältig die Produktion von Recht im Kontext der Digitalisierung ist und wie Normen gesellschaftliche Gestaltungsansprüche erheben – und dies sind nicht nur und nicht einmal vor allem *Rechts*normen.

Staaten, Individuen, privatwirtschaftliche Unternehmen, die Zivilgesellschaft und technische Standardsetzer – sie alle schaffen und vollziehen, bestreiten und bekräftigen in verschiedenen Konstellationen Normen. Deren Entstehung, Legitimität und Durchsetzbarkeit variiert stark: von privaten Normen durch normgebende Gremien und nationale Verfassungen bis hin zu bindenden Normen des Völkerrechts. Nur durch eine sorgfältige Analyse der Faktizität und Normativität der Regeln für das Netz und die digitale Welt kann ein Modell einer umfassenden und nuancierten Ordnung der

Digitalpolitik – einer normativen Ordnung des Internets[1] – herausdestilliert werden. Diese Ordnung speist sich aus privaten Normen und öffentlichen Regeln (Gesetzen), ist also hybrider Natur. Sie setzt sich zusammen aus internationalen Rechtsnormen, nationalem Recht und transnationalen Regelungsarrangements unterschiedlicher Art.

Dieser Beitrag stellt beispielhaft einige Akteurskonstellationen vor, in denen Digitalisierungspolitik stattfindet, Normen mit Digitalbezug gesetzt und normative Konflikte verhandelt werden. Eine Einordnung nach Ebenen (international, regional, national, lokal) kann nicht trennscharf erfolgen, da Akteur*innen in Foren zusammenwirken, die diese Ebenen gerade durchbrechen. Nicht zwingend, aber doch aufschlussreicher erscheint daher eine Einteilung auf Ebene der normativen Instrumente, die das Ergebnis der digitalpolitischen Arbeit verschiedener Akteurskonstellationen sind: darunter Verträge, Gesetze, Prinzipien, Standards.

Häufig liegen indes Mischformen vor: Technische Standardsetzung findet auf nationaler wie internationaler Ebene statt, mal als Versuch, qua Normierung nationale technologische Souveränität zu projizieren (wenn etwa China und Huawei einen neuen Internet Protocol-Standard vorschlagen), mal durch technisch dominierte globale Institutionen ohne vordergründig politische Agenden (wie die Standards der Internet Engineering Task Force [IETF]). Dabei ist jede technische Standardisierung immer auch politisch, da sie sowohl kontingent als auch normativ ist. Das dynamische Mehrebenensystem der Digitalpolitik charakterisiert aber auch, dass Akteur*innen gleichermaßen Normunternehmer (also Normenschaffer und -promoter), Normanwender und Normdurchsetzer sein können.

Internetvölkerrecht und Internet Governance

Das Konzept der *digitalen Welt* impliziert eine neue Lebensrealität jenseits des staatlichen Territoriums, in der Recht beziehungsweise Menschenrechte keine Gültigkeit hätten. Das ist falsch. Der Cyberspace ist keine rechtliche *ter-*

1 Vgl. Kettemann, Matthias: The Normative Order of the Internet. A Theory of Online Rule and Regulation (Oxford: Oxford University Press, 2020).

ra nullius.[2] Natürlich entstehen mit den neuen »Territorialitäten«[3] neue normative Herausforderungen, aber die Normativität des Rechts wird nicht vor grundlegend neue Herausforderungen gestellt.[4] Recht gilt online wie offline. Menschenrechte gelten online wie offline.[5] Völkerrecht gilt offline wie online. In der Tat hat die Regulierung internationaler Informations- und Kommunikationsflüsse durch das Völkerrecht eine lange Tradition. Das Völkerrecht ist das einzige Rechtsgebiet, mit dem globale öffentliche Güter verwaltet werden, das globale öffentliche Interessen schützt und über Verteilungsfragen entscheiden kann.[6]

Der Konsens der Staaten der Welt, dass sich das Internet nur mit einem globalen Ansatz gestalten lässt, wird schon in den Schlusserklärungen der Weltgipfel zur Informationsgesellschaft 2003 (Genf) und 2005 (Tunis) sichtbar. Die Staatengemeinschaft verpflichtete sich, mitzuwirken am Aufbau einer »den Menschen in den Mittelpunkt stellende[n], inklusive[n] und entwicklungsorientierte[n] Informationsgesellschaft […] gestützt auf die Ziele und Grundsätze der Charta der Vereinten Nationen, das Völkerrecht und den Multilateralismus sowie unter voller Achtung und Einhaltung der Allgemeinen Erklärung der Menschenrechte«[7], wobei bekräftigt wurde, dass »Menschenrechte und Grundfreiheiten, einschließlich des in der Erklärung von Wien verankerten Rechts auf Entwicklung, allgemein gültig und unteilbar sind, einander bedingen und miteinander verknüpft sind«[8].

---

2 Vgl. Hobe, Stephan: Cyberspace – der virtuelle Raum, in: Isensee/Kirchof (Hg.), HStR XI, 2013, 3. Auflage.

3 Sassen, Saskia: Territory, Authority, Rights. From Medieval to Global Assemblages (Princeton: Princeton University Press, 2006), 346: »[T]erritorialities […] entail specific political, operational, or subjective encasements, including some that might be formalized and some that might remain informal.« Die Formalisierung dieser ›Encasements‹ ist ein normativer Prozess. Vgl. auch instruktiv: Daniel Lambach, The Territorialization of Cyberspace, International Studies Review, viz022, https://doi.org/10.1093/isr/viz022.

4 Siehe hierzu auch den Beitrag von Ulf Buermeyer und Malte Spitz in diesem Band.

5 Siehe Kettemann, Matthias: Völkerrecht in Zeiten des Netzes: Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht (Bonn: Friedrich-Ebert-Stiftung, 2015), http://library.fes.de/pdf-files/akademie/12068.pdf

6 Ebd.

7 World Summit on the Information Society (WSIS), Tunis Commitment, WSIS-05/TUNIS/DOC/7-E vom 18.11.2005, Ziff. 2. Cf. auch WSIS, Geneva Declaration of Principles (2003), Ziff. 1.

8 Tunis Commitment (Fn. 2), Ziff. 3.

Deutlicher und verbindlicher wurde erstmals ein Bericht von 2013,[9] in dem ein staatenbeschicktes Gremium der Vereinten Nationen, die Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), festhielt, dass die Anwendung von Normen, die aus dem bestehenden Völkerrecht abgeleitet werden, »essenziell« ist, um Risiken für den Weltfrieden und die internationale Sicherheit und Stabilität zu minimieren.[10] Dies gelte auch für den völkerrechtlichen Schutz der Souveränität und der Verantwortung, die dieser entfließe, sowie für die Menschenrechte.[11]

2015 bestätigte die GGE erneut, dass Völkerrecht einen essenziellen Rahmen für die nationale Nutzung von Informations- und Kommunikationstechnologien darstelle.[12] Für die Gewährleistung der Integrität des Internets besonders relevant sind die angesprochenen völkerrechtlichen Grundsätze,[13] die teils in der Satzung der UNO in die Form von Vertragsrecht gegossen wurden, teils völkergewohnheitsrechtlich (also durch Anwendung und übereinstimmende gemeinsame Rechtsüberzeugung etabliertes Recht) geschützt sind und teils als Allgemeine Prinzipien des Völkerrechts auftreten: souveräne Gleichheit, Gewaltverbot, Interventionsverbot, friedliche Streitbeilegung, Menschenrechtsschutz, Kooperationsprinzip (das sich speist aus dem Grundsatz der guten Nachbarschaft) und Präventionsprinzip [*due diligence*].[14] Diese Prozesse wurden auch in der jüngsten Vergangenheit fortgesetzt. Russland schlug in einer Resolution die Schaffung einer Open-ended Working Group

9 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 vom 24.6.2013.

10 Ebd., Rz. 16.

11 Perspektiven darauf bei Kettemann, Matthias C./Kleinwächter, Wolfgang/Senges, Max: »Implementing Sustainable Digital Cooperation: Towards Next Generation Internet Governance«, in: Kettemann, Matthias C./Kleinwächter, Wolfgang/Senges, Max (Hg.): Towards a Global Framework for Cyber Peace and Digital Cooperation. An Agenda for the 2020s, BMWi: Berlin 2019, S. 31-46.

12 Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General, A/70/174 vom 22.7.2015, retrieved 15.2.2020 from https://www.un.org/ga/search/view_doc.asp? symbol=A/70/174.

13 Ebd., Abs. 26.

14 Vergleiche dazu auch Kettemann, Matthias C.: »Die Weltordnung des Digitalen, Vereinte Nationen«. Zeitschrift für die Vereinten Nationen und ihre Sonderorganisationen/German Review on the United Nations 5/2019, 195-200.

(OEWG) der Generalversammlung vor, die USA bevorzugen die Weiterführung der Group of Governmental Experts.

Neben dem klassischen Völkerrecht ist die zweite internationale Grundordnung des Internets das normativ weniger stringente, aber dennoch einflussreiche Internet-Governance-Regime.[15] Die Governance des Internets (oder »Internet Governance«) umfasst die »Entwicklung und Anwendung durch Regierungen, den Privatsektor und die Zivilgesellschaft, in ihren jeweiligen Rollen, von gemeinsamen Prinzipien, Normen, Regeln, Entscheidungsfindungsprozessen und Programmen, die die Weiterentwicklung und Verwendung des Internets gestalten«.[16] Die Bedeutung der Teilhabe aller Stakeholdergruppen (Staaten, Privatsektor, Zivilgesellschaft)[17] wird schon in der Definition deutlich. Die Realisierung demokratischer Partizipationsansprüche im Rahmen transnationaler Steuerungsprozesse ist indes schwierig.

Der Multistakeholderprozess als inklusiver Ansatz, die Internet-Governance-Policy zu gestalten, ist mit wenigen Ausnahmen (ordnungspolitische Initiativen souveränitätsbewusster bis autoritärer Regierungen) unumstritten. Da sich Staaten, der Privatsektor und die Zivilgesellschaft (Input-Legitimität) an dem Legitimationsprozess beteiligen und dabei eine gleichberechtigte Interaktion ermöglicht wird (Throughput-Legitimität), sind auch die Regelungsergebnisse besonders legitim (Output-Legitimität).[18] Diese Regelungsergebnisse sind aufgrund ihrer Legitimität auch im Großen und Ganzen effektiv, was wiederum ihre Legitimität befördert.

Die in den normativen Prozessen der Internet Governance entwickelten Normen gehören zur Kategorie der *transnationalen Regulierungsarrangements*. Hier ist als Ort der Diskussion besonders das Internet Governance Forum der Vereinten Nationen zu nennen, eine jährliche Konferenz, die Tausende

15 Vgl. Kettemann, Matthias: »Internet Governance«, in: Jahnel et al. (Hg.): Internetrecht, 4. Auflage Wien: Springer 2020, S. 47-73.

16 Arbeitsgruppe über Internet Governance (WGIG), Bericht der Arbeitsgruppe (2005), Abs. 10.

17 Zur Rolle der Zivilgesellschaft und Stärkung der Vielfalt siehe auch den Beitrag von Julia Kloiber und Elisa Lindinger, für Ideen zur Reform der nationalen Governance siehe den Beitrag von Stefan Heumann in diesem Band.

18 Vgl. die gute Übersicht über die Prozeduralisierung von Legitimation in transnationalen Konstellationen bei Michael Zürn, Michael/Binder, Martin/Ecker-Ehrhardt, Matthias/Radtke, Katrin: »Politische Ordnungsbildung wider Willen«, Zeitschrift für Internationale Beziehungen 14 (2007) 1, S. 129-164 (154ff, 157).

Akteure der Digitalpolitik versammelt, ohne konkrete Entscheidungsbefugnis zu haben. Internet Governance ist eine normativ wertvolle Ergänzung des Völkerrechts, da sie in einer nicht-binären Logik (legal/illegal) mit variierender, flexibler Normativität die *weicheren* Themen der Internetregulierung, wie zum Beispiel Rechenschaftspflicht, normativ rahmt.

Demokratie ist begrifflich die Herrschaft des Volkes, der Normunterworfenen, die sich selbst Normen geben. Im Kontext des Internets verlieren Grenzen an Bedeutung, trotz Tendenzen der Souveränitätsrückgewinnung in Russland und China. »Das Volk« des Internets diffundiert. Einzelne haben keine effektive Möglichkeit, Regeln von großen Plattformen zu beeinflussen. Mark Zuckerberg lässt sich nicht wählen. Dabei haben alle Menschen ein demokratisches Teilhabeinteresse am Internet und dessen Regulierung. Insofern haben sie ein wertefundiertes Interesse nicht nur am Regelungsergebnis, sondern auch am Regelungsprozess an sich, der voraussetzt, dass alle Akteur*innen in alle Phasen des normativen Prozesses eingebunden sind. Dieses wird auch (wenn auch primär hinsichtlich von technischen Grundfragen der Internet Governance) durch den Multistakeholderansatz durchgesetzt, der durch Regierungen (Staaten), den Privatsektor (Unternehmen) und die Zivilgesellschaft (Individuen) in ihren jeweiligen Rollen verwirklicht wird.

Multistakeholderansätze und technische Standards

Internet-Governance-Prozesse leiden unter einer vagen Sprache, wiederholten normativen Mantras (»Multistakeholderismus«) und intellektueller Dürftigkeit. Prinzipien, die innerhalb dieser Prozesse entwickelt werden, neigen dazu, aus wenigen Quellen zu schöpfen (wie den Ergebnisdokumenten des Prozesses zum World Summit on the Information Society und dem NetMundial-Treffen 2014). Dennoch sind diese Prozesse wichtig, weil sie Normen hervorbringen und Verfahren legitimieren, in denen diese Normen entwickelt werden. Diese wiederum sind Teil der hybriden normativen Ordnung des Internets. Viele von ihnen sind weder internationales noch nationales Recht, sondern bilden eine dritte Kategorie des normativen *Tertiums*. Als transnationale regulatorische Arrangements müssen sie sodann entweder durch ihre Genese (etwa in fairen Prozessen, an denen alle relevanten Akteur*innen beteiligt waren) oder die Ergebnisse, die sie hervorbringen, legitimiert werden.

So wie die Ausarbeitung und Akzeptanz von Internet-Governance-Mechanismen wichtige Beispiele für die staatliche Praxis sind, können neue rechtliche Instrumente, einschließlich Gerichtsentscheidungen, Governance-Entscheidungen und -Prozesse stark beeinflussen. So wurde die Global Commission on the Stability of Cyberspace beauftragt, die Internet Governance weiterzuentwickeln, um ein stabiles Internet zu gewährleisten. Die Kommission schlug Ende 2017 eine Norm vor, die speziell den öffentlichen Kern des Internets schützen und ein Prinzip der Nichteinmischung in diesen etablieren soll: »Unbeschadet ihrer Rechte und Pflichten sollten staatliche und nichtstaatliche Akteure keine Handlungen vornehmen oder wissentlich zulassen, die die allgemeine Verfügbarkeit oder Integrität des öffentlichen Kerns des Internets und damit die Stabilität des Cyberspace absichtlich und erheblich beeinträchtigen.«[19] Dies ist offensichtlich eine präzisere Formulierung des Nichteinmischungsprinzips, die sich an dem öffentlichen Kern des Internets orientiert, dessen Schutz im gemeinsamen Interesse liegt. Da die Staaten durch das Völkergewohnheitsrecht angehalten sind, die für die Gewährleistung der Integrität des Internets wesentliche Infrastruktur nicht zu beschädigen (weil deren Schutz im gemeinsamen Interesse liegt), beinhaltet die Norm keine neue Pflicht, sondern rückt eine bestehende stärker in den Fokus und fördert so normkonformes Verhalten.

Doch angesichts der Vielzahl politischer und rechtlicher Fragen, mit denen das Internet konfrontiert ist, hinterlässt selbst die Kombination der beiden Regime von *Recht* und *Governance* erhebliche Regelungslücken und normative Brüche. Obwohl Recht und Governance des Internets ineinander verwoben sind, treten diese Brüche bei einer kritischen Betrachtung der Ordnung des Internets leicht zutage.

Ein Kohärenzfaktor sind technische Normen. Ohne Regeln im weitesten Sinne (in ihrer Ausprägung als technische Spezifikationen), ohne einige Normen zur Zusammenarbeit und zum Austausch von Informationen, wären die Informations- und Kommunikationsflüsse über das Internet nicht möglich gewesen. Dass die eher technischen Spielregeln für das frühe Internet in informellen Rundschreiben (Requests for Comments; RFCs) veröffentlicht und *bottom-up* in Meetings von Ingenieur*innen entwickelt wurden, ändert nichts an der Tatsache, dass einige (hauptsächlich technische) Normen von

19 Global Commission on the Stability of Cyberspace, Norm to Protect the Core of the Internet, https://cyberstability.org/norms

den Normsubjekten als höchst legitim angesehen wurden. Aber Ingenieur*innen haben auch verhaltensorientierte Normen formuliert, wie beispielsweise der US-amerikanische Informatiker Jon Postel: »Sei liberal in dem, was du akzeptierst, und konservativ in dem, was du sendest.«[20] Darüber hinaus findet die Tätigkeit von Ingenieur*innen und Unternehmen in einem Rahmen nationaler und internationaler Normen statt, die ihr Handeln beeinflussen. Diese Normen, die im Kraftfeld von Technik und Recht entstehen, mögen hybridisiert und weitgehend privatisiert sein, bleiben aber innerhalb der Grenzen, die das nationale und internationale Recht setzt.

Konturen einer digitalen Wertordnung

Ziel einer gelungenen Gestaltung der Digitalisierung muss es sein, zentrale Werte in allen Teilen der normativen Ordnung zu verankern. So muss dem Mehrebenensystem der Internet Governance mit dessen vielen Akteur*innen und der nötigen Vielfalt im normativen Vokabular ein Anker gegeben werden: gemeinsame, geteilte Werte und insbesondere der Schutz des Gemeinwohls, die Gemeinwohlbindung der Ausübung von Gestaltungsmacht und die Gemeinwohlorientierung von Policymacht.

Jeder Internetuser kann menschenverachtende Kommentare melden. Jede Plattform kann sich menschenrechtssensible Standards geben. Jeder Staat kann sich zu einer menschenrechtswahrenden Cyberaußenpolitik verpflichten. Aufsichtsbehörden spielen zunehmend eine wichtige Rolle, um die Werte und Rechte in der digitalen Welt zu bewahren. International sind auch Ombudspersonen[21] von Bedeutung, ebenso bewusste Konsultationen von Expert*innen im Kontext von Rechtssetzungsverfahren,[22] verpflichtende Algo-

20 Braden, R. (Hg.): RFC 1222, Requirements for Internet Hosts -- Communication Layers, October 1989, https://www.ietf.org/rfc/rfc1122.txt, 1.2.2. October 1989.

21 Z.B. Australian Competition and Consumer Commission, ›Digital Platforms Inquiry – Final Report‹, Australian Competition and Consumer Commission, 2019.

22 ›Assessment for German Parliament's Commission on Artificial Intelligence: Technology-Driven Disinformation by Bots‹, Botswatch Technologies, 2020 https://www.botswatch.io/assessment-sb/

rithmenfolgenabschätzungen (Kanada[23]) sowie Modelle verstärkter Transparenz im Kampf gegen Hate Speech.[24] Zahlreiche hochspezialisierte Nichtregierungsorganisationen im Digitalbereich wie Access Now[25], Amnesty International[26] und AlgorithmWatch[27] zeigen beispielsweise beim Monitoring von Algorithmen, wie man effektiv in digitalen Konstellationen für Menschenrechte eintreten kann.

Das Recht ist (oder besser: die Normen und ihre Gefüge sind) das wichtigste Medium der Gesellschaft, um Ordnung zu schaffen, Herrschaft zu konstituieren und zu begrenzen und Gerechtigkeit zu gewährleisten.[28] Oben habe ich gezeigt, dass verschiedene Normen auf verschiedenen Ebenen für die Gestaltung der Digitalpolitik relevant sind. Wie können diese disparaten Prozesse zusammengeführt werden? Dafür bietet sich das Modell der *normativen Ordnung* der digitalpolitischen Gestaltung des Internets an.

Die normative Ordnung des Internets ist dezidiert kein hierarchisches System expliziter Normen. Es gibt keine Grundnorm. Sie ist vielmehr ein Komplex von Normen, Werten und Praktiken, die sich auf die Nutzung und Entwicklung des Internets beziehen. Durch die Ordnung werden die Aktivitäten und die Interaktionen verschiedener Akteur*innen, einschließlich Staaten, privater Unternehmen und der Zivilgesellschaft, die sich auf das Inter-

23 Treasury Board of Canada Secretariat Government of Canada, Algorithmic Impact Assessment (Archived) – Government of Canada Digital Playbook (Draft) https://canada-ca.github.io/digital-playbook-guide-numerique/views-vues/automated-decision-automatise/en/algorithmic-impact-assessment.html

24 Vgl. Wagner, Ben et al.: »Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act«, in: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, FAT* ›20 (Barcelona, Spain: Association for Computing Machinery, 2020), S. 261-271.

25 Experts Are Finished, Politicians to Deliver – the Council of Europe Publishes Expert Recommendations on the Human Rights Impacts of Algorithmic Systems, Access Now, 2019 https://www.accessnow.org/experts-are-finished-politicians-to-deliver-the-council-of-europe-publishes-expert-recommendations-on-the-human-rights-impacts-of-algorithmic-systems/

26 Amnesty International, Schütze deine Daten und deine Menschenrechte: Drei Schritte zum Datenschutz, https://www.amnesty.de/informieren/aktuell/schuetze-deine-daten-und-deine-menschenrechte-drei-schritte-zum-datenschutz

27 States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights, AlgorithmWatch, 2020 https://algorithmwatch.org/en/joint-statement-pandemic-surveillance-tech-and-human-rights

28 Vgl. Kettemann, Matthias: The Normative Order of the Internet. A Theory of Online Rule and Regulation (Oxford: Oxford University Press, 2020).

net beziehen oder durch dieses vermittelt werden, geregelt. Ebenso werden die Ausübung privater oder öffentlicher Autorität und die Verteilung gemeinschaftlicher Güter, einschließlich des Internetzugangs und des Zugangs zu Internetinhalten, normativ gerahmt. Die normative Ordnung des Internets ist somit die Menge an Normen, normativen Erwartungen und Legitimationsnarrativen, die die Nutzung und Entwicklung des Internets prägen. Sie ist im Kern das, woran sich die Digitalpolitik abarbeitet, der Regelungsgehalt des Politikfelds Digitalisierung.

Das Internet hat sich in der Tat zu einem lebenswichtigen Kommunikationsmedium entwickelt, durch das jede Person ihre Menschenrechte ausüben kann, insbesondere durch das ihr zustehende Recht auf freie Meinungsäußerung, das das Recht einschließt, Informationen und Ideen aller Art zu suchen, zu empfangen und weiterzugeben, und zwar über das Medium ihrer Wahl und ohne Rücksicht auf Grenzen. Das Internet ist jedoch kein ätherisches Subjekt utopischer normativer Projekte und Projektionen, sondern lediglich eine hardwarebasierte Datenübertragungsmöglichkeit, auf der Software läuft, die auf Protokollen basiert, die Interkonnektivität gewährleisten.

Beides – der öffentliche Kern des Internets und die dafür notwendigen Server – sind für das Funktionieren kritischer Infrastrukturen (z.B. Stromnetze) unabdingbar und stellen selbst kritische (Informations-)Infrastrukturen dar. Daher hat sich der Schutz der Integrität des Internets (seine Sicherheit, Stabilität, Robustheit, Widerstandsfähigkeit und Funktionalität) im gemeinsamen Interesse zu einer völkerrechtlichen Verpflichtung der Staaten entwickelt, sowohl einzeln als auch als Mitglieder der globalen Gemeinschaft. Wir sehen auch hier wieder, wie im Mehrebenensystem unterschiedliche Normen zusammenwirken.

Die flexible normative Geometrie der Digitalpolitik

Die normativen Akteure im Internet haben die Zusammensetzung des Mediums Recht beeinflusst und es in Richtung einer flexibleren Geometrie der Normativität bewegt. Unverbindliche Normen und Prinzipien, Standards und Codes haben sich zu einer dritten Art von relevanten Regeln neben den internationalen und nationalen Normen etabliert. Sie entstehen im umkämpften Raum zwischen technischer Notwendigkeit und sozialen und rechtlichen Werten und weisen eine variable normative Dichte und Bindungswirkung auf. Doch diese nicht-rechtliche Normativität muss (und wird) durch einen

wertebasierten normativen Ansatz neu ausgerichtet werden, der gleichwohl Normsetzungsverfahren einbezieht.

Jeder Bereich von Normen innerhalb der Ordnung – internationales Recht, nationales Recht, transnationale normative Arrangements – wird entweder durch traditionelle normative Prozesse oder durch seine Integration in nationale Rechtsordnungen legitimiert. Jede Akteur*innengruppe ist direkt oder indirekt legitimiert und überträgt dieses Legitimationspotenzial auf das normative Ergebnis, das oft – zusätzlich – epistemisch legitimiert ist. Die normative Ordnung selbst ist legitim als eine notwendige Ordnung, um den Schutz des Internets und den Schutz vor digital vermittelter oder mit digitalen Tools amplifizierter Gefahren zu gewährleisten.

Diese normative Ordnung des Internets integriert Normen, die materiell und normativ mit der Nutzung und Entwicklung des Internets verbunden sind, auf drei verschiedenen Ebenen (national, regional, international)[29], von zwei Typen (privat und öffentlich verfasst) und von wesentlich unterschiedlichem Charakter (von bindendem Völkerrecht bis zu technischen Standards). Wie eben erwähnt, handelt es sich um eine Rechtsordnung, die durch die Form des Rechts und in Analogie zu ihr funktioniert. Ihre Akteur*innen – Staaten, juristische Personen, natürliche Personen – erfüllen vielfältige Funktionen als Normunternehmer, Normanwender und Normdurchsetzer. Mit den Rechtfertigungsnarrativen werden technische Konsistenz und rechtlich-kulturelle Übereinstimmung bewertet. Die normative Ordnung des Internets ist durch Legitimationsbeziehungen mit nationalen und internationalen Rechtsordnungen verflochten.

Rules rule

Normen herrschen (vor). Eine normative Ordnung des Internets hat sich etabliert. Mit dem Recht als System sollen gemeinsame Werte realisiert, Autorität kontrolliert und grundlegende Güter und Rechte verteilt werden. Nur ein alle Akteur*innen in den Blick nehmender, für Regeln unterschiedlichster Art offener, ganzheitlicher und systematischer Ansatz zur normativen Ordnung im Internet kann zu gerechten Regeln in der (und über die) Digitalisierung führen. Diese Regeln schützen Rechte und Werte in der Strukturierung des

29 Zur Frage einer europäischen Strategie siehe auch den Beitrag von Tyson Barker in diesem Band.

Digitalen, legitimieren die Ausübung privater und öffentlicher Autorität und gewährleisten die gerechte Verteilung grundlegender Güter und Rechte, einschließlich des Internetzugangs.

Logiken der Technizität sind nicht zwingend beherrschend in normativen Debatten. Code ist Recht, indem er normativ ist, aber nicht Recht in dem Sinne, dass er Rechtsnormen verdrängt oder hierarchisch übergeordnet oder praktisch beherrschend ist. Code taucht nicht einfach auf, er wird in Prozessen geschrieben, die reguliert werden können, die an der normativen Ordnung des Internets gemessen werden können. *Protocols have politics* und Normen müssen konsequent auf ihre Entwicklung und Implementierung angewendet werden. Dieser Befund gilt für Algorithmen und algorithmische Entscheidungsfindung,[30] einschließlich Selektions- und Empfehlungslogiken, die klare Auswirkungen auf Rechte und Freiheiten haben, indem sie beispielsweise die Gestaltung und den Inhalt der informatorischen Diskursgrundlage beeinflussen, die für jede demokratische Gesellschaft in algorithmisierten Medienmärkten wesentlich ist.[31]

Digitalpolitik geht uns alle an. Die gesellschaftlichen Mehrwerte der Digitalisierung zu realisieren und die Risiken für individuelle Schutzgüter sowie für den gesellschaftlichen Zusammenhalt zu minimieren, ist die zentrale politische Aufgabe im Mehrebenensystem der Digitalisierung und ihrer Politik. Um die Zukunft gestalten zu können, müssen digitalisierungstheoretische und -praktische Erwägungen sowohl in die Wahl der Steuerungsinstrumente wie auch in das Objekt der Steuerung einfließen. Angesichts der Vielfalt möglicher Regulierungsebenen und -objekte ist es einfach, den Blick für das Wesentliche zu verlieren: den Schutz der Werte und Rechte. Digitalisierungsregulierung droht so zum Selbstzweck zu verkommen und ihren wichtigen Gestaltungsanspruch in dem Maße einzubüßen, in dem sie zunehmend diffundiert.

Wer glaubt, dass die Regulierung der Digitalisierung alle Probleme löst, hat weder Regulierung noch Digitalisierung noch die damit verbundenen Probleme verstanden. Wer Digitalisierungspolitik mit Sicherheitsagenden überfrachtet, wird sie zum Erstarren bringen; wer wiederum emanzipatorischen Freiheitshoffnungen folgend auf Utopien blickt, die durch Technologie realisiert werden sollen, läuft Gefahr, konkrete Probleme zu übersehen. Gera-

30 Siehe hierzu auch die Beiträge von Eric Hilgendorf und von Lorena Jaume-Palasí in diesem Band.

31 Siehe hierzu den Beitrag von Christian Stöcker in diesem Band.

de in Mehrebenensystemen mit einer Vielfalt an Akteur*innen und Normenformen muss Klarheit herrschen darüber, wer im Mittelpunkt zu stehen hat: der Mensch. Menschenrechte schützen, Menschenwürde sichern, menschliche Sicherheit wahren, menschliche Entwicklung fördern – das muss Gestaltungsziel der Digitalpolitik bleiben.

3.2 Governance

Update für die Brücke und den Maschinenraum – der digitale Staat braucht neue Werte und Strukturen

Stefan Heumann

In einem Punkt herrscht parteiübergreifend Einigkeit. Es läuft nicht rund in der Digitalpolitik in Deutschland. Bei zahlreichen Vorhaben bleibt die Bundesregierung seit vielen Jahren weit hinter ihren selbst gesteckten Zielen zurück. Digitale Themen wirken immer noch wie Fremdkörper im politischen Betrieb. Man hört zwar auch von Politiker*innen und Minister*innen regelmäßig die großen Buzzwords wie künstliche Intelligenz, Blockchain oder Cloud-Computing. Und man gibt sich gerne nah am Puls der Zeit, wenn bei Interviews und in Diskussionsrunden ein »digitales Mindset« gefordert wird. Die Realität in Regierung und Verwaltung sieht aber ganz anders aus. Statt Mut und Bereitschaft, etwas Neues auszuprobieren, herrscht das Prinzip der Risikominimierung. Entscheidungsfindungen laufen streng hierarchisch. Und man schottet sich nicht nur so gut wie möglich nach außen ab, sondern kontrolliert auch möglichst penibel interne Informationsflüsse. Noch mehr Vorsicht herrscht in der Zusammenarbeit zwischen Ministerien, Behörden oder unterschiedlichen Verwaltungseinheiten. Offenbar gilt es hier, eigene Zuständigkeiten und Interessen zu verteidigen. Die Diskrepanz zwischen großen Ambitionen und trauriger Wirklichkeit wächst in der Digitalpolitik seit vielen Jahren kontinuierlich. Wir werden diesen Trend nur umkehren, wenn wir uns grundsätzlich mit unseren politischen Institutionen auseinandersetzen.

Strenge Hierarchien und Risikominimierung sind wichtige Werte, die fest in den Strukturen von Regierung und Verwaltung verankert sind. Sie sollen dafür sorgen, dass Regierungshandeln verlässlich und rechtskonform ist, Ministerien und Verwaltung möglichst gut gegen Einflussnahme von außen geschützt sind und Entscheidungsfindung auf die hierzu demokratisch legiti-

mierten Personen im Bundestag und die Leitung der Ministerien zugeschnitten ist. In der Praxis stoßen diese Werte allerdings zunehmend an ihre Grenzen. Und nicht nur das. Sie erfüllen oft auch ihre Zwecke nicht mehr, wenn eine zentrale Ressource der Politik – Handlungsfähigkeit – durch mangelnde Anpassungs- und Veränderungsbereitschaft unterminiert wird.

Neue Zeiten verlangen neue Strukturen

Der digitale Wandel stellt Organisationen vor ganz grundsätzliche Herausforderungen. Um ihn zu bewältigen, sind neue Werte und ein Update der Organisationen dringend nötig. Wer die Problemursachen wirklich verstehen will, sollte sich weniger mit dem Ressortzuschnitt einzelner Ministerien befassen und vielmehr mit den Arbeitsprozessen und -Strukturen in Regierung und Verwaltung beschäftigen. Um es bildlich auszudrücken: wir verbringen viel zu viel Zeit auf der Kommandobrücke, wo das Problem doch eigentlich im Maschinenraum liegt. Dieser Maschinenraum braucht dringend ein Update. Zu dieser Erkenntnis zu gelangen, hat gerade in Deutschland lange gedauert. Aber abgesehen von der Politik hat sie sich weitgehend durchgesetzt. Die Organisationen, die den digitalen Wandel erfolgreich meistern, haben sich nicht auf die Entwicklung von Strategien beschränkt. Sie haben vor allem tradierte Arbeits-, Organisations- und Denkweisen hinterfragt und ihre Arbeitskultur und -prozesse an neuen Werten ausgerichtet.

Hinter den Hypes neuer Managementmethoden und Arbeitsstrukturen wie Agilität, Open Innovation oder New Work steckt vor allem die Frage, wie Organisationen weiterentwickelt werden müssen, um angesichts der Veränderungsdynamiken in Wirtschaft und Gesellschaft, die von der Digitalisierung ausgelöst wurden, erfolgreich bestehen zu können. Das ist im Kern eine Werte-Diskussion. Es braucht Offenheit für neue Ansätze. Es braucht Mut, Neues auszuprobieren. Und es braucht einen Führungsstil, der nicht auf Ansagen von oben, sondern das Einbinden von Expertise und Kompetenzen setzt. Was für Organisationen in Wirtschaft und Gesellschaft gilt, gilt auch für den Staat. Sein Handeln, seine Arbeitsweise und seine Arbeitskultur müssen an neuen Leitprinzipien ausgerichtet werden, um die zentralen Herausforderungen des digitalen Wandels meistern zu können. Hierbei geht es vor allem um drei Aspekte:

(1) *Aufbau und Entwicklung von Expertise zum digitalen Wandel.* Hierzu braucht es eine Befähigung der eigenen Mitarbeiter*innen. Dies kann nur über Wertschätzung und bessere Einbindung von Fachexpertise gelingen. Angesichts des demografischen Wandels, wird der Staat stärker um die besten Expert*innen kämpfen müssen. Wertschätzung allein aber wird nicht ausreichen. Sie muss sich auch in den entsprechenden Strukturen widerspiegeln. Diese müssen dringend weiterentwickelt werden, um Arbeitsmethoden und Prozesse in Regierungsinstitutionen und Verwaltung zu modernisieren.
(2) *Öffnung für Austausch und Zusammenarbeit mit externer Expertise.* Keine Organisation kann angesichts der dynamischen Veränderungen alles relevante Wissen bei sich selbst vorhalten. Das verlangt von der politischen Führung eine gewisse Demut gegenüber den Herausforderungen und die Bereitschaft, sich für Expertise von außen, insbesondere aus der Zivilgesellschaft, zu öffnen. Denn nur so kann eine gemeinwohlorientierte Digitalpolitik in der Praxis gelingen.
(3) *Vereinfachung von Strukturen zur Stärkung der Handlungsfähigkeit.* Anstatt Kompetenzbereiche und Entscheidungsprozesse zu vereinfachen, geht die Politik in der Regel den Weg des geringsten Widerstands. Es werden gerne neue Institutionen und Zuständigkeiten geschaffen, aber Bestehendes nur selten infrage gestellt. Aber was kurzfristig politisch opportun ist, ist noch lange nicht effektiv. Bei aller Komplexität darf der Blick aufs große Ganze nicht verloren gehen.

In der Diskussion über die großen Leitlinien der Digitalpolitik muss auch die Frage aufgeworfen werden, welche Werte unsere staatlichen Institutionen brauchen, um eine gemeinwohlorientierte Digitalpolitik auch in der Praxis umsetzen zu können. Dieser Punkt wurde in den vergangenen Jahren sträflich vernachlässigt. Nur wenn die nächste Bundesregierung auch ihrem eigenem Wertekompass ein Update verordnet, wird uns die Umsetzung unserer großen Ziele in konkrete und effektive Lösungen gelingen.

1. Neue Expertise

Während sich Unternehmen schon seit vielen Jahren damit beschäftigen, wie sie digitale Innovator*innen anziehen und digitale Expertise ausbauen können, hat sich in Behörden und Verwaltung nur wenig getan. Stattdessen wird

das Problem gerne auf die Frage von Gehältern und Zulagen reduziert. Gerade in der Politik haben viele noch nicht verstanden, dass die Attraktivität des öffentlichen Dienstes nicht allein eine Frage des Gehalts ist. Oftmals viel abschreckender als mögliche Einkommenseinbußen sind hierarchische und stark formalisierte Arbeitskulturen und mangelnde Flexibilität in der Laufbahngestaltung. Damit sich hier etwas ändert, brauchen wir eine viel stärkere Wertschätzung von Expertise und eine Arbeitskultur, die die Entwicklung von Lösungen über das Umsetzen von Vorgaben stellt. Allerdings stehen diese Werte in Konflikt mit Grundprinzipien von Regierungs- und Verwaltungshandeln.

Ministerien und Behörden sind auf Stabilität ausgelegt. Die Beamtenlaufbahnen sorgen dafür, dass der Personalstamm über Jahrzehnte relativ stabil bleibt. Üblicherweise beenden Beamt*innen ihre berufliche Laufbahn im Staatsdienst mit der Pensionierung. Das begrenzt die Möglichkeiten, durch größere Personalfluktuation, wie in der Privatwirtschaft üblich, neue Kompetenzen aufzubauen oder das Kompetenzprofil des Personalstamms stark zu verändern. Den Neueinstellungen und Verbeamtungen kommt somit eine ganz besondere, strategische Bedeutung zu, denn hier werden auf Jahrzehnte ausgelegte Personalentscheidungen getroffen.

Das Beamtentum ist eine Grundsäule unseres Staatswesens. Es sichert die Unabhängigkeit von Regierungsapparat und Verwaltung gegen ungeziemende politische Einflussnahme. Allerdings erschweren starre Laufbahnmodelle und formalistische Beförderungskriterien den Aufbau neuer Expertise. Expertise zu digitalen Trends oder modernen Projektmanagementmethoden wird bisher intern bei Beurteilungen und Beförderungen nicht honoriert. In Bezug auf IT- und Digitalisierungsprojekte sind dadurch im letzten Jahrzehnt bedenkliche Abhängigkeiten entstanden. Heerscharen von Berater*innen gehen in Ministerien und Behörden ein und aus. Die Umsetzung zentraler Digitalisierungsprojekte von Bund und Ländern, wie zum Beispiel des Online-Zugangsgesetzes oder der IT-Konsolidierung des Bundes, in die Milliarden versenkt wurden, wären ohne riesige Beratungsaufträge gar nicht möglich. Diese beschränken sich hierbei nicht auf eine rein technische Umsetzung, sondern schließen in der Regel auch die Erstellung von Konzepten, Planung und strategische Steuerung mit ein.

Hier entsteht mittel- und langfristig ein außerordentliches Problem für die Handlungsfähigkeit und Legitimität des Staates. Während die Ansprüche an den Staat in der Gesellschaft steigen und die politisch Verantwortlichen in Regierung und Parlamenten immer ambitioniertere Ziele für die Digitalpoli-

tik formulieren, fehlt es an grundlegenden Kompetenzen in Ministerien und Verwaltung, um diese Ambitionen in konkrete und praktikable Maßnahmen zu überführen und entsprechend umzusetzen. Die bisherige Bilanz spricht nicht für das Modell, Kernkompetenzen an externe Berater*innen zu übertragen. Zusätzlich verschärft sich die Handlungsunfähigkeit, da überfällige Verwaltungsreformen und der Aufbau eigener Kompetenzen weiter aufgeschoben werden.

Das Problem ist durchaus erkannt. Der Bundesrechnungshof hat bereits 2014 den Aufbau von Projektmanagementkompetenzen für große IT-Projekte im Bundesinnenministerium gefordert.[1] Passiert ist seitdem leider wenig. Es gibt im öffentlichen Dienst mittlerweile eine Fachkräftezulage, um besser mit dem Privatsektor um stark nachgefragte IT-Expert*innen konkurrieren zu können. Die Bundesregierung hat 2020 den Grundstein für den Aufbau einer eigenen Softwareschmiede gelegt, die beispielsweise als GmbH flexiblere Gehälter zahlen kann.[2] Diese und weitere Initiativen sind wichtig. Sie sind aber nicht der große Wurf. Der Aufbau digitaler Expertise und die Aneignung neuer Management- und Methodenkompetenzen in Ministerien und Verwaltung müssen politische Priorität erlangen.

Den Bedarf an neuen Kompetenzen belegen die beiden Fellowship Programme Tech4Germany[3] und Work4Germany[4]. Beide Programme stoßen in den Ministerien auf großes Interesse und können wichtige Impulse geben. Für langfristigen Kompetenzaufbau muss es aber gelingen, die über die Fellowships angeworbene Expertise fest in Ministerien und Verwaltung zu integrieren.

Wer Probleme der Moderne lösen will, muss sich selbst modernisieren

In Bezug auf den Aufbau digitaler Expertise gibt es zwei Bereiche, die zugleich besonders bedeutend wie auch kontrovers sind. Der erste Bereich umfasst

1 Vgl. https ://police-it.net/bundesrechnungshof-fordert-grundlegende-veraenderung-vom-bmi

2 Vgl. https ://digitalservice4germany.com/ueberuns/

3 Tech4Germany schickt für drei Monate Digital-Talente in Ministerien und Bundesbehörden, um mit agilen und nutzerzentrierten Methoden erste Prototypen für digitale Innovationen zu entwickeln. https://tech.4germany.org/

4 Work4Germany soll über ein sechs-monatiges Fellowship moderne Arbeitsmethoden in die Bundesministerien bringen.

Einstellungs- und Beförderungskriterien innerhalb der Verwaltung. So mangelt es in den Verwaltungen vor allem in den Führungs- und Leitungsebenen an Diversität, digitaler Expertise und Methodenkompetenzen. Der Ursprung des Problems liegt bereits in den Einstellungskriterien. Formalien wie Zeugnisse und Bildungsabschlüsse dienen als Ausschlusskriterien. Viel wichtiger wäre es allerdings, die Bewerber*innen noch stärker nach ihren Kompetenzen und Erfahrungen zu bewerten. Die Privatwirtschaft hat hier schon lange erkannt, dass es wichtiger ist, was die Bewerber*innen können, statt darauf zu achten, ob das Informatikstudium ordentlich abgeschlossen wurde. Die Flexibilisierung der Einstellungsvoraussetzungen und die stärkere Gewichtung von nicht formal nachweisbaren Kompetenzen würden den öffentlichen Dienst und die Beamtenlaufbahnen generell für einen wichtigen Talentpool öffnen.

Besonders wichtig hierbei sind Anreize und Belohnungen für ressortübergreifende Zusammenarbeit und Wissensaustausch. Denn nur so können die in den einzelnen Ministerien und Verwaltungseinheiten vorhandenen Kompetenzen optimal genutzt und in den Dienst des großen Ganzen gestellt werden. Es muss um das Erreichen leitender Ziele und nicht das Abarbeiten des ministeriumseigenen Lastenhefts gehen. Leistungsbewertungen sollten nicht allein von Vorgesetzten eingeholt werden, sondern auch von Mitarbeiter*innen und Kontaktpersonen außerhalb der Organisation. Kommunikations- und Problemlösungskompetenzen und Teamfähigkeit sowie die Bereitschaft zur Weiterentwicklung und zum Lernen sollten viel stärker berücksichtigt werden. Die starre Eingruppierung in unterschiedliche Laufbahnen (mittleren, gehobenen und höheren Dienst) sollte überdacht werden. Vielmehr sollten Fähigkeit und Leistung über Aufstiegschancen und Karriereoptionen bestimmen. Die Identifikation und Förderung von internen Innovator*innen muss zu einem zentralen Ziel für die Personalpolitik von Ministerien und Verwaltungen werden.

Der digitale Wandel ist zu groß, um ihn mit organisationseigenem Wissen zu gestalten

Der zweite Bereich bezieht sich darauf, wie der Staat auch kurzfristig seine digitale Expertise ausbauen kann. Hierzu muss der Staatsdienst stärker für Expertise von außen geöffnet werden, insbesondere auf Führungs- und Leitungsebene. Die sogenannte Drehtür – der Austausch von Spitzenpersonal zwischen Politik und Wirtschaft – wird zurecht kritisch gesehen. In

Deutschland ist es aber keine wirkliche Drehtür, sondern vielmehr eine einseitige Schwingtür für Spitzenpolitiker*innen, die ihre politischen Kontakte und Netzwerke durch wirtschaftliche Lobbyarbeit versilbern. Eher selten finden sich dagegen Fälle von angesehenen Expert*innen und Führungspersonen, die aus der Privatwirtschaft, Wissenschaft oder zivilgesellschaftlichen Organisationen auf Führungspositionen in Ministerien oder Verwaltung wechseln.

Dieser mangelnde Austausch schadet staatlichen Institutionen mehr, als er ihnen nützt. Neue Expertise, wie zum Beispiel zur Gestaltung des digitalen Wandels oder zur Konzeption und Umsetzung von IT-Projekten, kann so nicht einfach über Personen von außen mit dem entsprechenden Fachwissen in die Ministerien geholt werden. Es fehlt bei internen Beratungen und Entscheidungsprozessen an wichtigen Impulsen, wenn fast die gesamte Leitungsebene aus dem eigenen Haus kommt und berufliche Erfahrungen aus anderen Kontexten bereits sehr lange zurückliegen.

Bei Quereinsteiger*innen aus Wissenschaft, zivilgesellschaftlichen Organisationen und Privatwirtschaft sind natürlich auch mögliche Interessenskonflikte zu bedenken. Grundsätzlich können diese Konflikte mit klaren Regeln und Transparenz gut kontrolliert werden. Viel problematischer sind hingegen die starke Abhängigkeit von externen Berater*innen und die damit verbundenen Interessenskonflikte. Angesichts des Mangels an Durchlässigkeit ist es aber zurzeit die einzige Möglichkeit, nicht vorhandene eigene Expertise zu kompensieren. Letztendlich schafft die Verteidigung des Staatsdienstes gegen Flexibilisierung und Quereinsteiger*innen so langfristig viel größere Abhängigkeiten von privatwirtschaftlichen Interessen. Eine Öffnung und Flexibilisierung würde hingegen Performanz und Fähigkeiten des Staatsdienstes stärken und einer langfristig sehr schädlichen Aushöhlung von Kernkompetenzen entgegenwirken.

2. Offenheit als Leitprinzip

Ob Open Innovation oder Open Source – Offenheit ist eines der zentralen Paradigmen der digitalen Transformation. Das Internet selbst steht für Offenheit. Es bietet eine globale Plattform für Kommunikation, Wissensaustausch und Zusammenarbeit. Offenheit ist auch zu einem wichtigen strategischen Ansatz in der Organisationsentwicklung geworden. Denn mit der Verbreitung digitaler Technologien und globaler Vernetzung haben sich Innovationszyklen

rasant beschleunigt. Das gilt insbesondere für Software-Anwendungen. Internetplattformen und Technologiekonzerne wie Google, Amazon oder Facebook können neue Dienste und Funktionen quasi per Knopfdruck für Milliarden von Nutzer*innen weltweit zugänglich machen.

Angesichts der neuen Dynamiken, mit denen sich das technologische und geschäftliche Umfeld nicht mehr nur im Tech-Sektor, sondern mittlerweile in der Wirtschaft insgesamt wandelt, ist Öffnung für externe Expertise zu einer zentralen Managementherausforderung geworden. Es gibt eine große Bandbreite von Ansätzen und Strategien, mit denen Unternehmen sich dieser Herausforderung stellen. Bei der Entwicklung von Software setzen viele auf offene Standards und offenen Programmiercode (Open Source).Oder sie laden externe Entwickler*innen über Ideenwettbewerbe zur Mitarbeit an Innovationen ein. Größere Unternehmen versuchen über Förderprogramme (sogenannte Acceleratoren) und Wagniskapitalfonds Beziehungen zu innovativen Start-ups herzustellen. Dabei geht es vor allem um das bei diesen jungen Unternehmen vorhandene Know-how zu digitalen Trends und damit verbundene Innovationen und Geschäftsideen. Es ist mittlerweile eine eigene kleine Industrie entstanden, die mit einer Mischung aus Konferenz-, Netzwerk- und Beratungsformaten etablierte Unternehmen dabei unterstützt, Netzwerke zu den Innovator*innen und Vordenker*innen des digitalen Wandels aufzubauen und Wissensaustausch zu fördern.

Öffnung nach außen beruht auf der Einsicht, dass keine Organisation, so groß und ressourcenreich sie auch sein mag, die Herausforderungen des digitalen Wandels alleine meistern kann. Vernetzung und Austausch sollen helfen, relevante Entwicklungen und Trends möglichst früh zu erkennen und von externer Expertise bei Innovationen zu profitieren. Das kann nur in Kombination mit einer ausgeprägten Lern- und Fehlerkultur funktionieren. Das heißt, dass Offenheit auch eine Kultur- und Haltungsfrage ist. Denn nur dann können die Impulse von außen auch aufgegriffen und produktiv verarbeitet werden. Und genau das macht Öffnung in der Praxis so schwierig. Sie erfordert eine gewisse Demut – die Erkenntnis, dass die Organisation nicht alle Herausforderungen aus sich selbst heraus bewältigen kann. Und sie erfordert auch Mut zu Risiko und Fehlern. Denn die Öffnung nach außen bedeutet immer einen gewissen Kontrollverlust. Ohne selbst eigenes Wissen preiszugeben, kann der Beziehungsaufbau und Austausch mit Externen nicht gelingen.

Transparenz und Beteiligung für Wissen und Legitimität

Gerade für staatliche Institutionen bietet die Öffnung für externe Expertise in der Digitalpolitik riesige Chancen. In der Realität wirken Ministerien und Regierungsapparate aber wie Trutzburgen, die sich von der Außenwelt abschotten. Selbst die formalistischen Beteiligungsprozesse funktionieren nicht richtig. Einen neuen, unrühmlichen Rekord setzte im Dezember 2020 das Bundesministerium des Innern, für Bau und Heimat (BMI). Es räumte Verbänden und Zivilgesellschaft bei einem über 100-seitigen Gesetzestext gerade einmal 28 Stunden für eine Kommentierung und Stellungnahme ein. Da extrem kurze Fristen im Rahmen der sogenannten Verbändebeteiligung leider kein Einzelfall sind, fordern eine Reihe von Verbänden und zivilgesellschaftlichen Organisationen in einem offenen Brief an die Bundesregierung »angemessene Fristen statt Scheinbeteiligung«.[5] Dabei geht es grundsätzlich auch um mehr Transparenz bei Gesetzgebungsverfahren, wie zum Beispiel die frühzeitige Veröffentlichung von Entwürfen und die Dokumentation von Veränderungen an den Gesetzestexten.

Mit der Einbeziehung der zivilgesellschaftlichen Expertise für eine gemeinwohlorientierte Gestaltung der Digitalisierung fremdelt die Bundesregierung gewaltig.[6] Wenn man einmal von dem problematischen Demokratieverständnis absieht, das diese kurzen Beteiligungsfristen offenbaren, schadet dieses Verhalten auch der Qualität der Gesetzesvorhaben. Denn so wird ein produktiver Austausch mit Kritik und Ideen von außen unmöglich gemacht. Zur Verteidigung eines solchen Vorgehens wird oft angeführt, dass die Gesetzesvorschläge möglichst ohne Lobbyeinfluss in den Ministerien erarbeitet werden sollen. Aber gerade die vorherrschende Praxis der Abschottung gibt den wirtschaftlich stärksten Lobbygruppen den größten Einfluss. Denn nur sie verfügen über die Ressourcen und Kontakte, um trotzdem ihre Ideen und Positionen in die Entwicklung von Gesetzen und Verordnungen einzubringen. Wissenschaftler*innen oder zivilgesellschaftliche Organisationen verfügen in der Regel nicht über solche Möglichkeiten der Einflussnahme und ihre Expertise bleibt dann außen vor. Aber: Offenheit ermöglicht Vielfalt und Transparenz erhöht Legitimität.

Der digitale Wandel verschärft diese Problematik nun dramatisch. Wenn selbst globale Konzerne mit riesigen Forschungs- und Entwicklungsabteilu-

5 https://gi.de/meldung/offener-brief-ausreichende-fristen-fuer-verbaendebeteiligung

6 Siehe hierzu auch den Beitrag von Julia Kloiber und Elisa Lindinger in diesem Band.

gen sich eingestehen müssen, dass sie ohne eine Öffnung nach außen den dynamischen Innovationszyklen nicht mehr gewachsen sind, gilt diese Herausforderung erst recht für den Staat. Schließlich erwarten wir von unseren Politiker*innen, dass sie mit Gesetzen und Fördermaßnahmen den digitalen Wandel im Interesse der Gesellschaft gestalten. Dynamische Veränderungen treffen hier auf Institutionen in Regierung und Verwaltung, die auf Hierarchie, Kontrolle und Risikominimierung ausgerichtet sind. Eine stärkere Öffnung nach außen kollidiert mit der immanenten Systemlogik staatlicher Institutionen.

Der Staat als lernende Organisation

Eine solche Öffnung setzt ein ganz neues Selbstverständnis von Politik und Verwaltung voraus. Denn es wäre nicht damit getan, Expertenanhörungen im Bundestag oder die Beteiligung an Gesetzgebungsprozessen zu verbessern. Es geht vielmehr darum, den Staat als lernende Organisation zu begreifen und zu befähigen. Dies erfordert zuvorderst eine neue Haltung an der Spitze von Regierung, Ministerien und Behörden: ein Eingeständnis, dass man auf die vielen neuen Fragen selbst keine Antworten hat, und die Bereitschaft, die eigene Organisation und Mitarbeiter*innen bei der Suche nach Antworten bestmöglich zu unterstützen. Aus dieser Haltung folgt, dass eine Öffnung nach außen stattfindet, dass neue Netzwerke zu den Vordenker*innen und Expert*innen des digitalen Wandels aufgebaut werden und dass möglichst viele unterschiedliche Perspektiven in den Austausch einbezogen werden.

Es gibt starke Widerstände gegen Öffnung. Dabei wird vor allem das Argument angeführt, dass die politischen Vorgaben von oben kommen müssen, von den durch Wahlen demokratisch legitimierten Politiker*innen in Bundestag und Regierung. An diesem Prinzip soll auch nicht gerüttelt werden. Die politischen Ziele und Prioritäten sollen weiterhin von oben vorgegeben werden. Die Konzepte zu deren Umsetzung werden aus Regierungsapparaten und Ministerien heraus erarbeitet. Dort sind Öffnung und Austausch aber eher die Ausnahme. Wir kommen aber nur weiter, wenn diese Werte auf allen Ebenen des Regierungs- und Verwaltungshandelns die Regel sind.

Kulturwandel für den Organisationswandel

Die Öffnung kann nur gelingen, wenn sie von den politisch Verantwortlichen eingefordert und vorgelebt wird. Das erfordert ein Umdenken. Denn viele in

der politischen Verantwortung meinen, dass von ihnen in erster Linie Antworten erwartet werden. Es können aber nur diejenigen gute Antworten geben, die zuvor die richtigen Fragen gestellt haben. Diese Fähigkeit muss in öffentlichen Debatten und den Bewertungen von Politiker*innen viel mehr Raum bekommen. Und das Stellen guter Fragen muss zur Leitkultur in unseren Ministerien und Verwaltungen werden, einhergehend mit der Erkenntnis, dass ohne Öffnung und Austausch keine guten Antworten gefunden werden können.

Es gibt hierzu bereits erste Anstrengungen. Das oben angesprochene Work4Germany Fellowship soll die Auseinandersetzung mit innovativen Methoden und Management-Ansätzen in der Bundesverwaltung fördern. Das Digital Innovation Team im BMI beschäftigt sich mit agilen Arbeitsmethoden und scheut dabei nicht davor zurück, neue Wege zu gehen und sich auch mit Digitalisierungsexpert*innen außerhalb des öffentlichen Dienstes zu vernetzen und auszutauschen.[7] Die Bundesregierung hat bei der Durchführung ihres ersten Hackathons, einem digitalen Beteiligungsprozess zur Entwicklung von Innovationen und ersten Prototypen, gleich eine Rekordbeteiligung erzielt.[8] Allerdings machte der Hackathon auch deutlich, dass es in den Regierungsbehörden an Erfahrung und Strukturen mangelt, um aus dem Austausch mit Innovator*innen aus der Gesellschaft nachhaltig nutzbare Lösungen zu entwickeln und vor allem diese umzusetzen.[9]

In vielen weiteren Behörden und Ministerien sind in der vergangenen Legislaturperiode erste Versuche mit neuen Methoden und Arbeitsansätzen gestartet worden. Und die Innovator*innen aus der Verwaltung haben auch ihre eigene Plattform für hierarchie- und organisationsübergreifende Vernetzung und Austausch gegründet.[10] Aber zu einer richtigen Öffnung ist es bisher noch nicht gekommen. Diese kann nur gelingen, wenn Austausch mit der Zivilgesellschaft und externer Expertise nicht als Last, sondern als Chance gesehen wird. Hierzu braucht es politisch Verantwortliche, die diese Haltung vorleben und durch entsprechende Vorgaben für eine stärkere Öffnung von Regierung und Verwaltung nach außen sorgen.

---

7 Vgl. https ://verwaltungsrebellen.de/dat-is-dit/

8 Vgl. https://wirvsvirus.org/

9 Vgl. Marcel Grzanna, »Der Hackathon Hype« Tagesspiegel Background Digitalisierung & KI vom 13.07.2020 https://background.tagesspiegel.de/digitalisierung/der-hackathon-hype

10 Vgl. https ://next-netz.de/uber-uns

3. Vereinfachung der Governance – der Komplexitätsfalle entkommen

Die Gestaltung der digitalen Transformation stellt Gesellschaft, Wirtschaft und Politik vor große Herausforderungen. Sie betrifft alle Politikfelder und politischen Institutionen. Nachdem es anfangs vor allem Skepsis gegenüber der Relevanz von Vernetzung und digitalen Technologien gab, hat mittlerweile ein regelrechtes Wettlaufen begonnen, um sich für die zentralen Zukunftsaufgaben zu positionieren. So wird innerhalb und zwischen den Ministerien und Regierungsebenen um Zuständigkeiten und Führungsansprüche gestritten. Anstatt die Chance zu ergreifen, im Rahmen der neuen digitalen Herausforderungen Zuständigkeiten klarer zu regeln und Entscheidungsprozesse zu vereinfachen, wird die Steuerung digitalpolitischer Vorhaben immer komplexer. Selbst für ausgewiesene Expert*innen ist es oft schwierig, über die vielen unterschiedlichen Initiativen und Maßnahmen und die Frage, wer eigentlich genau für was zuständig ist, den Überblick zu behalten.

Dieses Problem wird zusätzlich durch die europäische Integration und die damit verbundene gewachsene Bedeutung der EU verschärft. Gerade in der Digitalpolitik spielt die EU zunehmend eine wichtige Rolle. Mit dem Ziel eines harmonisierten digitalen Binnenmarkts werden zentrale digitalpolitische Regulierungsvorhaben von Brüssel aus vorangetrieben. In diesem Aushandlungsprozess spielen die Mitgliedsstaaten aber weiterhin eine wesentliche Rolle. Die Umsetzung der Initiativen und Regulierungen der EU liegt bei den Mitgliedsstaaten und ihren hierfür zuständigen Institutionen. Das heißt, dass mit der EU eine weitere politische Ebene in der Digitalpolitik hinzugekommen ist, die auf komplexe, bereits bestehende nationale Strukturen aufsetzt.

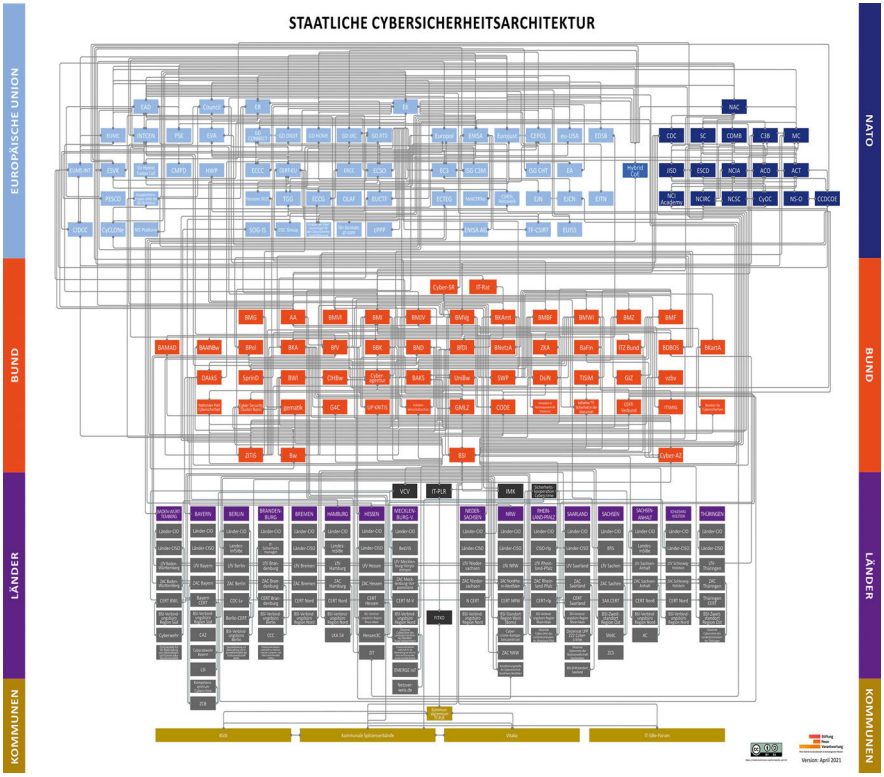
Der ehemalige US-amerikanische Außenminister Henry Kissinger soll einst in Bezug auf die europäische Integration gesagt haben: »Wen rufe ich dann an, wenn ich Europa anrufen will?« Entscheidungen werden in der EU in Aushandlungen zwischen Parlament, Kommission und Rat getroffen. Hinzu kommt, dass gerade die großen Mitgliedsstaaten über sehr viel Einfluss auf EU-Entscheidungen verfügen. Wenn diese unterschiedlichen Akteure keine gemeinsamen Interessen verfolgen und divergierende Positionen vertreten, ist es schwierig, eine Position der EU zu definieren. Dann wünschen sich sicherlich viele die eine Telefonnummer, die einem weiterhelfen kann. Ähnlich verhält es sich mit der Digitalpolitik. Zwar hat die Bundesregierung 2018 erstmals die Funktion einer Staatsministerin für Digitalisierung im Kanz-

leramt geschaffen. Aber ob Datenschutz, Verwaltungsdigitalisierung oder IT-Sicherheit – für zentrale Fragen der Digitalpolitik ist die Staatsministerin nicht zuständig.

Klare Verantwortlichkeiten statt Strickpulli

Anstatt einer Klärung von Zuständigkeiten und einer Verschlankung der Regulierungs- und Verwaltungsprozesse ist in der Politik eine Zunahme an involvierten Akteuren und an Komplexität von Koordination und Abstimmung zu beobachten. Ein Beispiel:

Abbildung 1: Akteure und Zuständigkeiten in der deutschen Cybersicherheitspolitik



Quelle: Stiftung Neue Verantwortung (Dr. Sven Herpig und Christina Rupp) – 6. Auflage April 2021 – CC-BY-SA

Die Übersicht über Akteure und Zuständigkeiten in der deutschen Cybersicherheitspolitik[11] sieht aus wie ein »Strickpulli« (vgl. Abb. 1). Über zweihundert unterschiedliche Organisationen sind dort von Länder- über Bundesbis hin zur EU-Ebene abgebildet. Die auf der Grafik mit Verbindungen visualisierten Beziehungen zwischen den Akteuren belegen eindrucksvoll die steigende Komplexität dieses Politikfelds. Allein zehn Ministerien haben unterschiedliche Berührungspunkte mit dem Thema Cybersicherheitspolitik. In den letzten Jahren sind noch verschiedene neue Institutionen von der Cyberagentur bis hin zur Zentralen Stelle für Informationstechnik im Sicherheitsbereich hinzugekommen beziehungsweise befinden sich im Aufbau. Eine kohärente Cybersicherheitspolitik wird in dieser komplexen Akteurslandschaft zur Mammutaufgabe. Hinzu kommt, dass die vielen unterschiedlichen Organisationen miteinander um hoch nachgefragte IT-Fachkräfte und Cybersicherheitsexpert*innen konkurrieren – und das in einem Umfeld, wo Unternehmen in der Regel bessere Gehälter und attraktivere Arbeitsbedingungen zu bieten haben.[12]

In vielen Bereichen ist die Komplexität über Jahrzehnte historisch gewachsen. Dies ist auch dem Föderalismus geschuldet. Dieser hat gegenüber politischem Zentralismus viele Vorteile. Er verhindert Machtkonzentration auf bundespolitischer Ebene. Viele staatliche Aufgaben können dezentral deutlich besser an die lokalen Bedingungen angepasst werden. Staatliche Institutionen sind im Föderalismus einfach dichter an den Bürger*innen dran. Bei digitalpolitischen Vorhaben können diese Stärken des Föderalismus aber oft gegeneinander ausgespielt werden oder wandeln sich gar in Schwächen. Das ist insbesondere bei digitalpolitischer Regulierung und Aufsicht der Fall. So ist es sinnvoll, dass die Bundesländer ihre Politik auf die jeweiligen geografischen, sozialen und wirtschaftlichen Verhältnisse zuschneiden. Wenig Sinn ergibt es dagegen, sich in 16 Ländern parallel mit der Frage zu befassen, wie das Internet am besten reguliert werden sollte. Denn ob Düsseldorf oder München, Hamburg oder Dresden: Das Internet sieht überall in Deutschland gleich aus.

Die föderale Zersplitterung schwächt staatliche Regulierungsfähigkeiten, Aufsicht und Rechtsdurchsetzung gegenüber weltweit operierenden Konzer-

11 Vgl. https://www.stiftung-nv.de/de/publikation/akteure-und-zustaendigkeiten-der-deutschen-cybersicherheitspolitik

12 Vgl. https ://www.stiftung-nv.de/de/publikation/warum-dem-staat-it-sicherheitsexpertinnen-fehlen

nen. Da es abgesehen von der Einigung auf technische Standards nie gelungen ist, sich auf einen internationalen Regulierungsrahmen zu verständigen, versuchen Staaten mit nationaler Gesetzgebung ihre Interessen gegenüber den globalen Internetkonzernen durchzusetzen.[13] Die dominanten Internetplattformen gehören zu den wertvollsten Unternehmen der Welt. Entsprechend verfügen sie über große Ressourcen, um sich gegenüber staatlichen Regulierungsversuchen zu behaupten. Hinzu kommt, dass diese Unternehmen in einem extrem dynamischen Markt agieren und mit ihren Technologien und Geschäftspraktiken der Politik in der Regel einige Jahre voraus sind.

Wenn zu viele Wächter weniger Schutz bedeuten

Während sich weltweit Staaten mit der Herausforderung konfrontiert sehen, wie sie mächtige, sehr dynamische und global agierende Internetplattformen erfolgreich regulieren können, sind bei uns zwei in diesem Bereich zentrale Politikfelder Ländersache. Die Datenschutzaufsicht fällt in Deutschland in den Zuständigkeitsbereich der Länder. So sind die Landesdatenschutzbehörden für die Einhaltung der Datenschutzregeln bei Unternehmen verantwortlich und haben Regelverstöße gegen die Konzerne anzuzeigen und das Recht durchzusetzen. Die magere Bilanz hierbei liegt aber nicht allein an der Zersplitterung von Kompetenzen über 16 Landesbehörden. Vor dem Inkrafttreten der Datenschutz-Grundverordnung im Mai 2018 entzogen sich Konzerne wie Facebook und Google auch immer wieder erfolgreich dem Zugriff deutscher Aufsichtsbehörden durch die, auch von deutschen Gerichten bestätigte, Zuständigkeit der Datenschutzbehörden Irlands, wo viele der großen US-Tech-Unternehmen ihre Europazentrale eingerichtet haben.

Bei der Durchsetzung des Datenschutzes ist schon lange klar, dass dies am besten auf europäischer Ebene gelingen kann. Denn nur so lässt sich verhindern, dass die Konzerne sich gezielt Standorte in der EU suchen, wo es an Ressourcen oder Willen zu einer effektiven Aufsicht fehlt. Die europäische Datenschutz-Grundverordnung hat zwar zu einer Vereinheitlichung der Regeln in der gesamten EU geführt. Für die Durchsetzung bleiben aber die Aufsichtsbehörden der Mitgliedsstaaten zuständig. Das heißt, dass in Deutschland weiterhin 16 Landesdatenschutzbehörden parallel Personalressourcen und Expertise aufbauen und sich in der Regelauslegung und

13 Siehe hierzu auch den Beitrag von Matthias C. Kettemann in diesem Band.

-anwendung abstimmen müssen. Das ist gerade bei komplizierten rechtlichen und technischen Fragen ein großer Nachteil. Schließlich funktionieren Facebook oder Google für eine Nutzerin in Baden-Württemberg genauso wie für einen Nutzer in Hamburg. Eine starke nationale Aufsichtsbehörde könnte die Ressourcen viel besser bündeln und sich so auch viel schneller und effektiver in oftmals sehr komplexe Datenverarbeitungsvorgänge einarbeiten. Zusätzlich würden der Koordinierungsaufwand und die Komplexität sinken, wenn es sowohl für die Politik in Deutschland als auch die EU eine zentrale Ansprechpartnerin für Datenschutzfragen gäbe.[14]

Wer reguliert die Plattformen?

Mit der Veränderung des Medienkonsums hin zu digitalen Angeboten sind die globalen Internetplattformen mittlerweile auch in der Verbreitung von medialen Inhalten zu mächtigen Gatekeepern aufgestiegen. Die Zuständigkeit der Länder für Medienpolitik ist derweil beibehalten worden. Der 1991 zwischen den Ländern ausgehandelte Rundfunkstaatsvertrag deckt schon seit vielen Jahren wichtige Bereiche der Mediennutzung nicht mehr ab, da Rundfunk, Fernsehen und Printmedien kontinuierlich an Bedeutung verloren beziehungsweise sich ins Internet verlagert haben. Nach einem langwierigen Prozess wurde 2020 ein neuer Medienstaatsvertrag geschlossen, der die Regulierungslücken im digitalen Bereich schließen soll. Es ist aber schon jetzt abzusehen, dass die Aufteilung der Zuständigkeit über 16 Landesmedienanstalten einer effektiven Durchsetzung und Weiterentwicklung des Regelwerks im Wege stehen wird.[15] Auch hier wäre eine Bündelung der Ressourcen dringend notwendig, um besser mit der Macht, Komplexität und Dynamik der großen Internetplattformen umgehen zu können. Mit der Regulierung der Internetplattformen durch den Digital Service Act und den Digital Market Act spielt die EU auch in der Medienregulierung eine immer wichtigere Rolle.

Datenschutz und Plattformregulierung sind nur zwei prominente Beispiele. Generell wird die Bedeutung der EU bei digitalpolitischen Regulierungsfragen weiter wachsen, sei es beim Einsatz von künstlicher Intelligenz oder bei Versuchen zur effektiveren Besteuerung der Digitalkonzerne. Nur so

14 Vgl. https ://www.golem.de/news/wirtschaftsminister-landesdatenschuetzer-sollen-kontrolle-ueber-firmen-verlieren-2006-148872.html

15 Vgl. https ://netzpolitik.org/2020/medienstaatsvertrag-der-lange-kampf-gegen-desinformation/

lässt sich die Vision eines einheitlichen europäischen digitalen Binnenmarkts verwirklichen. In der Praxis hat das in Deutschland dazu geführt, dass zum Zusammenspiel von Bund und Ländern die EU als weitere Regulierungsebene hinzugekommen ist. Der damit verbundene Koordinierungs- und Abstimmungsaufwand ist riesig. Zusätzlich verhindert die Zersplitterung eine Zusammenführung von Ressourcen, um den Regulierungsherausforderungen besser begegnen zu können.

Neu ist nicht immer besser

Der Ausbau von EU-Kompetenzen bei gleichzeitigem Beharren auf föderalen Strukturen schwächt Deutschlands Fähigkeiten für eine effektivere und dynamischere Regulierung und Aufsicht über digitale Märkte und Plattformen. Hier zeigt sich wieder die generelle Tendenz in der Politik, neue Strukturen, Institutionen und Kompetenzen zu schaffen, aber nur selten Bestehendes anzutasten oder infrage zu stellen. Denn auch auf nationaler Ebene haben wir es mit einem wachsenden Geflecht an überlappenden und oft auch miteinander konkurrierenden Institutionen zu tun. So entsteht über Jahrzehnte ein immer komplexeres Geflecht an Institutionen und Zuständigkeiten, das politische Entscheidungs- und Handlungsfähigkeit untergräbt. Auch hier brauchen wir zuvorderst Mut, dieses Problem offen auszusprechen. Es ist einfacher und konfliktvermeidend, Neues zu fordern anstatt Bestehendes infrage zu stellen. Beides sollte aber zusammengehören wie die zwei Seiten einer Medaille.

Die Frage nach der Komplexität der Governance-Strukturen in der Digitalpolitik betrifft nicht nur das Zusammenspiel und die Verteilung von Zuständigkeiten zwischen EU, Bund und Ländern. Hier müssten wir uns endlich ehrlich eingestehen, dass die in vielen Bereichen sinnvolle Forderung nach stärkeren EU-Kompetenzen mit einer Anpassung und Bündelung von Kompetenzen auf nationaler Ebene einhergehen muss. Diese Komplexitätsfalle stellt sich aber auch für die nationale Digitalpolitik insgesamt. Auch hier sehen wir die Tendenz, neue Organisationen und Kompetenzen zu schaffen und dabei die Frage nach der Kohärenz des großen Ganzen aus den Augen zu verlieren. Auch hier gilt, dass jede Diskussion über die Schaffung neuer Institutionen und Kompetenzen mit der Frage nach der Verschlankung und Vereinfachung von Zuständigkeiten und Entscheidungsprozessen und der Verbesserung ressortübergreifender Zusammenarbeit verknüpft werden sollte.

4. Fazit: Wenn schon Digitalministerium, dann als Treiber der Transformation unseres Staatswesens

Es ist viel zu tun, damit digitalpolitische Ambitionen endlich erfolgreich umgesetzt werden. Hierfür brauchen wir ein neues Leitbild für staatliches Handeln. In der politischen Debatte wird die Frage leider sehr verkürzt dargestellt. Anstatt über ein neues Wertesystem für unsere politischen Institutionen zu diskutieren, geht es in Berlin vor allem um Ressortzuschnitte. Die Frage, ob wir ein Digitalministerium bekommen und welche Kompetenzen es erhalten soll, ist aber nicht die entscheidende. Ein Digitalministerium kann hilfreich sein. Aber nur als ein Teil einer viel umfassenderen Reformagenda. Strukturen und Arbeitsprozesse in Ministerien, öffentlicher Verwaltung und Behörden – der Maschinenraum für die Umsetzung unserer digitalpolitischen Ideen – muss dringend auf den Prüfstand. So schaffen wir die Voraussetzungen, dringend benötigte Expertise zur Gestaltung des digitalen Wandels in staatlichen Institutionen massiv auszubauen. Hierfür braucht es eine neue Führungs- und Lernkultur und eine Öffnung nach außen. Wir müssen auch endlich einen Weg aus der Komplexitätsfalle finden. Das geht nur mit einer ehrlichen Diskussion über die Weiterentwicklung des Föderalismus und mit dem Anspruch, nicht nur Neues zu schaffen, sondern auch Bestehendes weiterzuentwickeln, Expertise zu bündeln und Entscheidungswege zu vereinfachen.

Die Fragmentierung von Zuständigkeiten und die hohe Komplexität der Herausforderungen führen dazu, dass wir uns im Kleinklein verlieren. Es braucht daher in der Regierung einen Ort, wo neue Ansätze der Öffnung, der Beteiligung und Einbindung externer Expertise und der Verschlankung von Verwaltungsprozessen entwickelt und ausprobiert werden können. Es braucht einen Ort, der als Impulsgeber und Treiber für die Transformation von Regierung und Verwaltung hin zum lernenden Staat fungiert. Und es braucht einen Ort, wo wir aufs große Ganze schauen und uns Gedanken machen, wie wir Governance-Strukturen und Zuständigkeiten am besten weiterentwickeln und reformieren, um der Komplexitätsfalle zu entkommen. Dieser Ort kann gerne Digitalministerium heißen. Wenn das am Ende aber nicht mehr bedeutet, als dass Zuständigkeiten, Abteilungen und Referate auf Organigrammen hin und her geschoben werden, dann werden wir pünktlich zur Bundestagswahl 2025 wieder diskutieren, warum es nicht läuft mit der Digitalpolitik in Deutschland.

3.3 Recht
Wenn Gerichte es im digitalen Zeitalter richten müssen

Ulf Buermeyer und Malte Spitz

Als im Mai 1949 das Grundgesetz der Bundesrepublik Deutschland verabschiedet wurde, sahen sich die Verfasser*innen einer Lebenswelt gegenüber, die mit der unsrigen kaum zu vergleichen ist. Computer im heutigen Sinne gab es nicht, das Internet sollte erst Jahrzehnte später erfunden werden. Trotzdem regelt das Grundgesetz, also die Verfassung der Bundesrepublik Deutschland, in seiner Auslegung durch die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) auch den digitalen Raum – und zwar im Grundsatz überzeugend: Das BVerfG hat es in bemerkenswerter Weise verstanden, die Grundrechte »entwicklungsoffen« zu interpretieren, ihnen wohldosiert neue Schutzdimensionen zu entnehmen und so einen im Kern rund achtzig Jahre alten Text fit für das digitale Zeitalter zu machen. Diese Entwicklung setzt sich inzwischen auch auf europäischer Ebene fort, wo der Europäische Gerichtshof auch die noch junge Charta der Grundrechte der Europäischen Union zu einem Maßstab der Digitalpolitik weiterentwickelt.

Im folgenden Beitrag werden wir zunächst die Entwicklung der höchstrichterlichen Rechtsprechung zu Fragen der Digitalisierung nachzeichnen. Im Ausgangspunkt wird es dabei um die informationelle Selbstbestimmung gehen, aber die betroffenen grundrechtlichen Konfliktlinien weisen längst weit über den Datenschutz hinaus. So werden wir auch Fragen der Meinungsfreiheit und der Informationsfreiheit behandeln und schließlich einen Ausblick wagen, welche Rechtsfragen der Digitalisierung in den nächsten Jahren zur Entscheidung anstehen.

I. Die Wurzeln der datenschutzrechtlichen Verfassungsjudikatur

In den frühen 1980er Jahren beschloss die Bundesregierung, das Leben in der Bundesrepublik statistisch präziser als zuvor zu erfassen. Im Rahmen einer sogenannten Volkszählung sollten die demografischen, wirtschaftlichen und sozialen Strukturen der Bundesrepublik ergründet werden. Gegen dieses Vorhaben und insbesondere die Auswertung und Speicherung der Daten durch Computer regte sich massiver öffentlicher Protest, der schließlich auch in Verfassungsbeschwerden gegen die Rechtsgrundlage des Zensus mündete, das Volkszählungsgesetz. Zwei Wochen vor Beginn der Zählung, im April 1983, stoppte das Bundesverfassungsgericht das Vorhaben in einer Eilentscheidung. Mit seinem im Dezember 1983 ergangenen »Volkszählungsurteil« legte das BVerfG schließlich den Grundstein für seine innovative Rechtsprechung im deutschen Datenschutzrecht: Dem Grundgesetz entnahm es ein neues Grundrecht – das Grundrecht auf informationelle Selbstbestimmung.

1. Das Volkszählungsurteil und das Recht auf informationelle Selbstbestimmung

Die informationelle Selbstbestimmung gewährleistet »die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen«.[1] Es ist Ausdruck der Menschenwürde, dass jeder Mensch als frei denkendes und handelndes Individuum selbst entscheiden kann, welche persönlichen Daten er oder sie wem und wie überlässt.[2] Daneben leitete das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung auch aus dem Allgemeinen Persönlichkeitsrecht her, das sich wiederum aus dem im Grundgesetz verankerten Recht auf freie Persönlichkeitsentfaltung (Art. 2 Abs. 1 GG) und aus der Menschenwürdegarantie (Art. 1 Abs. 1 GG) ergibt.

Ausgangspunkt der Entscheidung war die Erkenntnis, dass die moderne automatisierte Datenverarbeitung eine unbegrenzte Speicher- und Abrufbarkeit von persönlichen Daten ermöglicht. Damit wird der Staat in die Lage versetzt, umfassende Persönlichkeitsbilder über einzelne Bürger*innen zu erstellen. Die damit einhergehenden Möglichkeiten, die eigene Bevölkerung genauestens zu kontrollieren, erkannte das BVerfG vorausschauend als große

1 BVerfGE 65, 1, 1. Leitsatz.

2 Vgl. BVerfGE 65, 1, 41f.

Gefahr für die tatsächliche Wahrnehmung von Freiheitsrechten – ein Phänomen, für das sich später die Bezeichnung *chilling effect* einbürgerte:

»Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung entsprechender Grundrechte (Art. 8, 9 GG) verzichten.«[3]

Das beeinträchtigt indes nicht nur die individuelle Freiheit, sondern die demokratische Kultur:

»Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.«[4]

Das Recht auf informationelle Selbstbestimmung entfaltet also eine doppelte Schutzwirkung: Zum einen schützt es Einzelne vor der ungewollten Preisgabe und Verarbeitung persönlicher Daten. Es ermächtigt Menschen im Grundsatz, frei über sie betreffende Daten zu verfügen. Bürger*innen sollen sich individuell und frei von psychischem Konformitätsdruck entfalten und von ihren grundgesetzlich verbrieften Freiheiten möglichst ungehemmt Gebrauch machen können.

Zum anderen aber schützt das Recht auf informationelle Selbstbestimmung damit die demokratische Kultur an sich, denn »Selbstbestimmung [ist die] elementare Funktion eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens«.[5] Das Recht auf informationelle Selbstbestimmung flankiert und erweitert so die grundrechtlich geschützte Verhaltensfreiheit und Privatheit, und zwar bereits auf der Ebene der bloßen Gefährdung.[6]

Das Urteil wirkte sich keineswegs nur auf die Volkszählung aus. Vielmehr entwickelte das Bundesverfassungsgericht an diesem Beispiel grundrechtli-

3 Ebd. Rn. 146.
4 Ebd. Rn. 146.
5 Ebd. Rn. 154
6 Vgl. BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 –, Rn. 198.

che Garantien, die die Erhebung und Verarbeitung personenbezogener Daten begrenzen und die bis heute nachwirken – nicht zuletzt in der Datenschutzgrundverordnung der Europäischen Union, die maßgeblich auf der Dogmatik der informationellen Selbstbestimmung beruht. Demnach gilt jede staatliche Datenerhebung und -verarbeitung als Eingriff in das Grundrecht, der einer Rechtfertigung bedarf – entweder durch Einwilligung der Betroffenen oder durch eine hinreichend bestimmte gesetzliche Grundlage. Insbesondere muss ein solches Gesetz den Verwendungszweck der Daten begrenzen und verfahrensrechtliche Schutzvorkehrungen wie Aufklärungs-, Auskunfts- und Löschungspflichten der verarbeitenden Stelle vorschreiben.[7] Darüber hinaus etablierte das Urteil die Grundsätze der Datensparsamkeit und Zweckbindung, also der Beschränkung der Datenerhebung auf das für den gewünschten Zweck tatsächlich notwendige Maß. Spätestens seit dem Volkszählungsurteil gibt es kein »belangloses Datum« mehr.[8]

Mit seiner Entscheidung erfand das BVerfG zwar nicht den Datenschutz – die Sorge vor der »Verdatung« durch elektronische Datenverarbeitung lässt sich bis in die späten 1960er Jahre zurückverfolgen. Indes sensibilisierte das Gericht schon lange vor der Existenz sozialer Medien und ausschweifender Überwachungsprogramme eine breite Öffentlichkeit für die demokratische Relevanz des Datenschutzes. Im Volkszählungsurteil wurzeln bis heute wichtige Prinzipien des deutschen und europäischen Datenschutzrechts, die nicht zuletzt die Datenschutz-Grundverordnung maßgeblich prägen.

2. Die Entstehung des »Computer-Grundrechts«

Im Jahr 2008 verhandelte das Bundesverfassungsgericht über Verfassungsbeschwerden gegen das Nordrhein-Westfälische Landesverfassungsschutzgesetz. Dieses Gesetz erlaubte die sogenannte Online-Durchsuchung. Darunter versteht man den heimlichen Zugriff auf informationstechnische Systeme wie Computer, Smartphones oder Laptops mittels Infiltration durch staatliche Überwachungssoftware – sogenannte (Staats-)Trojaner.

Angesichts der digitalen Durchdringung aller Lebensbereiche erkannte das BVerfG das Gefahrenpotenzial einer Ausforschung von IT-Systemen wie insbesondere Smartphones: Die stetig zunehmende Masse immer persönlicherer Daten, die Menschen ihren Geräten anvertrauen, lässt detailliertes-

7 Vgl. BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 – 1 BvR 209/83 –, Rn. 154.
8 Vgl. BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 – 1 BvR 209/83 –, Rn. 150.

te Rückschlüsse auf deren persönliche Interessen, Neigungen, soziale, wirtschaftliche und nicht zuletzt physische wie psychische Situation zu.[9] Gleichzeitig wächst die Bedeutung solcher Informationssysteme für die individuelle Persönlichkeitsentfaltung.[10] Der im Gesetz vorgesehene heimliche Zugriff auf solche Daten geht laut BVerfG »in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen […] weit hinaus«.[11] Den bisherigen Schutz vor solchen Zugriffen im Rahmen des Rechts auf informationelle Selbstbestimmung erachtete das BVerfG daher als nicht mehr ausreichend: Komplexe Datensammlungen, wie sie etwa in einem Handy enthalten sind, lassen sich als »ausgelagertes Gehirn« der Menschen beschreiben, die das jeweilige System nutzen. Greifen Dritte auf ein solches Gerät zu, so verschaffen sie sich einen potenziell enorm weitreichenden und aussagekräftigen Datenbestand, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein.[12] Um trotz eines so umfassenden Zugriffs noch Verhaltensfreiheit und Privatheit zu garantieren, war daher der Schutz vor ungewolltem Zugriff auf IT-Systeme wie Laptops oder Smartphones insgesamt nötig – und nicht nur in Bezug auf einzelne Daten, wie sie im Fokus der informationellen Selbstbestimmung stehen.[13]

Um der besonderen Gefährlichkeit des Zugriffs auf IT-Systeme auch rechtlich gerecht zu werden, leitete das BVerfG daher aus dem Grundgesetz das neue »Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme« her, das auch als IT-Grundrecht oder Computer-Grundrecht bezeichnet wird. Dieses hat zwei Schutzrichtungen: Unter dem Aspekt der *Vertraulichkeit* schützt es das Interesse der an einem System Berechtigten, dass die von einem informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben, dass also Dritte nicht Kenntnis nehmen können. Zum anderen schützt es unter dem Aspekt der *Integrität* die berechtigten Nutzer*innen eines Systems davor, dass im System gespeicherte Inhalte, Funktionen oder Leistungen durch Dritte genutzt und so ausgespäht, manipuliert oder überwacht werden können.[14]

---

9 Vgl. BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 –, Rn. 178.
10 Vgl. BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 –,Rn. 169ff.
11 BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 –, Rn. 200.
12 Vgl. Conrad, Isabell in: Auer-Reinsdorff/Conrad (Hg.), Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 34 Rn. 43.
13 Vgl. BVerfGE 120, 274, 313.
14 Vgl. BVerfGE 120, 274, 314.

Wie alle Grundrechte wirkt das Computer-Grundrecht jedoch nicht nur als Abwehrrecht gegen staatliche Eingriffe, in diesem Fall insbesondere durch Staatstrojaner. Vielmehr entfaltet es als Teil der Wertordnung des Grundgesetzes eine wesentlich breitere Wirkung:

Vor allem verpflichtet das Grundrecht den Gesetzgeber, die Rechtsordnung insgesamt so zu formen, dass Gefahren für die Integrität und Vertraulichkeit von IT-Systemen minimiert werden. Dieser Schutzpflicht kommt der Gesetzgeber indes bisher nur sehr eingeschränkt nach. So fehlt es an hinreichend wirksamen Anreizen – beispielsweise durch entsprechende Regelungen zur Produkthaftung –, um Hersteller von Hard- und Software zu motivieren, ihre Produkte so sicher wie eben möglich zu gestalten. Weist etwa eine verbreitete Software für E-Mail-Server eine Sicherheitslücke auf, durch die serienweise Unternehmensnetze infiltriert werden, dann verursacht das zwar bei den betroffenen Unternehmen schnell Schäden in Millionenhöhe, etwa für das »Reinigen« ihrer Infrastruktur. Für den Hersteller der schadhaften Software hat dies jedoch meist keine unmittelbaren finanziellen Folgen, vor allem weil in Allgemeinen Geschäftsbedingungen typischerweise jede Haftung für Programmierungsfehler ausgeschlossen wird. Insbesondere bei sehr verbreiteter Software sehen sich die Hersteller dann nicht veranlasst, solche Sicherheitslücken möglichst von vornherein zu vermeiden, da die hierfür notwendigen Investitionen – beispielsweise in unabhängige Sicherheits-Audits – sich bisher nicht lohnen. Müssten Software-Hersteller hingegen für die Folgen von Sicherheitslücken einstehen, so würde dies einen starken Anreiz bedeuten, mehr Wert auf Sicherheit zu legen.

Daneben entfaltet das IT-Grundrecht eine sogenannte mittelbare Drittwirkung auch in Rechtsverhältnissen zwischen Privaten. Das heißt, es verpflichtet etwa Arbeitgeber*innen zum Schutz der Daten von Arbeitnehmer*innen auf Firmenrechnern.[15]

II. Die europäische Strahlkraft des Bundesverfassungsgerichts

Neben den Garantien des Grundgesetzes stehen Rechte auf überstaatlicher Ebene, die den rechtlichen Diskurs zum Umgang mit der Digitalisierung prägen. Große Wirkung zeigen auch die Europäische Menschenrechtskonventi-

15 Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 34 Rn.46.

on (EMRK) und die EU-Grundrechtecharta (GRCh), die mit dem Inkrafttreten des Vertrages von Lissabon im Jahr 2009 geschaffen wurde.

1. Digitalisierung im Mehrebenensystem – Grundgesetz, Europäische Menschenrechtskonvention und Europäische Grundrechtecharta

Seit 1978 trifft der Europäische Gerichtshof für Menschenrechte (EGMR) wesentliche Leitentscheidungen für den Datenschutz.[16] Diese basieren vor allem auf Art. 8 der EMRK, die jedem Menschen den Schutz von Privatleben und Korrespondenz garantiert. Zwar gilt die EMRK in Deutschland nur im Rang eines einfachen Bundesgesetzes und hat keinen unmittelbaren Verfassungsrang.[17] Allerdings bettet das Grundgesetz die Bundesrepublik Deutschland in einen internationalen Verantwortungszusammenhang zur Wahrung der Menschenrechte.[18] Folgerichtig urteilte das BVerfG, dass die Entscheidungserwägungen des EGMR für deutsche Gerichte zu berücksichtigen und insofern bindend sind. Eine Abweichung von dessen Rechtsprechung muss besonders begründet werden.[19] Daher sind alle deutschen Gerichte angehalten, »solange im Rahmen geltender methodischer Standards Auslegungs- und Abwägungsspielräume eröffnet sind«[20], deutsches Recht im Einklang mit europäischem Recht auszulegen. Hierdurch entfalten die Entscheidungen des EGMR eine mittelbare Bindungswirkung. Daneben kann ein Urteil des EGMR, das eine Verletzung der Konvention feststellt, sogar die Rechtskraft einer bundesverfassungsrechtlichen Entscheidung durchbrechen und so zu dessen Revision führen.[21] So bildet auch die EMRK einen entscheidenden Maßstab für die Konkretisierung und Fortentwicklung der deutschen Grundrechte.[22]

Eine noch bedeutsamere Wirkung entfaltet die EMRK auf EU-Ebene. Denn die EU gab sich mit dem Inkrafttreten des Vertrages von Lissabon einen

16 Z.B. 1978 im Fall Klass u.a. gegen die Bundesrepublik Deutschland die durch Gesetzgeber und BVerfG bestimmten Schutzmaßnahmen, Kontrollen und Rechtsmittel bei geheimen Datenbearbeitungen bestätigt und ergänzt; Vgl. EGMR Urt. v. 6.9.1978, EuGRZ 1979, 278.

17 Herberth, Bethge in: Sachs (Hg.), GG-Kommentar, 8. Aufl., 2018, Art. 5 Rn. 6b.

18 Vgl. Art. 1 Abs. 2 GG.

19 BVerfGE 111, 307, 324.

20 BVerfGE 111, 307, 329.

21 Vgl. BVerfGE 128, 326, 36f.

22 Vgl. BVerfGE 74, 358, 370.

eigenen Grundrechtekatalog, die Europäische Grundrechtecharta (GRCh). Diese bindet alle Organe, Einrichtungen und sonstige Stellen der Union sowie Mitgliedstaaten, sobald sie Unionsrecht anwenden (Art. 51 Abs. 1 Satz 1 GRCh). Zudem gewährleistet die GRCh ein ausdifferenziertes europäisches Datenschutzgrundrecht (Art. 7, 8 GRCh).[23] Die EMRK verstärkt diesen unionsrechtlichen Datenschutz, indem sie einen Mindeststandard etabliert, der auch für die Anwendung der Unionsgrundrechte gilt (Art. 53 Abs. 3 Satz 1 GRCh).[24]

Die Rechtsprechung des BVerfG ist damit heute Teil eines Verfassungsverbundes, geprägt von nationalen Verfassungen, EMRK und Europäischer Grundrechtecharta. Die hieran von den jeweiligen Höchstgerichten entwickelten Maßstäbe bedingen und beeinflussen sich in einem judikativen Innovationsnetzwerk gegenseitig und garantieren so einen Mindeststandard. Einem datenschutzrechtlichen *race to the bottom*, also einer Entwicklung hin zu einem möglichst niedrigen Schutzniveau, wirkt die europäische Gerichtsstruktur so automatisch entgegen. Vielmehr entfalten die aufeinander bezogenen und jeweils für sich mit erheblichem Innovationspotenzial ausgestatteten Rechtsprechungen Synergieeffekte, die die Einhegung der Digitalisierung auf drei gerichtlichen Ebenen ermöglichen: durch mitgliedstaatliche Verfassungsgerichte, den EGMR und den Europäischen Gerichtshof (EuGH).

Die Rechtsprechung des BVerfG wird diesen Verfassungsverbund aber wohl auch in Zukunft erheblich beeinflussen. Denn die Europäische Grundrechtecharta (Art. 7, 8 GRCh) und die Europäische Menschenrechtskonvention (Art. 8 EMRK) knüpfen im Datenschutz an die Achtung des Privatlebens an, wohingegen das BVerfG die Datenhoheit als Voraussetzung zur individuellen Entfaltung sieht.[25] Hierdurch verlagert es den grundrechtlichen Datenschutz und damit die gerichtliche Kontrolle vor.

2. Der EuGH als Wächter der Europäischen Grundrechtecharta

Auch der EuGH war bisher vielfach mit datenschutzrechtlichen Fällen konfrontiert:

23 Vgl. Art. 8 Abs.1, Absatz 2 Satz 2, Absatz 3.
24 EuGH, Rechtssache C-528/15, Rn. 37.
25 BVerfGE 121, 1, 19.

a) Wächter im Inneren: Die Richtlinie zur Vorratsdatenspeicherung

2014 entschied der EuGH, dass die Richtlinie zur Vorratsdatenspeicherung von Verbindungsdaten (2006/24/EG) mit europäischem Recht nicht vereinbar ist. Die Richtlinie verlangte insbesondere von Telekommunikationsanbietern, anlasslos sämtliche Verbindungsdaten ihrer Kund*innen für sechs Monate bis zwei Jahre ab Zeitpunkt der Kommunikation zu speichern, vor allem Verkehrs- und Standortdaten.[26] In dieser Regelung sah der EuGH einen Eingriff »von großem Ausmaß« und von »besonders schwerwiegend[er]« Natur.[27] Dies stützte er auf vier Gesichtspunkte:

Erstens kritisierte der EuGH die personelle und kommunikationstechnische Streubreite der Normen, die sich »auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten […], ohne irgendeine Differenzierung« erstrecke sowie auf alle von ihr erfassten Daten, unabhängig davon, ob sie in irgendeinem Zusammenhang mit der öffentlichen Sicherheit stehen.[28] Zweitens enthalte die Richtlinie keine ausreichend konkreten, auf den Einzelfall bezogenen Kriterien und keine verfahrensrechtlichen Regelungen für den Zugang zu den Daten.[29] Drittens erfolge die Speicherung für mindestens sechs Monate unabhängig davon, ob die Daten tatsächlich so lange gebraucht würden.[30] Viertens würden keine ausreichenden Regelungen zur Sicherheit der gespeicherten Daten getroffen.[31]

Als besonders problematisch erachtete der EuGH die Möglichkeit, dass die Daten in Drittstaaten gespeichert werden, in denen das notwendige Schutzniveau nicht als gewährleistet angesehen werden könne[32] – ein deutlicher Verweis auf die bekannt gewordenen Enthüllungen Edward Snowdens und einen entsprechenden Datenaustausch zwischen der EU und US-Geheimdiensten. Kernthese war letztlich, dass sich eine derartige anlasslose Massenüberwachung auf das »absolut Notwendige« beschränken müsse.[33]

Das Urteil des EuGH war in mehrfacher Hinsicht revolutionär:

Inhaltlich übertrug der EuGH grundrechtliche Schutzpflichten auf den EU-Gesetzgeber. Diese Aufgabe hatte er bis dato den Mitgliedstaaten bei der

26 Vgl. Art. 5 RL 2006/24/EG.
27 EuGH, Rechtssachen C-293/12 und C-594/12, Rn. 37.
28 Ebd., Rn. 57ff., Zitat in Rn. 57.
29 Vgl. Ebd., Rn. 60ff.
30 Vgl. Ebd., Rn. 63ff.
31 Vgl. Ebd., Rn. 66ff.
32 Ebd., Rn. 68.
33 EuGH, Rechtssachen C-293/12 und C-594/12, Rn. 52.

Umsetzung der Richtlinien und damit den entsprechenden nationalen Verfassungsgerichten überlassen.[34] Infolgedessen spielt die Europäische Grundrechtecharta in der heutigen Gesetzgebungsarbeit von Kommission und Parlament eine größere Rolle. Methodisch arbeitete der EuGH wie ein selbstbewusstes nationales Verfassungsgericht. Mit der Grundrechtecharta mobilisierte er in klassisch verfassungsrechtlicher Art höherrangiges, dem einfachen Gesetzgeber nicht verfügbares »Verfassungsrecht« der EU gegen deren Sekundärrecht, also insbesondere gegen die auf Grundlage der EU-Verträge erlassenen Verordnungen und Richtlinien. Darüber hinaus gab er dem Gesetzgeber für eine rechtliche Neugestaltung konkrete legislative Instrumente vor.[35] So bekannte sich der Gerichtshof zu effektiver Grundrechtskontrolle.[36] Der EuGH bezog sich dabei erkennbar auf die Datenschutzrechtsprechung des BVerfG und des EGMR.[37]

b) Wächter nach außen: Das Privacy-Shield-Urteil 2020

Seit vielen Jahren findet ein transatlantischen Datenaustausch zwischen der EU und den USA statt – insbesondere durch US-Internetkonzerne wie Facebook und Co., aber auch durch die Datenverarbeitung zahlreicher deutscher Unternehmen, die ihre EDV zu großen Teilen in die »Cloud« verlagern, die oft durch US-Konzerne bereitgestellt wird. Bereits im eben angesprochenen Urteil zur Vorratsdatenspeicherung deutete der EuGH demgegenüber an, dass die Datenspeicherung europäischer Bürger*innen nur in Drittstaaten erfolgen könne, deren Datenschutzniveau dem europäischen entspreche.[38]

Rechtliche Grundlage dieses Datenaustausches war seit 2016 der sogenannte Privacy Shield, eine informelle Absprache zwischen der EU und den USA. Den Vorläufer »Safe Harbor« hatte der EuGH bereits 2015 für nichtig erklärt.

---

34 Vgl. Granger, Marie-Pierre/Irion, Kristina: https://www.ivir.nl/syscontent/pdfs/77.pdf vom 17.12.20, S. 24.

35 EuGH, Rechtssachen C-293/12 und C-594/12, Rn. 57-62.

36 Vgl. Classen, Clauss Dieter: »Datenschutz ja – aber wie?« in Europarecht 2014,. 441, 442.

37 Vgl. Ebd. EuR 2014, 441, 443. So decken sich die Entscheidungsgründe des EuGHs im Wesentlichen mit den Erwägungsgründen des BVerfG sowie jenen des EGMR zur Vorratsdatenspeicherung. Petri, Thomas, Urteilsanmerkung zu: »EuGH, Rechtssachen C-293/12 und C-594/12« in: Zeitschrift für Datenschutz 2014, 296, 300.

38 Vgl. EuGH, Rechtssachen C-293/12 und C-594/12, Rn. 68. Dies verlangt auch Art. 44 DS-GVO.

Konkret stellte der EuGH fest, dass das Abkommen kein vergleichbares Schutzniveau gewährleiste. Zum einen bemängelte der EuGH einen zu weitreichenden und weitgehend unkontrollierten Zugriff der US-Behörden auf die übermittelten Daten, da im Abkommen den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses und der Durchführung von Gesetzen der Vorrang gegenüber den Vorgaben zum Schutz der Betroffenen eingeräumt werde.[39] Konkret erlauben Section 702 des Foreign Intelligence Surveillance Act (FISA), eines US-Bundesgesetzes, sowie Executive Order 12333, ein Präsidialerlass aus der Amtszeit Ronald Reagans, den US-Geheimdiensten pauschale Überwachungsprogramme. Sie dürfen demnach auf sämtliche übermittelte Daten von Nicht-US-Bürger*innen zugreifen, die sich nicht in den USA aufhalten. Damit ist die komplette weltweite Datenverarbeitung in der »Cloud« dem Zugriff durch US-Geheimdienste ausgeliefert. Gleichzeitig ließen die Vorschriften in keiner Weise erkennen, dass für die darin enthaltene Ermächtigung zur Durchführung dieser Programme Einschränkungen bestehen.[40] Zum anderen kritisierte der EuGH, dass hinreichende Rechtsschutzmöglichkeiten zur Rüge und Verfolgung von Verstößen auch und gerade gegen die Vorgaben zum Grundrechtsschutz fehlen.[41]

Damit erweitert der EuGH die Rechtsschutzmöglichkeiten erheblich: Mit den Anforderungen an vertragliche Standardklauseln ordnet er wirtschaftliche Interessen klar datenschutzrechtlichen Bedenken unter und führt so seine Rolle als Wächter der Datenschutzgrundrechte in der Union fort.[42] Bemerkenswert ist auch, dass der EuGH den Privacy Shield im Urteil aufhebt, obwohl dies nicht zwingend entscheidungserheblich war.[43]

Der wohl wichtigste Aspekt dürfte aber sein, dass der EuGH zwar vordergründig nur Anforderungen an Unternehmen und Einzelpersonen in der EU definiert, damit der Sache nach aber auch über das Recht von Drittstaaten und dessen Vereinbarkeit mit europäischen Grundrechten urteilt. Hierdurch hebt der Gerichtshof den europäischen Datenschutzstandard faktisch auf eine internationale Ebene und macht ihn für alle Länder verbindlich, in die Daten aus der EU transferiert werden sollen. Mittelbar entfalten dadurch europäische Mindeststandards weltweite Wirkung. Daher ist zu erwarten,

39 Vgl. EuGH, Rechtssache C-362/14, Rn. 86ff.
40 EuGH, Rechtssache C-362/14, Rn 180ff.
41 EuGH, Rechtssache C-362/14, Rn. 89ff.
42 Vgl. verfassungsblog.de/a-groundhog-day-in-bruessels/ vom 17.12.2020.
43 Vgl. *Øe*, Schlussanträge v. 19.12.2019 – EUGH Rechtssache C-311/18, Rn. 161ff.

dass dies auch die rechtspolitische Debatte in anderen Rechtsräumen beeinflusst. Denn beispielsweise US-amerikanischen Wähler*innen dürfte kaum zu vermitteln sein, warum einheimische IT-Unternehmen die Daten von US-Bürger*innen weniger schützen müssen als jene der EU-Bürger*innen. Der öffentliche Diskurs über Datenschutz und den richtigen Umgang mit Digitalisierung wird so ein transnationaler.

Auch die Rechtssetzung durch die EU greift diese Tendenz in der Rechtsprechung des EuGH bereits auf: Kommission, Rat und insbesondere das Europäische Parlament werden den bewussten Export von grundrechtlichen Anforderungen absehbar fortsetzen und damit nicht nur EU-weit, sondern global den Rechtsrahmen für die Digitalisierung prägen. Die internationale Strahlkraft der europäischen Gesetzgebung wird sich beispielsweise auch auf Fragen der Regulierung großer Internetplattformen ausdehnen. Mit den anstehenden Gesetzesvorhaben des Digital Markets Act (DMA) und Digital Services Act (DSA) stehen bereits zwei Großprojekte in den Startlöchern, die ausdrücklich das Ziel verfolgen, einen verbindlichen Rechtsrahmen für alle Dienste zu setzen, die sich (auch) an Menschen in der Europäischen Union richten – also de facto so gut wie alle Internet-Dienste.

III. Aktuelle Herausforderungen der Gerichte und Ausblick

Auch 2020 trafen BVerfG und EuGH wegweisende Urteile.

1. Überwachung durch Geheimdienste – das BND-Urteil des BVerfG

Auch das im Mai 2020 ergangene BND-Urteil des BVerfG entfaltet internationale Wirkung. Auf Initiative der Gesellschaft für Freiheitsrechte e.V. (GFF) hatte ein Bündnis mehrerer Organisationen[44] gegen die 2016 verabschiedete Novelle des BND-Gesetzes Verfassungsbeschwerde erhoben. Das BND-Gesetz ermächtigte in der Fassung von 2016 den BND zur sogenannten strategischen Ausland-Ausland-Fernmeldeaufklärung. Darunter versteht man das anlasslose und massenweise Mitschneiden von Telekommunikationsverbindungen, beispielsweise via Glasfaserkabel oder Satellitenleitungen,

44 Neben der Gesellschaft für Freiheitsrechte waren dies der Deutsche Journalisten-Verband, die Deutsche Journalistinnen- und Journalisten-Union in ver.di, n-ost, das Netzwerk Recherche und Reporter ohne Grenzen.

und die Durchsuchung der so abgefischten Datenberge mittels sogenannter Selektoren. Der Geheimdienst nutzt Suchbegriffe, die angeblich auf Inhalte hinweisen, die für die Tätigkeit des Dienstes von Bedeutung sind. Für diese strategische Überwachung musste nach dem Gesetz weder ein konkreter Verdacht (daher führt die Bezeichnung »strategisch« in die Irre) noch eine richterliche Genehmigung vorliegen. Die BND-Überwachung konnte damit praktisch jede Person treffen.

Das BVerfG erklärte weite Teile des Gesetzes wegen Verstoßes gegen das grundrechtlich geschützte Fernmeldegeheimnis (Art. 10 Abs. 1 GG) und gegen die Pressefreiheit (Art. 5 Abs. 1 Satz 2 GG) für verfassungswidrig. Zentrale Aussage und Errungenschaft des Urteils ist die unmissverständliche Klarstellung des BVerfG, dass Grundrechte auch für im Ausland lebende Menschen gelten und – jedenfalls soweit sie nicht explizit ausgenommen sind – auch für Ausländer*innen.[45] Weiterhin entschied das BVerfG, dass das grundgesetzliche Fernmeldegeheimnis auch Menschen schützt, die im Ausland für ausländische Personen tätig sind.[46]

Bemerkenswert umfangreich und detailliert gibt das BVerfG dem Bundesgesetzgeber Maßstäbe für eine Neuregelung des BND-Gesetzes mit. So fordert es Einschränkungen des Datenvolumens, die Sicherstellung der geografischen Begrenzung der Datensammlung[47], Regeln zur Aussortierung von Inlands- beziehungsweise Inlands-Auslandskommunikation[48], die Festschreibung konkreter und prüfbarer Überwachungszwecke[49] sowie den Schutz vertraulicher Beziehungen, beispielsweise zwischen Medien und ihren Quellen, durch eine gerichtsähnliche Ex-ante-Kontrolle.[50]

Weiterhin stellt das BVerfG klar, dass Daten nur unter hohen Auflagen an ausländische Stellen übermittelt werden dürfen. Voraussetzung ist eine Vergewisserung über deren rechtsstaatlichen Umgang mit den Daten.[51] Der BND muss sicherstellen, dass seine Informationen nicht genutzt werden, um gegen grundlegende Menschenrechte oder Völkerrecht zu verstoßen.[52] Eine automatisierte Datenweitergabe ist damit in der bisherigen Form nicht

45 BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 – 1 BvR 2835/17 –, 1. Leitsatz; Rn.94.
46 Ebd., 3. Leitsatz.
47 Ebd., Rn. 169.
48 Ebd., Rn. 170f.
49 Ebd., Rn. 175.
50 Ebd., Rn. 193f.
51 Ebd., Rn. 233ff.
52 Vgl. Ebd., Rn. 238.

mehr zulässig. Weiterer zentraler Aspekt der Entscheidung ist die umfangreiche[53] Forderung des BVerfG nach einer deutlich effektiveren Kontrolle des BND. Diese muss sich aus einer Art unabhängigem Geheimgericht und einer zusätzlichen unabhängigen Rechtskontrolle administrativen Charakters zusammensetzen.

Das BVerfG reagiert mit seinem Urteil auf das inhärente Potenzial, dass Auslandsnachrichtendienste innerstaatliche Bindungen zu umgehen versuchen.[54] Beeindruckend ist die Wirkung des Urteils: An die Stelle anlassloser weltweiter Überwachung tritt die weltweite Bindung der deutschen Staatsgewalt an Grund- und Menschenrechte. Damit setzt das Urteil neue Standards im internationalen Menschenrechtsschutz und für die Pressefreiheit. All diese Entscheidungen hätte das BVerfG nicht treffen müssen, da das Gesetz schon formell verfassungswidrig war. Es erklärte weiterhin, dass es nur »zentrale Defizite«[55] des Gesetzes festgestellt hätte, behält sich also weitere strenge Kontrollen vor. Die Entscheidung dürfte Vorbildcharakter für künftige Verfahren des EGMR haben.[56]

Das Verfahren legt so nicht nur den Grundstein für die Entwicklung einer umfassenden Nachrichtendienstkontrolle in Deutschland, sondern setzt auch einen Akzent für eine progressive, menschenrechtsfreundliche internationale Entwicklung in Richtung auf eine Verrechtlichung der Geheimdienstarbeit. Mittelfristig dürfte dies der Willkür im Geheimen arbeitender Behörden immer engere Grenzen setzen und so zugleich menschenrechtliche Standards stärken.

2. Predictive Policing – die Fluggastdatenrichtlinie vor dem EuGH

Derzeit liegt dem EuGH die Frage zur Entscheidung vor, ob die europäische Fluggastdatenrichtlinie 2016/681 mit der Grundrechtecharta vereinbar ist. Die 2016 erlassene Richtlinie verpflichtet Luftfahrtunternehmen, bei jedem Drittstaatenflug (außereuropäisch) sogenannte PNR (Passenger Name Records, Passagier-Namens-Datensätze) aller Fluggäste an die PNR-Zentralstellen der Mitgliedstaaten zu übermitteln, bei denen diese Daten automatisiert verarbeitet und dauerhaft gespeichert werden. Einen bestimmten Anlass braucht

53 Vgl. Ebd., Rn. 272ff.
54 Vgl. Ebd., Rn. 250
55 Ebd., Rn. 301
56 Vgl. Huber, Bertold: »Das BVerfG und die Auslands-Auslands-Fernmeldeaufklärung des BND« in: NvWZ-Beilage 2020, 3, 9.

es hierzu nicht. Die zu übermittelnden Datensätze umfassen neben den Namen und Adressen der Fluggäste und dem gesamten Reiseverlauf auch Angaben über ihr Gepäck, ihre Mitreisenden, alle Arten von Zahlungsinformationen sowie nicht näher definierte »allgemeine Hinweise« (ein Freitextfeld, das von der Fluggesellschaft auszufüllen ist). Die so erhobenen Daten werden sechs Monate personenbezogen und danach weitere 54 Monate pseudonymisiert gespeichert. Zusätzlich ermöglicht die Richtlinie über Umwege[57], diese Fluggastdaten an Drittstaaten für nahezu jeglichen Zweck zu übermitteln: zur Abwehr von irgendwelchen nicht näher bestimmten Gefahren, zur Geltendmachung irgendwelcher Rechtsansprüche und so weiter.

Die Verabschiedung dieser Richtlinie erscheint aus mehreren Gründen unverständlich. So bescheinigte ein EuGH-Gutachten bereits dem zum PNR-Abkommen zwischen der EU und Kanada die Grundrechtswidrigkeit. Grund hierfür waren das ebenfalls im Abkommen vorgesehene Freitextfeld,[58] der fehlende Schutz vor Weitergabe der PNR-Daten durch kanadische Behörden an Drittstaaten[59] und die vorgesehene fünfjährige Speicherdauer[60] – allesamt Bestimmungen, die die neue Richtlinie ungeachtet der klaren Vorgaben des EuGH wieder enthält.

Das deutsche Umsetzungsgesetz der Richtlinie, das Fluggastdatengesetz, geht nichtsdestotrotz sogar über die EU-Richtlinie hinaus. Es erfasst nicht nur Drittlandflüge, sondern auch unionsinterne. Darüber hinaus soll das Bundeskriminalamt die PNR-Daten mittels automatisierter Mustererkennung mit Polizeidatenbanken abgleichen und so verdächtige Flugbewegungen erkennen. Hier werden also erste Formen algorithmischer Verdachtsgewinnung, des sogenannten Predictive Policing, eingeführt. Diese Technik, bei der mit vorab festgelegten Kriterien Daten abgeglichen werden, soll die Gefährlichkeit von Menschen anhand von alltäglichen Daten beurteilen, die keinen Bezug zu einer konkreten Straftat haben. Die davon betroffenen Menschen werden allein durch algorithmische Berechnungen als

57 Vgl. Art. 11 Abs. 1 lit. a) Detaillierte Erläuterung: VG Wiesbaden, Beschluss vom 13.5.2020 – 6 K 805/19.WI, Rn. 96-98.

58 EuGH, Gutachten vom 26.7.2017 – Gutachten (Avis) 1/15, Rn. 160.

59 Ebd., Rn. 215.

60 Ebd., Rn. 206.

potenzielle Gefahrenquelle behandelt. Dies widerspricht grundlegend dem in der Europäischen Grundrechtecharta formulierten Menschenbild.[61]

Insgesamt sind die PNR-Richtlinie und deren deutsches Umsetzungsgesetz ein legislativer Frontalangriff auf die Grundrechte aller Unionsbürger*innen und auf die bisherige EuGH-Rechtsprechung. Es ist daher damit zu rechnen, dass der EuGH die Richtlinie für nichtig erklären wird, so wie er bereits das Abkommen mit Kanada kippte. Ein von der GFF initiiertes Verfahren gegen die Speicherung von PNR in Deutschland wurde bereits dem EuGH zur Vorabentscheidung vorgelegt. Besondere Aufmerksamkeit verdient nun, welche Ausführungen der EuGH zur algorithmischen Verdachtsgewinnung machen wird.

3. EUGH zu Uploadfilter

Auf eine Nichtigkeitsklage Polens gegen Bestimmungen der Urheberrechtsrichtlinie hin verhandelt der EuGH derzeit spannende Fragen im Konfliktfeld von Meinungs- und Informationsfreiheit einerseits und dem Schutz des geistigen Eigentums andererseits. Kern des Rechtsstreits sind dabei Verfahren zur technischen Filterung von Inhalten. Beispielsweise durch sogenannte Uploadfilter, die vermeintlich rechtswidrige hochgeladene Inhalte gar nicht erst online stellen, und die Frage, ob Überwachungspflichten für Betreiber von Online-Plattformen entstehen.

Der Europäische Gerichtshof (EuGH) prüft insbesondere die Vereinbarkeit einiger Bestimmungen des Artikels 17 der Urheberrechtsrichtlinie mit der EU-Grundrechtecharta.[62] Die polnische Regierung rügt, dass die angefochtenen Bestimmungen den Einsatz von Uploadfiltern vorschreiben. Dies verstoße gegen das in Art. 11 der EU-Grundrechtecharta verankerte Recht auf Meinungs- und Informationsfreiheit.

Der Prüfungsmaßstab des Gerichtshofs ist jedoch nicht auf die Prüfung der explizit gerügten Grundrechtverletzte beschränkt.[63] Es ist vielmehr damit

61 Vgl. http://freiheitsrechte.org/home/wp-content/uploads/2020/09/GFF-Stellungnahme-an-den-EuGH-zur-FluggastdatenspeicherungPNR-Richtlinie-2020.pdf vom 17.12.2020, S. 2.

62 Fall C-401/19 – Republik Polen v Europäisches Parlament und Rat der Europäischen Union.

63 Vgl. Reda, Julia/Selinger, Joschka/Servatius, Michael: Article 17 of the Directive on Copyright in the Digital Single Market: a Fundamental Rights Assessment. Kapi-

zu rechnen, dass der Gerichtshof eine umfassende Abwägung aller betroffenen Grundrechte mit dem Recht auf geistiges Eigentum (Art. 17 Abs. 2 GRCh) vornehmen wird. In der mündlichen Verhandlung zu dem Verfahren im November 2020 hat der Gerichtshof insbesondere die Frage aufgeworfen, ob Artikel 17 zur Einführung allgemeiner Überwachungspflichten führt.[64] Solche Überwachungspflichten sind nach der Rechtsprechung des Gerichtshofs unzulässig, da sie neben dem Recht auf Meinungs- und Informationsfreiheit (Art. 11 GRCh) auch den Schutz personenbezogener Daten der Nutzer*innen (Art. 7 GRCh) sowie die unternehmerische Freiheit der Plattformunternehmen (Art. 16 GRCh) verletzen.

Der EuGH stellte in der mündlichen Verhandlung zudem darauf ab, ob der Europäische Gesetzgeber ausreichende verfahrensrechtliche Schutzvorkehrungen für den Eingriff in die Grundrechte in Artikel 17 vorgesehen hat. So enthält Artikel 17 die abstrakte Vorgabe, dass legale Inhalte nicht beeinträchtigt werden. Die EU-Institutionen argumentieren, diese Vorschrift stelle sicher, dass nur offensichtlich rechtswidrige Inhalte gesperrt werden. Tatsächlich gibt Artikel 17 aber keine Anhaltspunkte, wie die automatische Sperrung legaler Inhalte in der Praxis verhindert werden soll. Es ist also durchaus plausibel anzunehmen, dass die Regelung an der Unbestimmtheit ihrer grundrechtlichen Schutzvorkehrungen scheitern könnte.[65]

IV. Chancen und Grenzen des Rechts – warum Gerichte digitale Zukunft mitgestalten (müssen)

Wie die genannten Beispiele zeigen, sind Gerichte ein machtvolles Instrument, um Grundrechtsverletzungen im digitalen Raum effektiv zu begegnen, die insbesondere durch staatliche Massenüberwachung und das ungeregelte Sammeln von Daten entstehen. In der EU bieten dabei drei Ebenen rechtlichen Schutz: der EGMR auf völkerrechtlicher, der EuGH auf europarechtlicher und die Verfassungsgerichte auf nationaler Ebene. Diese Gerichte ha-

---

tel 2. https://freiheitsrechte.org/home/wp-content/uploads/2020/11/GFF_Article17_Fundamental_Rights.pdf

64 Vgl. Reda, Julia: In zwei Stunden von Luxemburg nach Brüssel spazieren: Der Europäische Gerichtshof wird über die Legalität von Uploadfiltern urteilen. Verfassungsblog. https://verfassungsblog.de/in-zwei-stunden-von-luxemburg-nach-brussel-spazieren/

65 Husovec, Martin: Over-Blocking: When is the EU Legislator Responsible? 2021 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3784149

ben sich als innovative und im Grundsatz auch willige Verteidiger der Freiheitsrechte erwiesen, die in ihrer Rechtsprechung nicht nur aktuelle Gefahren einhegen, sondern auch vorausschauend Maßstäbe zur Unterbindung künftiger Grundrechtsverletzungen setzen und Rechtsschutzmöglichkeiten stärken. Dabei sind sie auch durchaus bereit, über den eigentlichen Fall hinaus Grundsatzfragen zu entscheiden – wie etwa das BVerfG im BND-Urteil oder der EuGH beim Privacy Shield. Die Gerichte greifen dabei wechselseitig auf die grundrechtlichen Erkenntnisse anderer Gerichte zurück und können daher die Gestaltung der Digitalisierung in grundrechtfreundlichere Richtungen weisen als es die Legislative mitunter vermag.

Zweifellos setzen Obergerichte dem Gesetzgeber und damit letztlich auch der Exekutive langfristig Grenzen. So heikel die mitunter drastischen Korrekturen gegenüber der Legislative aus einer demokratietheoretischen Perspektive sein mögen – der Fehler ist nicht in der Rechtsprechung zu suchen. Im Gegenteil, die systematische Unterbelichtung individueller Freiheiten seitens der Legislative im Namen strukturell nicht einzulösender Sicherheitsversprechen, zwingt die Judikative oft genug in eine aktivere Rolle, die sie dann wiederum konservativer Kritik aussetzt. In Wahrheit sind Gerichte in solchen Verfahren jedoch nur Lackmustest und zugleich Therapie legislativer Fehlsteuerungen, aber keineswegs selbst kritikwürdige Akteure oder gar *judicial activists*.

Dabei erstreckt sich der gerichtliche Schutz immer häufiger über das Unions- beziehungsweise Bundesgebiet hinaus. Insbesondere in dieser transnationalen Dimension europäischer Rechtsprechung liegt ein Potenzial, die Digitalisierung fair und grundrechtsfreundlich zu gestalten. Gesellschaftliche Debatten um Datenschutz können so von europäischen Gerichten ausgehend insbesondere in die USA getragen werden und beeinflussen damit zentrale Diskurse des 21. Jahrhunderts. Wenn sie Eingang in die Rechtsprechung des EGMR finden, gelten sie weit über die Grenzen der europäischen Union hinaus auch etwa in Russland, Georgien, Armenien, Aserbaidschan und anderen Ländern.

Die Gerichte können so einen wichtigen Beitrag dazu leisten, Freiheitsrechte in der digitalen Welt zu sichern und auszubauen. Hierfür müssen sie aber mit akribisch vorbereiteten strategischen Klagen mobilisiert werden. Dieser für die effektive Geltung von Grund- und Menschenrechten elementaren Aufgabe haben sich spezialisierte Nichtregierungsorganisationen unter dem Stichwort der strategischen Prozessführung verschrieben.

Gleichzeitig bleiben zentrale Fragen der rechtlichen Regelung der Digitalisierung bisher ungelöst und stellen sowohl die Legislative als auch die Rechtsprechung vor große Herausforderungen. So wird die Einwilligung, unter anderem bekannt als allgegenwärtige *Cookie-Banner*, als in der Theorie optimaler Ausdruck informationeller Selbstbestimmung zunehmend zur Fiktion: Viele Dienste, auf die die Menschen in der digitalen Gesellschaft nur unter großen sozialen oder beruflichen Kosten verzichten können, lassen sich Blankoschecks zum Umgang mit personenbezogenen Daten ausstellen – weil sie es können, und weil Einzelne jedenfalls subjektiv keine andere Wahl haben als zuzustimmen. Hier werden Gesetzgeber und Gerichte bestimmten »Einwilligungen« die rechtliche Anerkennung versagen müssen, so wie sich vor Jahrzehnten eine Rechtsprechung zur Inhaltskontrolle von Allgemeinen Geschäftsbedingungen (AGB) herausgebildet hat, die besonders krasse Klauseln im Kleingedruckten für unwirksam hält. Diese Regeln wiederum hat der Gesetzgeber schließlich erweitert, systematisiert und ins Bürgerliche Gesetzbuch übernommen. Eine ähnliche Form der »AGB-Kontrolle« wird auch im Bereich der Einwilligungen in die Datenverarbeitung erforderlich sein.

Strukturell ähnliche Probleme zeigen sich im Bereich der IT-Sicherheit, wo Einzelne meist nicht über die Marktmacht verfügen, mehr Investitionen von IT-Unternehmen in *security by default* (höchsten Sicherheitseinstellungen ab Werk) zu erzwingen. Gerichte und Gesetzgeber hingegen können die richtigen Anreize setzen, damit sich Investitionen in Sicherheit für Hersteller von Hard- und Software wirklich lohnen, indem sie Ansprüche auf Schadensersatz im Falle von Sicherheitsvorfällen deutlich erweitern. Und dies sind nur zwei der besonders heiklen Problemfelder.

Es ist nicht selbstverständlich, dass das Grundgesetz sowie die Grundrechtsquellen auf europäischer Ebene tatsächlich die Gefahren der Digitalisierung einhegen können. Wenn dies aber gelingt, so haben wir dies engagierten und innovativen Jurist*innen zu verdanken – bei den europäischen Gerichten, aber auch bei den Organisationen, die den Gerichten möglichst gut aufbereitete Rechtsfragen zur Entscheidung vorlegen.

3.4 Vielfalt

Gestalten statt reagieren – Was wir von der Zivilgesellschaft für eine gelungene Digitalisierung lernen können

Julia Kloiber und Elisa Lindinger

Zivilgesellschaftliche Organisationen setzen sich seit Jahrzehnten für eine gemeinwohlorientierte Digitalisierung ein. Für sie ist Digitalisierung kein Mittel zum Zweck, sondern ein Werkzeug, mit dessen Hilfe wir auf eine soziale, gerechte und nachhaltige Digitalisierung und Gesellschaft hinarbeiten können. Während Technologiekonzerne heute den digitalen Fortschritt dominieren und die Politik in erster Linie versucht, sie reaktiv zu reglementieren, entwickelt die Zivilgesellschaft einen Gegenentwurf: Dieser sieht vor, digitale Technologien dem Gemeinwohl zu unterstellen. Dafür gestaltet sie Werkzeuge und erprobt neue Möglichkeiten der Zusammenarbeit und der Verbreitung von Wissen. Zivilgesellschaftliche Organisationen setzen sich für ein freies und offenes Internet und eine gerechte Digitalisierung ein, von denen möglichst viele profitieren. Dabei vertreten sie auch die Interessen von marginalisierten Gruppen und denjenigen, die von neuen Entwicklungen oft ausgeschlossen oder von negativen Auswirkungen betroffen sind.

In diesem Beitrag zeigen wir auf, wie zivilgesellschaftliche Organisationen Digitalisierung mitgestalten, welche Visionen sie antreiben und was Politik und Wirtschaft von ihnen lernen können, damit der digitale Wandel möglichst gemeinwohlorientiert gelingt und der digitale Fortschritt der gesamten Gesellschaft zugutekommt.

1 Die historischen Leitideen der Digitalisierung

Schneller, billiger, effizienter: Das sind Begriffe, die wir mit der Digitalisierung und Computern verbinden. Computer sind ein Mittel, um Prozesse effizienter zu machen, Geschäfte schneller zu erledigen und Transaktionskosten zu senken. Wie wir über die Gestaltung der Digitalisierung denken, ist stark geprägt von den Idealen des öffentlichen Dienstes des 19. Jahrhunderts.[1]

In seinem Buch *The Government Machine* zeigt der Technikhistoriker Jon Agar,[2] dass der Computer letztlich das Produkt einer technokratischen Vision des Regierens ist, die sich ab dem späten 18. Jahrhundert in dem Versuch entwickelte, eine sich schnell verändernde Welt zu verwalten, indem sie so viele statistische und andere Informationen wie möglich sammelte. Der deutsch-US-amerikanische Informatiker, Wissenschafts- und Gesellschaftskritiker Joseph Weizenbaum[3] sprach davon, dass der Computer von Beginn an »eine fundamental konservative Kraft« gewesen sei. Der Computer »hat die Rettung von Institutionen möglich gemacht, die andernfalls hätten verändert werden müssen«[4]. Als ein Beispiel nennt er das Bankenwesen in den USA, das in der Mitte des letzten Jahrhunderts aufgrund des schnellen Bevölkerungswachstums immer mehr Schecks verarbeiten musste. Für die Banken kam der Computer genau zur richtigen Zeit. Anstatt das bestehende System mit nicht-technischen Mitteln, beispielsweise sozialen Erfindungen, zu reformieren, wurde es mithilfe des Computers automatisiert. Der Computer festigte so, laut Weizenbaum, die Macht der alten Systeme. Dem Soziologen Armin Nassehi zufolge ist die Digitalisierung aus der Gesellschaft heraus entstanden und nicht als etwas Neues oder Fremdes hinzugekommen. »Wenn sie nicht zu dieser Gesellschaft passen würde, wäre sie nie entstanden oder längst wieder verschwunden.«[5]

Dem gegenüber beschreibt Weizenbaum, wie digitale Werkzeuge die Lösungen determinieren, zu deren Zweck sie eingesetzt werden: »Der Compu-

1 Vgl. https ://dingdingding.org/issue-2/what-the-enlightenment-got-wrong-about-computers/

2 Agar, Jon: The Government Machine. A Revolutionary History of the Computer, MIT Press, 2003

3 Nach dem auch das erste öffentlich finanzierte »Internet-Institut« benannt wurde https://weizenbaum-institut.de/

4 http://tech.mit.edu/V105/N16/weisen.16n.html

5 Nassehi, Armin: Muster. Theorie der digitalen Gesellschaft, C.H. BECK, 2019, S. 8.

ter war von Anfang an eine Lösung auf der Suche nach einem Problem.«[6] Er wurde entwickelt, um eine sich schnell verändernde Welt zu managen. Anstatt Probleme an der Wurzel zu packen, sie in ihrer Komplexität zu durchdringen und ganzheitliche Lösungen zu erarbeiten, wird vorschnell zu technischen Lösungen gegriffen. Ein aktuelles Beispiel dafür ist die Blockchain-Technologie, die auf unzählige Bereiche projiziert wird, von »Banking the Unbanked«, also dem Versuch, Menschen ohne Bankkonto den Zugang zum digitalen Zahlungsverkehr zu ermöglichen,[7] bis hin zu Aufforstungsprojekten[8] Hinter dieser Art zu denken steckt ein Phänomen, das als *Solutionismus* bezeichnet wird. Dabei werden alle Probleme so definiert, als ließen sie sich mit technischen Mitteln lösen.[9]

Der Computerpionier Douglas Engelbart verknüpft seine Kritik mit einer Aufforderung. Er spricht davon, wie die Menschheit zwar enorme technologische Fortschritte gemacht hat. Wie wir in der Lage sind, Wettervorhersagen zu berechnen, den genetischen Code zu knacken, kurz: Probleme zu lösen, die wir ohne die Rechenpower so nicht aufklären könnten. Doch trotz all dieser ganzen Errungenschaften haben wir laut Engelbart das wahre Potenzial von Computern noch nicht gehoben. Denn um komplexe Herausforderungen wie beispielsweise die Bekämpfung von Armut oder die Klimakrise zu bewältigen, braucht es mehr als Daten und Rechenpower. Es braucht Menschen, die zusammenarbeiten und ihre individuellen Problemlösungskompetenzen in Prozesse einbringen können. Engelbarts Meinung nach sollen uns Computer neue Wege der Kollaboration eröffnen. Sie sollen unsere Vorstellungskraft anfachen und uns dabei helfen, unsere Kreativität voll auszuschöpfen. Das Internet und die damit verbundene Technologie bilden dafür eine gute Grundlage.[10] Gleichzeitig entfernen wir uns immer weiter von den frühen Idealen des Internets, in dem jeder Nutzer und jede Nutzerin mitgestalten und entwerfen konnte. Die digitale Infrastruktur wird heute faktisch von großen Plattformbetreibern dominiert, deren Geschäftsmodelle auf der

6 http://tech.mit.edu/V105/N16/weisen.16n.html

7 Vgl. https ://www.forbes.com/sites/yayafanusie/2021/01/01/stop-saying-you-want-to-bank-the-unbanked/

8 Vgl. https ://www.vice.com/de/article/7xjpkg/blockchain-probleme-die-schon-geloest-sind-bitcoin

9 Vgl. Morozov, Evgeny: To Save Everything, Click Here: The Folly of Technological Solutionism New York: PublicAffairs 2013.

10 Vgl. https ://www.dougengelbart.org/content/view/348/

Sammlung und der Vermarktung von Nutzer*innendaten basieren.[11] Mit der wachsenden Macht der globalen Konzerne wird es immer schwieriger, sich der Plattformisierung zu entziehen und Alternativen zu bestehenden Systemen zu denken oder gar zu entwickeln.

2 Digitale Technologien im Spannungsfeld von Wirtschaft und Gesellschaft

Digitale Technologien und später auch das Internet waren zunächst Herrschaftstechnologien: Sie standen nur wenigen Menschen zur Verfügung, hatten ihrerseits aber teils fatale Auswirkungen auf die gesamte Gesellschaft. Deutlich wird das am Beispiel von Lochkarten, also frühen Datenträgern, die ab 1890 bei Volkszählungen weltweit zum Einsatz kamen und die oben beschriebene Leitidee der Effizienz repräsentierten. Die Folgen dieser frühen Digitalisierungswelle und der Verdatung von Menschen waren weitreichend: In seinem Buch *IBM and the Holocaust* zeigt der US-amerikanische Journalist Edwin Black,[12] dass die umfassende Datensammlung den Holocaust massiv beschleunigte, da Juden beziehungsweise Jüdinnen und Menschen jüdischer Herkunft über automatisierte Suchen in den Zensusdaten leicht identifizierbar waren. Die Politikwissenschaftlerin Virginia Eubanks liefert weitere Beispiele für Digitalisierung als Herrschaftstechnologie. Sie nimmt die Rolle von Computersystemen und Daten im US-amerikanischen Sozialwesen unter die Lupe nimmt und beschreibt, wie schon kleine Versäumnisse oder Fehler seitens der Verwaltung dazu führen, dass Menschen ihnen zustehende soziale Leistungen verwehrt bleiben und sie kaum eine Möglichkeit haben, die Situation zu ändern.[13]

Jahrzehnte nach diesen frühen digitalen Technologien entstanden die Vorläufer des heutigen Internets. Dieses hat seine Wurzeln im ARPANET, einem 1961 gestarteten Netzwerk von Rechenanlagen US-amerikanischer Militär- und Forschungseinrichtungen, die wertvolle Rechenressourcen und Wissen miteinander teilen, sich durch Dezentralität gegen feindliche

11 Siehe hierzu auch den Beitrag von Christian Stöcker in diesem Band.

12 Black, Edwin: IBM and the Holocaust. Expanded Edition, Dialog Press, 2012.

13 Vgl. Eubanks, Virginia: Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor, New York: St Martin's Press, 2017.

Angriffen absichern wollten und deshalb ihre Großrechner vernetzten.[14] Der Zugang zum frühen Internet – bis in die 1980er Jahre hinein – war deshalb vor allem wenigen militärischen und wissenschaftlichen Einrichtungen vorbehalten, und damit auch die Möglichkeit, diese neue Technologie mitzugestalten. Nicht wenige Internetprotokolle aus dieser Zeit werden noch heute verwendet.

Durch die zunehmende Verbreitung von PCs und den weltweiten Ausbau der Internetknotenpunkte nahm die wirtschaftliche Nutzung digitaler Technologien in den 1980er und 1990er Jahren enorm zu. Unternehmen begannen, die digitale Entwicklung weiter voranzutreiben und zu dominieren. Während in den frühen Zeiten der Digitalisierung und besonders von den Akteuren des ARPANET und anderer früher Netzwerke Software oft frei geteilt und gemeinschaftlich weiterentwickelt wurde – schließlich ging es genau darum, sich miteinander zu vernetzen –, erhielt nun proprietäre, das heißt geschlossene, Software einen enormen Aufschwung. Proprietäre Software ist durch technische und rechtliche Maßnahmen (wie Patent- und Urheberrecht) davor geschützt, bearbeitet und verbreitet zu werden. Ihr Siegeszug trug dazu bei, dass technische Systeme für die Benutzer*innen nicht transparent arbeiteten und damit nicht überprüfbar oder gar gestaltbar waren.

Dagegen regte sich bald Widerstand, zunächst aus der akademischen Forschung, die aus den frühen Zeiten offenen, also lesbaren, Quellcode und kollaborative Arbeit gewohnt war, auch wenn diese auf wenige, privilegierte Akteur*innen beschränkt waren. Daher entstand 1985 die Free Software Foundation[15], die sich dafür einsetzt, dass Software mit bestimmten Rechten einhergehen muss: der Freiheit, Code zu verstehen, zu verwenden, zu verbreiten und zu verbessern.[16] Mit der GNU General Public Licence wurde 1989 die erste freie Lizenz entwickelt, die diese Rechte sicherstellt. Software, die unter einer freien Lizenz erarbeitet wird, heißt deshalb auch *Freie Software*. In der Folgezeit entstanden zahlreiche weitere sogenannte offene Lizenzmodelle, weshalb heute meist von Freier und Open-Source-Software (FOSS) gesprochen wird, um dieses Phänomen zu beschreiben.[17] Die Grundidee wurde auch auf an-

14 Vgl. Navarria, Giovanni: How the Internet was born: from ARPANET to the Internet. The Conversation, 2. November 2016. https://theconversation.com/how-the-internet-was-born-from-the-arpanet-to-the-internet-68072

15 https://www.fsf.org/about/what-is-free-software

16 https://fsfe.org/freesoftware/freesoftware.de.html

17 Zur Geschichte von Freier Software siehe auch Grassmuck, Volker: Freie Software – Zwischen Privat- und Gemeineigentum, bpb, 2007.

dere Kulturgüter übertragen. So können Werke wie Texte, Musik oder Videos mit offenen Creative Common Lizenzen einfacher geteilt werden.

Die Free Software Foundation war eine von mehreren zivilgesellschaftlichen Organisationen, die in dieser Zeit entstanden und digitale Themen ins Zentrum ihrer Arbeit stellten.[18] Die Forderung nach Transparenz technischer Systeme und sozial verantwortungsvoller Technikgestaltung ist seither nicht verklungen.

3 Eine starke Zivilgesellschaft als Basis für gemeinwohlorientierte Digitalisierung

3.1 Zivilgesellschaftliche Organisationen als Watchdogs und Policy-Expertinnen

Ein wichtiger Teil der Arbeit zivilgesellschaftlicher Organisationen ist die Kontrolle von politischen Prozessen. Als sogenannte Watchdogs beobachten sie sehr genau politische oder ökonomische Macht. Zivilgesellschaftliche Organisationen decken Missstände auf und erforschen die Auswirkungen neuer Technologien beispielsweise auf marginalisierte Gruppen. Sie schaffen Öffentlichkeit und geben Impulse für eine gemeinwohlorientierte Gestaltung. Ihre Arbeit ist eine Antwort »auf die Kontrolldefizite in einer globalisierten Welt, in der das Handeln selbst und seine Folgen kaum von den nationalstaatlichen Akteuren in den Blick genommen werden«.[19] Die digitale Zivilgesellschaft hat sich in den letzten Jahrzehnten um mehrere Schutzgüter organisiert: Sie hat sich zum Beispiel für den Schutz der Privatsphäre, gegen Überwachung, für Netzneutralität und Nutzer*innenrechte im Urheberrecht eingesetzt, um nur eine kleine Auswahl an Themen zu nennen. Sie vertritt die Interessen von Bürger*innen im digitalen Raum und macht sich für ihre Rechte stark. Mit ihrer Arbeit stellt sie sich gegen globale Konzerne, die aus Nutzer*innendaten maximalen Profit schlagen wollen, oder Regierungen, die ihre Bevölkerung mithilfe digitaler Werkzeuge überwachen. Sie klärt über komplexe Sachverhalte auf und trägt dazu bei, dass Themen öffentlich diskutiert werden. Ein aktuelles Beispiel aus dem letzten Jahr sind

18 Weitere Beispiele sind der Chaos Computer Club in Deutschland und die Electronic Frontier Foundation in den USA.

19 Speth, Rudolf: Machtkontrolle durch Watchdogs (FJ SB 3/2018, S. 3).

die Corona-Warn-App und der Schutz der Privatsphäre von Bürger*innen. Zivilgesellschaftliche Organisationen haben maßgeblich zur Aufklärung rund um die Apps beigetragen und Regierungen dabei beraten, welche Protokolle in Hinblick auf den Datenschutz zu bevorzugen sind. So basiert die deutsche Corona-Warn-App auf einer offenen Software und dezentralen Speicherung personenbeziehbarer Daten.

Organisationen der digitalen Zivilgesellschaft nutzen unterschiedliche Mittel, um ihrer Arbeit als Watchdog, Aufklärerin und Expertin gerecht zu werden. Kampagnen, wissenschaftliche Studien, Sitze in Beratungsgremien, strategische Klageführung – die Palette der Maßnahmen ist lang. Je nach Thema werden diese Maßnahmen auch kombiniert.

3.2 Die digitale Zivilgesellschaft als Übersetzerin und Sprachrohr

Kampagnen sind ein Mittel, um öffentliche Aufmerksamkeit auf ein Thema zu lenken und Druck auf Politik oder Konzerne auszuüben. Trotz der teils geringen finanziellen Ressourcen, die ihren Organisationen zur Verfügung stehen, hat die digitale Zivilgesellschaft in den vergangenen Jahren große netzpolitische Kampagnen auf die Straße gebracht und damit die Gesetzgebung in ungekanntem Ausmaß beeinflusst. Prominente Beispiele sind die globalen Aktionen gegen die US-amerikanischen Gesetzentwürfe SOPA[20] und PIPA[21] sowie gegen ACTA, ein geplantes internationales Handelsabkommen. Mit diesen drei Vorhaben sollten unter anderem Urheberrecht und andere Schutzrechte für geistiges Eigentum international vereinheitlicht und die Rechtsdurchsetzung stark verschärft werden. Sie waren damit eine Gefahr für die kreative, auf Sharing und Remix bauende internationale Netzkultur. Als Teil einer globalen Kampagne[22] blieben vielbesuchte Webseiten wie Wikipedia, Reddit, Google, Mozilla und Tumblr schwarz. Weltweit protestierten Menschen gegen die Abkommen[23] – mit Erfolg: Alle drei Vorhaben wurden auf Eis gelegt oder nicht ratifiziert.

Der Erfolg der Arbeit zivilgesellschaftlicher Organisationen im netzpolitischen Bereich fußt unter anderem darauf, dass sie abstrakte Policy- und

20 Patel, N.: What is SOPA and how does it work? The Stop Online Privacy Act explained. The Verge, 22.12.2011. https://www.theverge.com/2011/12/22/2648219/stop-online-piracy-act-sopa-what-is-it

21 https://de.wikipedia.org/wiki/PROTECT_IP_Act

22 https://www.wired.com/2012/01/websites-dark-in-revolt/

23 Vgl. https ://www.bbc.com/news/technology-16999497

Technologiethemen so kommunizieren, dass sie einer breiten Masse an Menschen zugänglich werden. Mithilfe von Aufklärungskampagnen, Slogans oder Comics werden komplexe Inhalte so aufbereitet, dass die unmittelbaren Auswirkungen auf den Alltag deutlich werden. Im Fall von ACTA oder den Protesten rund um Upload-Filter war es die drohende Beschränkung der Freiheit im Netz, die Tausende Menschen mobilisierte. Neben der Aufklärung werden Bürger*innen Mittel und Wege aufgezeigt, wie sie aktiv werden können, seien es Aufrufe zu Anrufen bei Abgeordneten[24] oder der Versand von Aktionspaketen für lokale Proteste.[25]

Eine solche Mobilisierung durch Skandalisierung einer abzulehnenden Maßnahme kann nur dann dauerhaft erfolgreich sein, wenn die Zivilgesellschaft es gleichzeitig schafft, eigene Forderungen zu benennen und sich für bessere Lösungen einzusetzen.

3.3 Die digitale Zivilgesellschaft als Fürsprecherin von Minderheiten

Neben Netzneutralität oder Urheberrecht, die das gesamte Internet betreffen, konzentrieren sich zivilgesellschaftliche Organisationen auch auf Themen, von denen zunächst nur Teile der Bevölkerung betroffen sind. Denn häufig sind es Minderheiten und gesellschaftliche Randgruppen, die die negativen Auswirkungen neuer Technologien und Policies als Erste zu spüren bekommen. Die digitale Zivilgesellschaft untersucht deshalb auch Themen wie den Einsatz von automatisierten Entscheidungssystemen in Behörden oder von Überwachungstechnologie an Landesgrenzen.

So hat beispielsweise die Arbeit der polnischen Panoptykon Foundation[26] maßgeblich dazu beigetragen, dass ein Algorithmus zurückgezogen werden musste, mit dem die polnische Arbeitslosenbehörde Arbeitssuchende bewerten wollte.[27] Das polnische Ministerium für Arbeit und Soziales hatte das Bewertungssystem 2014 vorgestellt. Mithilfe des Informationsfreiheitsgesetzes und einem Gerichtsverfahren konnte die Panoptykon Foundation weitere Details zum Scoring-Verfahren des Systems in Erfahrung bringen. Das System sollte die Arbeitsagentur bei der Beurteilung von Fördermaßnahmen für arbeitssuchende Menschen unterstützen. Dazu wurden Arbeitssuchende von

24 Vgl. https ://ffii.org/contact-your-mep-over-acta/
25 Vgl. https ://digitalegesellschaft.de/2012/05/hol-dir-jetzt-dein-acta-infopaket/
26 https://en.panoptykon.org/
27 https://en.panoptykon.org/articles/profiling-unemployed-poland-%E2%80%93-report

dem System in Kategorien eingeteilt. Ein Kritikpunkt der Panoptykon Foundation war die mangelnde Transparenz. Denn die Kriterien, anhand derer Arbeitssuchende eingestuft wurden, waren nicht offengelegt und konnten sich jederzeit ändern. Zudem hatten Arbeitssuchende keine Möglichkeit, im Fall von Falscheinträgen ihr Profil berichtigen zu lassen.[28] Eine Untersuchung des obersten Rechnungshofes ergab, dass das System zu Diskriminierung führen kann, da Frauen und benachteiligte Bevölkerungsgruppen schlechter bewertet werden. Ende 2018 entschied das polnische Verfassungsgericht, dass der Umfang der vom System verwendeten Daten in einem Gesetz hätte festgelegt werden müssen. Damit kippte das Verfassungsgericht den Einsatz des Algorithmus.[29]

3.4 Digitale Zivilgesellschaft als Expertin und Beraterin

Neben der Tätigkeit als Watchdog und als durchbremsendes Korrektiv sitzen zivilgesellschaftliche Organisationen auch in zahlreichen Beratungsgremien wie zum Beispiel der High-Level Expert Group on Artificial Intelligence[30] der Europäischen Kommission oder sind Teil von Multistakeholder-Prozessen wie beim Internet Governance Forum der Vereinten Nationen (IGF)[31]. Durch zahlreiche zivilgesellschaftliche Akteure kommen beim IGF Perspektiven auf den Tisch, die in Wirtschaft, Wissenschaft und Politik nicht oder nur sehr spärlich vertreten sind.[32]

Auffällig ist, dass zivilgesellschaftliche Organisationen trotz der wichtigen Perspektiven, die sie einbringen, im Vergleich zu Wirtschaft und Wissenschaft nur einen geringen Teil in politischen Beratergremien ausmachen.[33]

---

28 https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf

29 Vgl. https ://algorithmwatch.org/story/polnische-regierung-schafft-umstrittenes-scoring-system-fuer-arbeitslose-ab/

30 https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

31 https://www.igf2019.berlin/IGF/Navigation/DE/Home/home.html

32 https://www.intgovforum.org/multilingual/igf-2019-approved-onsite-participants-statistics

33 Ein Beispiel: Von 52 Akteuren der High-Level Expert Group on Artificial Intelligence kommen mit Vertreter*innen von Access Now und der Hilfsgemeinschaft der Blinden und Sehschwachen Österreichs (nach dem Ausscheiden von AlgorithmWatch 2018) nur zwei Akteure aus der Zivilgesellschaft. https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

Anders als große Unternehmen, die vielfältige Lobby-Anstrengungen verfolgen können, hat die Zivilgesellschaft verhältnismäßig geringe finanzielle Ressourcen, um langwierige Verhandlungen beobachtend zu begleiten und Gesetzesentwürfe innerhalb kurzer Fristen zu kommentieren. Im Fall des vierten, mehrere hundert Seiten starken Entwurfs für das IT-Sicherheitsgesetz, das massive Auswirkungen auf die Sicherheit informationstechnischer Systeme hätte, waren beispielsweise nur 28 Stunden zur Kommentierung durch externe Stakeholder vorgesehen.[34]

4 Gemeinwohlorientierte Digitalisierung braucht Transparenz und Offenheit

4.1 Räume für digitale Öffentlichkeit

Mit der Digitalisierung verschiebt sich auch der Ort, an dem sich Menschen politisch informieren und weiterbilden, gesellschaftliche Diskurse austragen und Allianzen schmieden, zunehmend ins Digitale. Dort fehlt jedoch ein hinreichender Ersatz für einen öffentlichen Raum, denn die Kommunikationsplattformen sind größtenteils in privatwirtschaftlicher Hand. Sie sollen nicht den gesellschaftlichen Diskurs ermöglichen und fördern, sondern Gewinne erwirtschaften. So kommt es, dass auf Plattformen wie Youtube und Facebook Inhalte von staatlichen Einrichtungen und dem öffentlichen Rundfunk bereitgestellt, diskutiert und verbreitet werden. Daraus ergeben sich verschiedene Probleme; beispielsweise stimmen die Rechts- und Wertemodelle der Plattformbetreiber*innen nicht mit einzelnen gesellschaftlichen und rechtlichen Normen überein.[35]

Das Geschäftsmodell dieser Plattformen basiert auf Werbung und ist deshalb davon abhängig, dass Nutzer*innen möglichst lange auf ihnen verweilen. Um das zu erreichen, werden Algorithmen eingesetzt, die entscheiden,

34 Vgl. https ://www.fiff.de/presse/offener-brief-beteiligung

35 Beispielsweise wird auf Facebook Nacktheit – insbesondere weibliche Nacktheit – so rigoros zensiert, dass sogar Kunstwerke betroffen sind und ein Austausch über sie unmöglich gemacht wird. Gleichzeitig wurden regional spezifische Straftatbestände wie z.B. die Leugnung des Holocaust von den Plattformen lange nicht unterbunden – erst 2020 verpflichtete sich Facebook, dagegen vorzugehen. https://www.dw.com/de/facebook-l%C3%B6scht-erneut-kunstwerk-wegen-nacktheit/a-43048946 https://about.fb.com/de/news/2020/10/weltweite-entfernung-von-inhalten-die-den-holocaust-leugnen/

welche Inhalte den Nutzer*innen bevorzugt angezeigt werden. Studien belegen, dass sich durch diese Algorithmen Filterblasen bilden, die offenen Meinungsaustausch verhindern. Filterblasen und Empfehlungsalgorithmen können demnach zur Radikalisierung ganzer Szenen beitragen.[36]

Mit der Verschiebung ins Digitale findet bürgerliches Leben zunehmend im Privaten statt, wo die Regeln nicht primär gesellschaftlich ausgehandelt werden. Mit diesem Wechsel zu privaten Plattformen ist der Zugang zur Öffentlichkeit und die eigene Sichtbarkeit für einige erschwert oder gar unmöglich gemacht worden. Diese Plattformen sind extra so gebaut, dass sie auf alten Betriebssystemen und leistungsschwächeren Smartphones nicht funktionieren. Sie benötigen eine große Internetbandbreite, die sich viele nicht leisten können. Menschen, deren audiovisuelle oder motorische Fähigkeiten eingeschränkt sind, haben oft Schwierigkeiten mit diesen Diensten. Die Technologie ist nämlich so optimiert, dass sie für eine kleine Gruppe von technikaffinen 20- bis 40-Jährigen, die gesund und wohlhabend sind, sehr gut zu handhaben ist; andere Teile der Gesellschaft sind aus wirtschaftlichen Gründen nicht interessant genug.

Zudem zensieren soziale Medien, aber auch Dienstleister wie der Videotelefonieanbieter Zoom, Inhalte und Veranstaltungen auf ihren Plattformen,[37] darunter politische Diskussionen, die von Hochschulen ausgerichtet werden, oder schließen nach internen Regeln Kund*innen aus: Private Unternehmen entzogen der Enthüllungs-Plattform Wikileaks 2010 nach der Veröffentlichung geheimer diplomatischer Depeschen den Speicherort ihrer Webseite, ihre Domain sowie die Möglichkeit, digital Spenden entgegenzunehmen.

Aus all diesen Gründen sind private Plattformen derzeit nicht dafür geeignet, alleine Räume für die digitale Öffentlichkeit herzustellen – auch wenn es seitens der Europäischen Union Bestrebungen gibt, für mehr rechtliche Klarheit zu sorgen und die Plattformbetreiber zur Rechenschaft zu ziehen. Die Zivilgesellschaft versucht, dem mit unterschiedlichen Ansätzen zu begegnen. Dazu gehören Faktenchecks auf den Plattformen, die von gemeinnützigen Organisationen durchgeführt werden – im Fall von Correctiv sogar im

36 Vgl. Darby, Luke: Facebook Knows It's Engineered to »Exploit the Human Brain's Attraction to Divisiveness«. gq.com, 24. Mai 2020. https://www.gq.com/story/facebook-spare-the-share;Ribeiro, M. H., Raphael Ottoni, Robert West, Virgílio A. F. Almeida und W. Meira: »Auditing radicalization pathways on YouTube.« Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (2020): n. pag.

37 Vgl. https://www.insidehighered.com/quicktakes/2020/10/27/zoom-faces-more-allegations-censorship

Auftrag des Plattformbetreibers Facebook.[38] Andere entwickeln alternative Technologien unter offenen Lizenzen, die zivilgesellschaftliche Organisationen und öffentliche Einrichtungen selbst betreiben können, um weniger auf proprietäre, privatwirtschaftliche Plattformen angewiesen zu sein. Beispiele gibt es viele, Nutzer*innen allerdings nur wenige: Mastodon, eine Open-Source-Alternative zu Twitter, ist eine solche Technologie. Dabei ist nicht nur die Lizenz offen im Sinne des Gemeinwohls, sondern auch der Aufbau: Das Netzwerk besteht aus vielen verschiedenen Instanzen, die von Einzelpersonen oder Organisationen betrieben werden können und die untereinander vernetzt sind, aber nicht zentral gesteuert werden. Auch ohne Internetverbindung funktioniert die Chat-App Briar, die auf lokale Mesh-Netzwerke (wie lokales WLAN, Bluetooth) zurückgreifen kann und sich zudem Sicherheit und Datenschutz auf die Fahnen geschrieben hat. Open-Source-Alternativen zu kommerziellen Plattformen im Bildungsbereich sind beispielsweise Moodle und Big Blue Button.

4.2 Zugang zu Wissen, offene Daten und Partizipation

Wie Douglas Engelbart in seinem eingangs erwähnten Vortrag beschreibt, haben Internet und digitale Werkzeuge großes Potenzial, gemeinsam Probleme zu lösen und zu kollaborieren. Neben kommerziellen sozialen Netzwerken sind in den letzten Jahren auch einige Partizipationsplattformen entstanden, auf denen Bürger*innen sich politisch beteiligen können. Sie können online über Bürger*innenhaushalte abstimmen[39] und Gesetzesentwürfe kommentieren. Zivilgesellschaftliche Organisationen haben diese Bewegung von Anfang an vorangetrieben. Denn die Grundlage für politische Mitbestimmung, gesellschaftliche Gestaltung und damit auch für eine gemeinwohlorientierte Digitalisierung ist der Zugang zu Informationen und das Vertrauen in demokratische Prozesse. Zivilgesellschaftliche Organisationen waren Vorreiter*innen darin, den gesellschaftlichen Mehrwert von offenen Daten anhand von digitalen Werkzeugen zu demonstrieren. Erst nach jahrelangem Engagement zivilgesellschaftlicher Organisationen ist Deutschland der Open Government Partnership beigetreten und hat sich damit zu offenem Regierungshandeln

38 Vgl. https ://correctiv.org/faktencheck/

39 Vgl. https ://www.deutschlandfunk.de/wenn-buerger-politik-gestalten-barcelonas-erfolg-mit-der.795.de.html ?dram :article_id=471680

verpflichtet.[40] Dabei ist der Zugang zu offenen Daten eine Grundlage für informierte Entscheidungen von Bürger*innen, die zum Beispiel anhand von Finanzdaten nachvollziehen können, wie öffentliche Gelder verwendet wurden.

So ermöglicht das Online-Portal KleineAnfragen.de[41] beispielsweise einen einfachen Zugang zu Informationen. Über diese zivilgesellschaftliche Plattform werden die namengebenden Kleinen Anfragen – also formal eingereichte Anfragen von Abgeordnet*innen in Bundes- und Landesparlamenten in Deutschland – bundesweit archiviert und über eine Volltextsuche verfügbar gemacht.[42] Ein Beispiel aus Taiwan zeigt, wie erfolgreich solche Angebote sein können, wenn sie Unterstützung von staatlichen Stellen erhalten: Die taiwanesische Civic-Tech-Community g0v zero[43] hat die Plattform vTaiwan entworfen, auf der Vorschläge für die Gesetzgebung rund um die digitale Wirtschaft gesammelt, diskutiert und abgestimmt werden. Seit dem Start von vTaiwan im Jahr 2015 haben sich mehr als 200.000 Menschen auf der Plattform beteiligt. Auf Basis der Vorschläge aus den Beteiligungsverfahren wurden 26 Gesetzesentwürfe des taiwanesischen Parlaments verabschiedet.[44] Die Plattform wird von der Digitalministerin und vom Parlament gefördert.

40 Vgl. https ://opengovpartnership.de/beitritt-deutschlands-zur-open-government-partnership-wie-geht-es-weiter/

41 https://kleineanfragen.de/

42 Eine solche Suche ist nicht nur für Journalist*innen und Bürger*innen interessant, sondern auch für Verwaltungsangestellte, die Informationen aus den Antworten auf diese Anfragen benötigen. KleineAnfragen.de wurde 2014 von einem Freiwilligen entwickelt. Das ehrenamtliche Projekt, wurde maßgeblich auch von Mitarbeiter*innen aus der öffentlichen Verwaltung, sowie Politker*innen genutzt, die in den Dokumenten Informationen fanden, die sie für ihre Arbeit benötigen. Nachdem die Dokumente der kleinen Anfragen von Seiten der Verwaltung auch nach jahrelangem Nachfragen der Zivilgesellschaft, nicht über eine maschinenlesbare Schnittstelle bereitgestellt wurden, wurde der Aufwand Seitens der Ehrenamtlichen zu groß und das Portal musste mit 31.12.2020 eingestellt werden https://kleineanfragen.de/info/stilllegung

43 https://g0v.asia/

44 Vgl. https ://www.nesta.org.uk/report/using-collective-intelligence-solve-public-problems/

5 Digitale Grundsicherung geht vor Spitzentechnologie

Neben ihrer Tätigkeit als kritische Kommentatorin und beratende Instanz zu Digitalisierungsthemen betätigt sich die digitale Zivilgesellschaft auch aktiv daran, die digitale Transformation der Gesellschaft voranzutreiben: Sie entwickelt Anwendungen, stellt Datensätze bereit und bietet digitale Dienste ganz unterschiedlicher Art an. Dabei tritt sie nur scheinbar in Konkurrenz zu öffentlichen Angeboten oder der Wirtschaft. Die Angebote aus der Zivilgesellschaft folgen nämlich anderen Zielsetzungen und Werten: Ihr geht es darum, durch digitale Angebote eine Grundversorgung zu gewährleisten, die eigentlich von staatlicher Seite bereitgestellt werden müsste, wie die oben genannten Open-Data-Initiativen, Partizipations- und Transparenzangebote wie KleineAnfragen.de oder abgeordnetenwatch.de zeigen. Sie befasst sich aber auch mit ganz grundlegenden Herausforderungen wie dem Zugang zum Netz. Sie überträgt damit das Konzept von Gemeinwohl ins Digitale und wird zur schützenden Instanz.

Ein Beispiel hierfür ist der Verein Freifunk[45], ein Netzwerk aus lokalen und regionalen Initiativen, die in Städten und Gemeinden freie Funknetze aufbauen und betreiben und so Menschen Zugang zum Internet gewähren. Hierfür entwickeln sie auch die notwendige offene Firmware und Software, um handelsübliche Geräte für ihre Netzwerke nutzbar zu machen. Freifunk ist die zivilgesellschaftliche Antwort auf zwei grundlegende Herausforderungen der Digitalisierung in Deutschland: Zum einen geht der Netzausbau immer noch nur schleppend voran und ist mit langwierigen, kostenintensiven Bauarbeiten verbunden. Mesh-Netzwerke lassen sich im Vergleich dazu schnell anlegen und können auch besser angepasst werden, wenn sich der Bedarf oder das Nutzungsverhalten vor Ort ändert. Zum anderen hat die rechtliche Lage dazu geführt, dass in Deutschland weniger offene WLAN-Netze angeboten werden als in anderen Ländern. Im Rahmen der sogenannten Störerhaftung konnten Betreiber*innen solcher Netzwerke rechtlich belangt werden, wenn aus ihrem WLAN-Netz beispielsweise nicht-lizensierte Kopien von Filmen oder Musik heruntergeladen wurden. Einzig die Freifunk-Initiative nahm das Risiko auf sich und lieferte vielerorts das, was für die Teilhabe an der digitalen Gesellschaft Grundvoraussetzung ist: freien Zugang zum Netz.

45 https://freifunk.net/

Freier Zugang bedeutet dabei nicht nur kostenloser Zugang. Basis des freien Zugangs sind zudem Werte wie das Recht auf Anonymität, Freiheit von Zensur, gemeinschaftliche Verwaltung des Netzes und eine nicht-kommerzielle Ausrichtung.

6 Open-Source-Software und Dienste als Fundament der digitalen Öffentlichkeit

Freifunk ist zweifellos das eingängigste Beispiel, wie die Zivilgesellschaft dafür sorgt, dass die digitale Grundsicherung gewährleistet wird. Aber auch zahlreiche andere Initiativen und Gruppen tragen dazu bei, indem sie, unter anderem, Open-Source-Software (wie den Browser Mozilla Firefox oder das Betriebssystem Linux) mitentwickeln oder digitale Dienste betreiben.

Auch sie folgen in ihrer Arbeit den oben aufgeführten Werten Freier und offener Software, die sie von gängigen kommerziellen Lösungen abhebt. Dazu gehört, die Software für möglichst viele Menschen nutzbar zu machen (durch offene Lizenzen), die Funktionsweise der Software nachvollziehbar zu machen (durch die Veröffentlichung des Quellcodes und reproduzierbare Builds) sowie offene Schnittstellen und Interoperabilität zwischen verschiedenen digitalen Anwendungen oder Plattformen (beispielsweise ActivityPub für interoperable soziale Netzwerke) zu gewährleisten. Durch diese Grundwerte wird es möglich, Dienste dezentral zu betreiben, wodurch die Nutzer*innen wiederum verhältnismäßig einfach zwischen verschiedenen Anbieter*innen dieser Dienste wechseln können.

Diese Anbieter*innen arbeiten zwar oft wirtschaftlich und sind somit nicht Teil der digitalen Zivilgesellschaft, haben ihre Wurzeln jedoch häufig in Community-Projekten und arbeiten eng vernetzt mit Ehrenamtlichen zusammen. Im Gegensatz zu den Softwareunternehmen, die auf proprietäre Software setzen, um Kund*innen an sich zu binden und im Wettbewerb zu bestehen, rücken Open-Source-Unternehmen häufiger nachhaltiges Wachstum sowie Kooperation und Austausch mit anderen Anbieter*innen in den Mittelpunkt.

Stärker zivilgesellschaftlich geprägt ist der Bereich Civic Tech, also die Entwicklung von digitalen Technologien für die Gesellschaft. Hinter Civic Tech stehen keine großen Unternehmen, sondern ehrenamtliche Softwareentwickler*innen, Designer*innen, Erfinder*innen und mehr. Sie erschaffen Anwendungen, die dem Gemeinwohl dienen und es den Menschen erleichtern

sollen, sich zu informieren, ihre Rechte wahrzunehmen und an politischen Prozessen teilzuhaben.[46] Sie entwerfen damit nicht selten Angebote, die eigentlich von öffentlichen Einrichtungen selbst bereitgestellt werden sollten, wie im Fall der oben beschriebenen gov-Community aus Taiwan. So üben sie einerseits Druck auf öffentliche Einrichtungen aus, ihr Angebot zu erweitern, zeigen andererseits aber auch gleich einen möglichen Lösungsweg auf.

Die digitale Zivilgesellschaft tritt also ganz unterschiedlich für die digitale Grundsicherung ein und setzt damit einen Gegenpunkt zur öffentlichen Förderpraxis, die sich mit wenigen Ausnahmen[47] auf Innovation und sogenannte Spitzentechnologien wie künstliche Intelligenz konzentriert. Allerdings kann es dauerhaft nicht die Aufgabe der Zivilgesellschaft sein, eine digitale Grundsicherung zu gewährleisten. Dafür fehlen ihr die Mittel, der gesellschaftliche Auftrag und der notwendige Rechtsrahmen, wie das Beispiel Störerhaftung zeigt. Deshalb braucht es dringend einen kontinuierlichen Dialog zwischen staatlichen Einrichtungen, Zivilgesellschaft und Wirtschaft, der die grundlegenden Bedürfnisse der Gesellschaft bei der Digitalisierung in den Fokus nimmt, bestehende *digital gaps* aufzeigt, die zu Benachteiligung einzelner sozialer Gruppen führen, und Lösungen im Sinne des Gemeinwohls anstrebt.

7 Digitalisierung muss im Interesse der gesamten Gesellschaft gestaltet werden

Eine digitale Grundsicherung ist für eine lebendige, digital aktive und selbstbestimmte Gesellschaft elementar. Deshalb muss sich die Gestaltung der Digitalisierung an den Bedürfnissen der gesamten Gesellschaft orientieren. Dafür gibt es jedoch mehrere ganz praktische Hürden. Eine davon ist mangelnde Diversität: Wie schon bei den politischen Entscheider*innen und in der Wissenschaft sind auch in der Technologieentwicklung manche Gruppen über- und andere unterrepräsentiert. Am häufigsten diskutiert wird das Ungleichgewicht zwischen Männern und Frauen. So waren 2018 nur 16,6 Prozent der in der IT-Branche Beschäftigten Frauen.[48] Menschen mit Behinderungen

46 Vgl. Prototype Fund: Civic Tech: Technologie für Bürger*innen. Medium, 7.9.2016. https://medium.com/@prototypefund/civic-tech-technologie-f%C3%BCr-b%C3%BCrger-innen-8ddf22c492#.420v5a8ys

47 Z.B. durch das Open-Source-Förderprogramm Prototype Fund.

48 Vgl. https://de.statista.com/infografik/13283/frauen-in-der-tech-branche/, https://www.honeypot.io/de/women-in-tech-2018/

machten 2015 weniger als 1 Prozent der IT-Auszubildenden aus.[49] Das deutsche Bildungssystem ist stark sozial selektiv und wenig durchlässig für Menschen, die nicht bereits aus einem akademischen Umfeld stammen.[50] Dadurch dürften auch unter Informatikstudierenden und studierten Entwickler*innen Menschen aus Akademikerfamilien überwiegen. Als immer noch relativ neues und stetig wachsendes Berufsfeld beschäftigt die IT-Branche auch wenig ältere Menschen. Kurz: Die Technologiebranche bildet nicht annähernd die pluralistischen Erfahrungen und Hintergründe der Gesellschaft ab. Sie verfügt schlichtweg nicht über das notwendige Wissen, um die Bedürfnisse verschiedener Gruppen mitzudenken, Produkte für alle zugänglich und nutzbar zu gestalten und Diskriminierung aktiv vorzubeugen. Zudem ist dieses Wissen oft nicht außerhalb individueller Erfahrungen verfügbar. Marginalisierte Gruppen sind nicht nur persönlich unterrepräsentiert, sondern auch in den Daten. Missstände, beispielsweise beim Einsatz datengetriebener algorithmischer Entscheidungssysteme, können deshalb häufig gar nicht objektiv dargestellt werden.[51]

Zivilgesellschaftliche Organisationen, die Menschen aus marginalisierten Gruppen repräsentieren, verbinden zunehmend ihre sozialen Inhalte mit digitalen Themen und werden damit zu den wenigen Interessensvertreterinnen, die sich für die Belange unterrepräsentierter Gruppen im Digitalbereich einsetzen. Durch die zunehmende Verbreitung und Relevanz algorithmischer Systeme sind in den letzten Jahren mehrere internationale Initiativen entstanden, wie die 2016 von der Informatikerin Joy Buolamwini gegründete Algorithmic Justice League,[52] die das Diskriminierungspotenzial dieser Systeme aufzeigen und sich für eine transparentere Technikentwicklung einsetzen, die Chancengleichheit als Grundsatz hat.

49 Vgl. https ://www.bonn-rhein-sieg-fairbindet.de/wp-content/uploads/2015/10/141031_PM_Inklusive_IT-Berufe.pdf

50 Vgl. https ://www.hochschulbildungsreport2020.de/chancen-fuer-nichtakademikerkinder

51 Vgl. die Beiträge von C. Hustedt, Leonie Beining und L. Jaume-Palasi in diesem Band.

52 Vgl. https ://www.ajl.org/

8 Ausblick: Welche Wege eröffnen sich durch eine gemeinwohlorientierte Digitalisierung?

Die Zivilgesellschaft macht vor, wie die Digitalisierung im Sinne des Gemeinwohls und der Gesellschaft gestaltet werden kann, wenn die richtigen Rahmenbedingungen geschaffen und die Werte der Zivilgesellschaft auch an anderer Stelle gelebt werden.

8.1 Zivilgesellschaft als Visionärin und Treiberin

Die Arbeit als Korrektiv bindet derzeit noch viele begrenzte Ressourcen zivilgesellschaftlicher Organisationen. Wenn ihre kontinuierlich vorgebrachten Forderungen (zum Beispiel die nach mehr Transparenz im öffentlichen Sektor oder echten Beteiligungsmöglichkeiten an politischen Diskussionen) eines Tages Gehör finden, kann sich die Zivilgesellschaft verstärkt der aktiven Mitgestaltung der digitalen Zukunft widmen, indem sie neue Visionen einer Digitalisierung für die Gesellschaft entwirft und vorsorglich Vorschläge in digitalpolitische Debatten einbringt. So forderten 2020 zahlreiche Organisationen der digitalen Zivilgesellschaft: »Digitalpolitik, die das Gemeinwohl ins Zentrum stellt, lässt sich nur gemeinsam mit gesellschaftlichen Akteurinnen, Akteuren und Initiativen verwirklichen. Hierfür muss sich die Politik noch weiter für Vorschläge aus der Gesellschaft öffnen und diese in die Politikgestaltung miteinbeziehen.«[53] Wenn sich diese Einbindung nicht mehr auf eine rein kommentierende, erst zum Ende des politischen Prozesses einsetzende Scheinbeteiligung beschränkt, kann sie ihr volles Ideenpotenzial ausschöpfen und die politischen Debatten rund um Digitalisierung mit mutigen gesellschaftlichen Visionen ergänzen. Eine vielfältige und fachlich kompetente Zivilgesellschaft kann mit ihrer Expertise eine Lücke füllen, die seit Jahren in der deutschen Digitalpolitik klafft.

8.2 Nachhaltige und belastbare zivilgesellschaftliche Strukturen schaffen – durch neue Formen der Förderung

Die Zivilgesellschaft zeigt nicht nur, wo es an Förderung fehlt, wenn alleine an die Wirtschaft gedacht wird – sie macht auch vor, wie Förderung neu gestaltet werden kann. Aufbauend auf erfolgreichen Pilotprojekten wie dem Pro-

53 https://digitalezivilgesellschaft.org/

totype Fund[54] können andere Förder- und Investitionsprogramme getestet werden, die der digitalen Zivilgesellschaft eine längerfristige Planung und eine strategische Schwerpunktsetzung ermöglichen, statt auf kurzfristige, wenig nachhaltige Projektarbeit zu setzen. So können Organisationen gesellschaftlich relevanten Themen im Digitalbereich wie Barrierefreiheit, Zugang zu Informationen oder Nachhaltigkeit mehr Gewicht verleihen, statt politisch gewollten Digitalisierungstrends wie künstlicher Intelligenz folgen zu müssen. Eine solche Förderung könnte auch die Wirtschaft positiv beeinflussen, wenn sie die Zusammenarbeit von Stakeholdern aus Wissenschaft, Zivilgesellschaft, öffentlicher Verwaltung und Wirtschaft forciert.

8.3 Offenheit und Diversität als Leitwerte für Digitalpolitik

Was die Arbeit der Zivilgesellschaft im Digitalbereich – und darüber hinaus – auszeichnet, sind die ihr zugrunde liegenden Werte. Dazu gehört allen voran Offenheit: Die offene, transparente Arbeitsweise ermöglicht es, sich kontinuierlich zu vernetzen, voneinander zu lernen, gemeinsam Strukturen aufzubauen und Ressourcen klug zu nutzen. Nicht zuletzt deshalb fordert die Zivilgesellschaft eine vergleichbare Offenheit von Politik und Wirtschaft, insbesondere dort, wo diese Werkzeuge oder Dienstleistungen für die öffentliche Verwaltung umsetzen – sei es in Form von offenen Daten, Transparenzberichten oder Open-Source-Anwendungen. Schafft sie es, sich mit dieser Forderung Geltung zu verschaffen, ist eine im Sinne des Gemeinwohls gestaltete Digitalpolitik ebenso möglich wie innovatives, digitales Sozialunternehmertum, das auf nachhaltige Geschäftsmodelle setzt und eine digitale Gesellschaft besonders für unterrepräsentierte und benachteiligte Gruppen besser macht und nicht nur für die Interessen einer finanziell starken Minderheit.

8.4 Digitale Souveränität neu denken

Die genannten Entwicklungen sind eine notwendige Grundlage für eine digitale Souveränität, wie sie das Kompetenzzentrum Öffentliche IT definiert: »Digitale Souveränität ist die Summe aller Fähigkeiten und Möglichkeiten von

54 Bei diesem öffentlichen Open-Source-Förderprogramm, das von einer zivilgesellschaftlichen Organisation begleitet wird, steht statt der Technologie die gesellschaftliche Herausforderung im Mittelpunkt.

Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.«[55] Nur mit aktiver Mitwirkung der Zivilgesellschaft, mit vorausschauender Gestaltung und vielfältigen Visionen in der Digitalpolitik und der Technologieentwicklung können wir sie erreichen.

55 Goldacker, G.: Digitale Souveränität, Berlin 2017, S. 3. https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t

3.5 Internationales
Geopolitische Diplomatie und die europäische Digitalstrategie

Tyson Barker

Im Mai 1844 übermittelte der US-amerikanische Erfinder Samuel Morse die erste elektronische Nachricht über eine 44 Kilometer lange Telegrafenleitung zwischen Washington, DC, und Baltimore. Diese Nachricht, die ihm die Tochter eines Freundes vorgeschlagen hatte, enthielt den Bibelvers: »What hath God wrought?« (zu Deutsch: »Was hat Gott geschaffen?«[1]). Morse sendete damals aus einem Raum direkt im US-Kapitol, in dem noch heute eine Gedenktafel an diese erste elektronische Mitteilung der Welt erinnert. Der Inhalt seiner Nachricht spricht für die tiefe Ehrfurcht vor der Erkenntnis, welche unglaubliche Kraft und Macht diese technische Innovation für das noch junge Industriezeitalter mit sich brachte. Schon bald verbanden Telegrafenleitungen Nationen miteinander, schufen neue Lieferketten und revolutionierten die Kriegsführung. Im Jahr 1946, fast hundert Jahre später, wurde derselbe Raum im US-Kapitol die neue Heimat des Joint Committee on Atomic Energy, dem führenden Gremium für die zivile und militärische Nutzung von Atomkraft.[2] Wiederum war ein neues Zeitalter angebrochen – das Atomzeitalter –, getragen von einer weiteren transformativen Technologie, die Potenzial, Macht, militärische und ökonomische Emanzipation und beängstigende Zerstörungskraft in sich vereint.[3]

In jedem dieser technologisch-historischen Schlüsselmomente war die internationale Gemeinschaft gezwungen, zusammenzuarbeiten, um

1 Vgl. https ://www.loc.gov/item/today-in-history/may-24

2 Records of the Joint Committees of Congress 1789-1989, in: National Archives https://www.archives.gov/legislative/guide/house/chapter-23-joint-atomic-energy.html

3 Vgl. Barker, Tyson: NextGen Network: How AI can work for humanity, in: NextGen Network Report 2020 https://www.aspennextgen.org

Normen, technische Standards, Regelwerke, Kommunikationsmittel, internationale Institutionen und letztlich eine internationale Ordnung zu schaffen. Wenn also heute eine internationale digitale Ordnung entsteht, müssen sich die Demokratien Europas fragen: Welche Art globale technologische Ordnung brauchen wir? Wollen wir wertebasierte Gesellschaften, Staaten und Mächte nach dem Vorbild der EU schaffen? Wie können unsere Werte und das Gemeinwohl zur treibenden Kraft bei der Gestaltung der Digitalisierung werden? Wie erreichen wir dieses Ziel vor dem Hintergrund des geopolitischen Systemwettbewerbs im digitalen Raum? Klar ist, Europas digitale Regulierungsstrategie und Industriepolitik müssen sich an internationalen Interessen orientieren, wie der Sicherung der wirtschaftlichen Stärken Europas, der Bewahrung demokratischer Grundwerte, der Förderung globaler Cyber-Resilienz, dem Schutz einer offenen digitalen Ordnung und der Förderung grüner Technologien zur Reduzierung von CO_2-Emissionen.

Schließlich steuert die Welt heute auf ein neues technologisches Zeitalter zu, da gleich mehrere transformative digitale Technologien wie künstliche Intelligenz (KI) und Big Data, Cloud- und Edge-Computing, Quantentechnologien, Blockchain und Internet of Things zum Einsatz kommen. Sie ermöglichen neue Formen des medizinischen Screenings und der Patientenbehandlung, sicherere, selbstfahrende Fahrzeuge, eine einfachere, natürlichere Mensch-Maschine-Interaktion, eine effizientere Logistik, bessere landwirtschaftliche Methoden und höhere Ernteerträge sowie eine schnellere Entscheidungsfindung in allen Bereichen, angefangen vom Versicherungs- über das Bankwesen und die Polizei bis hin zur nationalen Sicherheit. Zusammengenommen werden die digitalen Technologien das globale wirtschaftliche und geopolitische Kräfteverhältnis so nachhaltig und grundlegend verändern, wie es seit der industriellen Revolution nicht mehr der Fall war.

Die Notwendigkeit zur Zusammenarbeit und Verständigung über die offenen Fragen ist groß. Insbesondere angesichts der zunehmenden Fragmentierung des Internets, der Lokalisierung von Daten, der wachsenden Rolle von Technologien als ideologische Einflussfaktoren für den Export von Governance-Modellen – durch neue Internetprotokolle wie New IP, Chinas digitale Seidenstraße, die Nutzung und den Export von KI-gestützter Massenüberwachung, unter der derzeit mehr als eine Million Uiguren leiden – sowie auch der stärkeren Instrumentalisierung digitaler Abhängigkeiten als politische Waffen. Die Corona-Krise hat viele dieser Trends beschleunigt, sowohl im Positiven als auch im Negativen. Sie hat einerseits eine vermehrte Nutzung digitaler Technologien bewirkt und andererseits ein neues

Bewusstsein für die Anfälligkeit globaler Lieferketten und neue Formen technologischer Abhängigkeiten geschaffen. Tatsächlich hat die Corona-Krise zahlreiche neue Cyber-Schwachstellen geöffnet und grundsätzliche Fragen zur Zukunft der Demokratie, der digitalen Souveränität und der Menschenwürde aufgeworfen. Vor diesem Hintergrund entsteht eine neue geotechnologische Landschaft – also ein Umfeld, bei dem die NATO kürzlich von einer »strategischen Gleichzeitigkeit« sprach, in dem also mehrere miteinander verbundene Herausforderungen parallel auf die Demokratien zukommen.[4]

Zudem setzen neue disruptive Technologien die Governance-Architektur der meisten Länder unter Druck und konfrontieren Gesellschaften mit ethischen, wirtschaftlichen und politischen Differenzen, die es auszugleichen gilt. Weltweit haben sich Regierungen, Technologieunternehmen, die Europäische Union, die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung, die NATO, Multi-Stakeholder-Foren, internationale Gremien für Normen wie die International Standards Organization (ISO), die Kommunistische Partei Chinas und sogar der Vatikan mit den ethischen und geopolitischen Herausforderungen der nahezu prometheischen Kräfte auseinandergesetzt, die durch Deep Learning, 5G, Cybersicherheit, Edge-Computing und digitale Währungen entfesselt werden können. Was Gott geschaffen hat, in der Tat.

Das Zeitalter der technologischen Revolutionen brachte neue Ethiken, Regulierungsphilosophien, Institutionen und Governance-Modelle hervor. Innerhalb der ersten 21 Jahre nach der Erfindung des Telegrafen gründeten die Staaten Europas in Paris die Internationale Fernmeldeunion (engl. International Telegraph Union, ITU). Als eine der ersten multilateralen Institutionen der Welt wurden mithilfe der ITU das Alphabet standardisiert, das Recht auf Telegrafenzugang für alle geschützt und Regeln für das Briefgeheimnis geschaffen. Die ITU existiert heute unter dem Namen International Telecommunications Union als UN-Sonderorganisation. Mit der Entwicklung der Atomenergie entstand ein Dickicht von Normen, technischen Standards, Institutionen und Protokollen.[5] In Europa wurde die Europäische Atomge-

4 https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

5 Eisenhowers »Atoms for Peace«-Programm von 1953, der Gründung der Internationalen Atomenergie-Organisation (IAEO) von 1958, den Nichtverbreitungs- und Rüstungskontrollregimen wie dem Atomwaffensperrvertrag (Non-Proliferation Treaty, NPT) und stark regulierten Exportkontrollen.

meinschaft (Euratom) gegründet, eine europäische Vorgängerorganisation, die der EU auch als Integrationsprojekt diente. Dazu gehörte ebenfalls das gemeinsame Forschungszentrum Conseil Européen pour la Recherche Nucléaire (CERN), aus dem schließlich das World Wide Web hervorging.[6] Auf jeden Fall brachte die Technologie eine neue internationale Ordnung hervor, indem sie neue Werte, Instrumente und Institutionen zusammenführte, um die Kraft der Technologie zu kanalisieren – und ihre Macht an internationales Recht und Normen zu binden.[7]

Im Laufe der Jahrzehnte haben Europa und die USA mit anderen Demokratien zusammengearbeitet, um Multi-Stakeholder-Foren wie das World Wide Web Consortium (W3C), das Institute of Electrical and Electronics Engineers (IEEE) und das Internet Governance Forum (IGF) als zentralen Ort der Internet-Governance und -Standards zu fördern, in denen Staaten mit der Zivilgesellschaft, der Wirtschaft, Expert*innen und Akademiker*innen gemeinsam beraten, um einen Konsens über die Governance-Inhalte und Strukturen zu schmieden. Dieses Modell wird zunehmend von autoritären Mächten wie China und Russland infrage gestellt, die die Kontrolle über die digital Governance in die merkantilistischen Hände des Staates legen wollen, oft mit der Begründung, dass sie Cybersicherheit oder digitale Souveränität wiederherstellen wollen.

Europas großes technisches Umdenken

Die EU unternimmt bereits ehrgeizige Anstrengungen bei der Neufassung digitaler Regulierung, die auf den Prinzipien von Menschenrechten, Rechtsstaatlichkeit und Demokratie beruht. Zu den Vorschlägen der EU gehören neue Ansätze in den Bereichen Data Governance, Cloud-Computing, künstliche Intelligenz, Content-Moderation von Hassrede und Desinformation, Cybersicherheit und Marktmacht. Europas Bemühungen stellen einen ehrgeizigen Versuch dar, ein neues Regelwerk für die digitale Welt zu schaffen.[8] Bei der Regulierung von Plattformen ist Europa führend und wähnt sich als

6 CERN: Die Geburt des Webs, in: https://home.cern/science/computing/birth-web

7 Siehe hierzu auch den Beitrag von Matthias C. Kettemann in diesem Band.

8 Vgl. Barker, Tyson: 2021 Is the Year the Internet Gets Rewritten, in: Foreign Policy, 19.01.2021, https://foreignpolicy.com/2021/01/19/2021-is-the-year-the-internet-gets-rewritten/

Kämpfer gegen eine Art »dunkle Aufklärung«, die von einer pervertierten Anreizstruktur angetrieben wird: Mit emotional aufgeladenen Inhalten wird eine Nutzung gefördert, die abhängig macht und so ihrerseits die massenhafte Datensammlung zwecks gezielter Werbung befeuern soll. Zusammengenommen entstehen auf diese Weise Netzwerkeffekte, die es Big-Tech-Plattformen ermöglichen, zu mächtigen Online-Gatekeepern zu werden.[9]

Aber die Bemühungen gehen weiter als nur bis zur Festlegung des Regelwerks. Im März 2021 stellte die Europäische Kommission ihren umfassenden Digitalen Kompass vor, »der die konkreten digitalen Ambitionen der EU für 2030 darlegt«. Der Digitale Kompass soll die europäischen Anstrengungen in verschiedensten Politikbereichen der Digitalisierung standardisieren. Die Themen reichen von Industrieprojekten zur Stärkung der industriellen Innovationsbasis der EU bis hin zur Schaffung eines digitalen Binnenmarktes. Die Staats- und Regierungschefs fordern konkrete Ziele bis 2030. So sollen beispielsweise alle EU-Haushalte über Gigabit-Internet-Anschlüsse verfügen. Alle bewohnten Regionen sollen mit 5G versorgt werden. Die EU will die Zahl der Einhorn-Startups, also der Start-ups mit einer Marktbewertung von über einer Milliarde US-Dollar, verdoppeln, den europäischen Anteil an der Produktion von High-End-Halbleitern von 10 auf 20 Prozent der weltweiten Kapazität erhöhen und 10.000 Edge-Computing-Knoten hinzufügen, um die nächste Welle der Cloud-Computing Anwendung und Europas Streben nach einer souveränen Cloud zu beschleunigen. Zum Digitalen Kompass soll auch ein Beaufsichtigungsprozess von Investition und Entwicklung gehören, der »permanent, wiederkehrend und auf einer breiten gesellschaftlichen, wissenschaftlichen und wirtschaftlichen Basis aufgebaut sein sollte«[10].

Innenpolitisch und innerhalb der EU sind die Kommission und die Mitgliedsstaaten dabei, die digitale Politik – und auch sich selbst – auf diese neue Ära vorzubereiten. Einige fordern, die geltende Regulierung komplett zu überarbeiten, also ein institutionell fokussiertes Regelwerk (verstaubte Behörden setzen verstaubte Gesetze um) in ein beziehungsbasiertes regulatorisches Ökosystem zu verwandeln. Ähnlich wie beim maschinellen Lernen soll

9 Vgl. Angela Merkel et al., Brief an Ursula von der Leyen, 01.03.2021, https://www.politico.eu/wp-content/uploads/2021/03/01/DE-DK-FI-EE-Letter-to-COM-President-on-Digital-Sovereignty_final.pdf

10 Angela Merkel et al., Brief an Ursula von der Leyen, 01.03.2021.

ein sogenannter »lernender Staat« entstehen.[11] Die EU beginnt bereits, solche neuen Managementmodelle für die Regulierung anzuwenden. Zum Beispiel zielt der Digital Services Act darauf ab, eine unabhängige Rechenschaftspflicht, Prüfung und Überwachung von Big-Tech-Plattformen zu schaffen, an der nicht nur Big Tech und Regulierungsbehörden beteiligt sind, sondern auch unabhängige Akteure, Akademiker*innen, vertrauenswürdige Hinweisgeber (*trusted flaggers*) und staatsferne Beratungs- und Entscheidungsgremien. So soll sichergestellt werden, dass die Big-Tech-Plattformen ihre eigenen Nutzungsbedingungen in Bezug auf hetzerische Inhalte und Desinformation auch durchsetzen.

In der Vergangenheit ging der Innovationsschub der industriellen Revolutionen mit einer Neuerfindung der Rolle des Staates einher; Sozialstaat, Gewerkschaften, Arbeitsgesetze, Produktsicherheitsstandards und neue internationale Organisationen entstanden. Der industrielle Kapitalismus des 19. Jahrhunderts war mit maschinenbezogenen, dauerhaften Technologien in den Fabrikhallen straff organisiert. Der Internet-Kapitalismus dagegen ist agil, vermittelnd und verhaltensorientiert. Seine Regulierung hat mit dieser Entwicklung aber nicht Schritt gehalten. Es ist eine Diskrepanz entstanden, die es den agilen Big-Tech-Unternehmen ermöglicht hat, diese Art der staatlichen und statischen Aufsicht zu umgehen. Die EU und die europäischen Demokratien müssen sich mit diesem Missverhältnis auseinandersetzen.

Was bedeutet das für die europäischen Demokratien im globalen Tech-Rennen?

Auch wenn Europa mit der Neuerfindung des Staates begonnen hat, gibt es eine weniger offensichtliche geoökonomische – und letztlich geopolitische – Dimension in den Digitalstrategien vieler europäischer Staaten. Die heutigen Architekten der Digitalpolitik in den einzelnen europäischen Demokratien dürfen die Notwendigkeit einer digitalen Gesamtstrategie nicht aus den Augen verlieren. Mithilfe einer sogenannten Digital Grand Strategy können sie ihre heimischen technologischen Fähigkeiten und Ziele mit internationalen Werten und Interessen verbinden. Letztlich werden Europas Bemühungen

11 Vgl. Nadine Schön, Thomas Heilmann, Jens Spahn: »Neustaat« – Für eine Reform der Politik, 02.06.2020, https://www.cducsu.de/themen/innen-recht-sport-und-ehrenamt/neustaat-fuer-eine-reform-der-politik

nur dann erfolgreich sein, wenn die EU in der Lage ist, eine selbstbewusste, leistungsstarke, europäische digitale Wirtschaft zu entwickeln, die in eine offene, demokratische, regelbasierte digitale Ordnung eingebettet ist.

Sich mit diesen Fragen auseinanderzusetzen, war noch nie so dringend wie heute. Zwei politische Realitäten haben Europas technologische Landschaft seit 2017 geprägt. Die erste, aus China kommende, ist der Aufstieg einer neuen Form von unerbittlicher technologischer Industriepolitik, die von einem autoritären Bedürfnis nach absoluter Kontrolle im eigenen Land und einer Mischung aus inländischem Protektionismus, Diebstahl von geistigem Eigentum, strategischen Investitionen, Regierungsplänen, brachialen Subventionen und einem nationalen Gefühl der gemeinsamen Mission angetrieben wird. Die zweite, aus den USA kommende Realität, ist die Bereitschaft der Trump-Regierung, technologische und wirtschaftliche Engpässe anderer Länder zu nutzen, um diese zu zwingen, sich den geopolitischen Zielen der USA zu beugen. Diese beiden Lektionen – das Streben nach größerer technologischer Autonomie im eigenen Land und die Ausnutzung gegenseitiger Abhängigkeiten als Waffe auf globaler Ebene – deuten auf ein härteres geotechnisches Umfeld hin, in dem das Risiko einer *Versicherheitlichung* und Fragmentierung des digitalen internationalen Systems hoch ist.

Wie andere Mächte ist auch die EU zunehmend ins Kreuzfeuer geraten und wird gezwungen, zwischen dem Zugang zum chinesischen Markt oder der Nutzung von US-Technologie zu wählen. Sich technologisch von China oder den USA abzukoppeln, ist für Europa keine Option. Aber da Europas Abhängigkeit von China wächst, könnte die Verflechtung der europäischen industriellen Basis mit der chinesischen, etwa bei der Verschmelzung von Systemen, die intelligente Städte, autonome Fahrzeuge und Produktionsprozesse steuern, zunehmen. Mit dem Wachstum ihrer technologischen Macht ist der Umgang der Kommunistischen Partei Chinas mit Technologie brachialer, unberechenbarer und ideologisch unvereinbar mit dem europäischen politischen System geworden. Europas Demokratien werden sich die Frage stellen müssen, inwieweit ihr technologisches Entgegenkommen gegenüber China letztlich dazu beitragen könnte, Chinas autoritäre Dominanz zu stärken.

Chinas relativer Aufstieg in der technologischen Wertschöpfungskette in den letzten zehn Jahren war ein disruptiver Faktor im globalen Technologie-Ökosystem. Die von der Kommunistischen Partei Chinas propagierte Verschmelzung von Staat und Unternehmen zu einer vertikalen Organisation nimmt verschiedene Formen an, von staatseigenen Unternehmen über Vor-

standsstrukturen bis hin zu rechtlichen Zugriffsmöglichkeiten auf alle »wichtigen Daten«. Gepaart mit massiven nationalen und lokalen Staatsinvestitionen, staatlich begünstigten Unternehmen, erzwungenen Joint Ventures und der gemeinsamen Nutzung von technologischem Wissen, das auch durch staatlich unterstützte oder instruierte Industriespionage gesammelt wurde, veredeln Nachahmerfirmen im eigenen Land dieses Know-how. Diese Co-Abhängigkeit vom Staat und von der Kommunistischen Partei Chinas als unangefochtenem Seniorpartner ist ein charakteristisches Merkmal des chinesischen Technologiesektors und wurde zum Maßstab für seine Expansion in Bereichen wie Telekommunikationshardware, Mobiltelefonie, Fintech, E-Commerce, soziale Medien und Internet of Things. Dieser Zusammenschluss hat andere Großmächte, insbesondere die USA, aber auch Großbritannien, Kanada, Japan, Südkorea sowie die EU, dazu veranlasst, den Zugang zu und die Kontrolle über Schlüsseltechnologien zu überdenken.

Jenseits des Atlantiks spielen die USA immer noch eine wichtige Rolle als Sicherheits- und Technologie-Garant für Europa. Auch wenn die Biden-Administration ein neues Angebot für eine enge transatlantische Zusammenarbeit und die Stärkung des Multilateralismus unterbreitet hat, haben die Nachwirkungen der Snowden-Enthüllungen (2013), der Trump-Wahl (2016), von Cambridge Analytica (2018) und der allgemeinen Verschlechterung der amerikanischen Demokratie zu einem berechtigten europäischen Bedürfnis geführt, sich nach verschiedenen Seiten abzusichern. Die jüngste Zeit ist jedoch durch ein strukturelles Ungleichgewicht in Europas Tech-Politik gekennzeichnet, das in erster Linie durch die Bedrohungswahrnehmung der amerikanischen Tech-Dominanz definiert wurde und weniger durch die zunehmende Rolle Chinas als digitaler Akteur oder die ideologischen Auseinandersetzungen zwischen demokratischen und autoritären Visionen vom digitalen Raum.

Europa muss deutlich machen, dass ein äquivalent großer Abstand zu China und zu den USA (Äquidistanz) keine Option ist. Im Kampf um den Schutz der Grundrechte, die Einhaltung des Völkerrechts beim Schutz des geistigen Eigentums, von Cybersicherheit und der demokratischen Ausgestaltung von Technologien müssen die EU und ihre Mitgliedsstaaten an der Seite gleichgesinnter Akteure stehen, einschließlich der USA. Gleichzeitig muss sich Europa aber auch gegen Schwachstellen wappnen, die durch den immer härter werdenden, technologischen Wettbewerb zwischen den USA und China zustande kommen. Und es muss sicherstellen, dass die beschlossenen Maßnahmen ausreichen, um die Aushöhlung der Wertschöp-

fungspotenziale in Europas Industrien zu verhindern: Ein hoher Anspruch angesichts der Bedeutung der Industrie für Europas Stärke und der sich verändernden Natur von Technologie und Produktion.

Europas Vorbereitungen für den großen Wurf

Vor diesem Hintergrund ist die Wettbewerbsfähigkeit Europas, die industrielle Basis der EU und das Fundament ihrer globalen Macht, unter Druck geraten. Der Zugang zu und die Kontrolle über Plattformen, Datenpools, Cloud- und Internet-Infrastrukturen, hochentwickelte Algorithmen wie KI, Quantentechnologie und fortschreitende Mikroelektronik werden zu zentralen Elementen wirtschaftlicher, strategischer und demokratischer Macht und Verwundbarkeit. Die Fähigkeiten und die Raffinesse, grundlegende Technologien in klassische Produkte und Dienstleistungen zu integrieren, definieren zunehmend innovatorischen Erfolg. Alteingesessene Sektoren wie die Automobilindustrie, Haushaltsgeräte- und Maschinenbau, die industrielle Fertigung in der Chemie und Pharmazie – mit anderen Worten: das Herz der europäischen Industrie – basieren zunehmend auf Software, dienstleistungsbasierten Systemen und Datenverarbeitung. Daher müssen Europas traditionelle Unternehmen zu Tech-Unternehmen werden. Sie stehen dabei in einem harten Wettbewerb mit amerikanischen und chinesischen Tech-Konkurrenten. Der Wettstreit um die technologische Führung wird verstärkt auf industriellem Terrain ausgetragen, das Europa lange Zeit dominiert hat, in dem es aber zunehmend an Vorteil verliert. Wie die Europäische Kommission selbstkritisch festgestellt hat: »The EU trajectory is not catching up with that of its key competitors, notably China and the US, accelerating far more sharply since 2017.«[12]

Das wichtigste Element, um in diesem Wettlauf zu bestehen, ist Ursula von der Leyens Versprechen der »Digitalen Dekade«. Massive finanzielle Investitionen sollen zur Verfügung gestellt werden, um europäische Technologie- und Digitalisierungsprojekte zu finanzieren. 20 Prozent des 672,5 Milliarden Euro schweren Pakets zur Aufbau- und Resilienzfazilität der EU sollen dafür verwendet werden, den Kontinent für das digitale Zeitalter

12 European Commission: Communication on a Europe's digital decade: 2030 digital targets, 10.02.2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AAres%282021%29152850&qid=1617291312020

fit zu machen. Die ehrgeizigen Tech-Kommissare Margrethe Vestager und Thierry Breton sind bereits dabei, die Industriepolitik der EU zu aktualisieren. Frankreich, Deutschland und die EU haben gemeinsam eine Phalanx neuer Projekte zu 5G-Netzwerkinfrastrukturen, Halbleitern, Cloud und Daten, Wasserstoff und Batterien angedeutet. Wie andere fortschrittliche Industriemächte hat Europa die Überwindung der Corona-Krise mit dem Bestreben verbunden, seine industrielle Basis zu erneuern. Die europäischen Demokratien haben umfangreiche Investitionen in aufstrebende Technologien zugesagt, insbesondere in künstliche Intelligenz, Hochleistungscomputer und Quantencomputer, und bauen Technologie-Innovationscluster wie das baden-württembergische Cyber Valley für KI und maschinelles Lernen auf.[13]

In Europa werden die Rufe nach einer Rückeroberung der »digitalen Souveränität«[14] durch die EU entsprechend immer lauter. Doch die genaue Ausrichtung der »digitalen Souveränität« ist umstritten. Sie spiegelt die wechselnden Positionen, Interessen und Weltanschauungen wider, die die Ziele bestimmen. Handelt es sich um einen Aufruf zur Wiederherstellung der informationellen Selbstbestimmung der Nutzer*innen, zur Förderung von mehr Wettbewerb, zur Festlegung klarer, menschenzentrierter digitaler Regeln und zur Aufrechterhaltung offener Märkte? Oder ist es ein Vorstoß für eine Art *Techno-Gaullismus*, in dem Europa seine eigenen Tech-Champions schafft? Kann es wirklich beides sein?

Drei strategische Entscheidungen/ Drei Wege in die digitale Zukunft Europas

Die verschiedenen genannten Initiativen sind für die digitale Souveränität Europas von Bedeutung und können zusammen dazu beitragen, dass Europa die globale digitale Ordnung mitgestaltet. Aber hierin liegt bereits das zentrale Paradox. Die Vielzahl der Herausforderungen vernebelt ein klares strategisches Narrativ. So erscheint die Technologiepolitik der demokratischen Staaten unausgewogen und manchmal sogar hilflos. Wenn alles oberste Priorität hat, hat nichts mehr Priorität. Aus diesem Grund müssen die europäischen Demokratien einen ausbalancierten Ansatz in der internationalen

13 Vgl. Max-Planck-Gesellschaft: Ein Schub für die künstliche Intelligenz, 17.12.2020, https://www.mpg.de/16192562/kuenstliche-intelligenz-ai-breakthrough-hub

14 Siehe hierzu auch den Beitrag von Julia Pohle und Thorsten Thiel in diesem Band.

Tech-Diplomatie finden und klare Prioritäten setzen. Dazu müssen drei strategische Entscheidungen getroffen werden.

Eine Werte-Technologie-Fusion schaffen

Erstens: Wie kann Europa zur treibenden Kraft hinter einer Fusion von Werten und Technologie werden, die Menschenwürde und Nachhaltigkeit fördert? Weltweit haben Technologieunternehmen, Regierungen, internationale Organisationen und die Zivilgesellschaft die letzten Jahre damit verbracht, über die Ethik der Technologie – insbesondere der künstlichen Intelligenz – zu diskutieren. Dabei haben sie es versäumt, den Schwerpunkt darauf zu legen, diese Ethik bereits in den Design-Spezifikationen der neuen Technologien zu kodifizieren und zu implementieren. Das kann beispielsweise bedeuten, internationale Leitplanken zu schaffen, die die potenziell *orwellsche Reichweite* digitaler Technologien begrenzen. Dazu gehören Bestimmungen gegen algorithmische Diskriminierungen, der Vorrang menschlicher Entscheidungen sowie das Verbot von Profiling und die Verwendung von Stimm-, Gesichts- oder gar neuronaler Daten für bestimmte Anwendungen.

Europas Demokratien müssen abwägen, wie sie ihre politische und ökonomische Macht am besten nutzen können, um globale Regelwerke mit Partnern wie den USA, Japan, Südkorea und vielleicht subnationalen staatlichen Akteuren wie Kalifornien festzulegen. Die demokratischen Staaten sollten neue Bestrebungen unterstützen, die auf eine Charta der digitalen Rechte sowohl im Inland als auch in einem Multi-Stakeholder-Kontext weltweit drängen. Das bedeutet aber auch, das technologische Design von Beginn an an diesen Werten auszurichten. Sie sollten diese Verschmelzung auch für innovative Technologien zur Bekämpfung des Klimawandels ausweiten. Eine Rolle, die die »digitale Dekade« der EU bereits hervorhebt. Europa kann eine führende Rolle bei der internationalen Förderung neuer Technologien zur Bekämpfung von Kohlenstoffemissionen einnehmen, so wie es dies bei Solar- und Windtechnologien getan hat.

Die globale Rolle der EU als Regelsetzer ist ihr offensichtlichster und stärkster Hebel, insbesondere bei Normierungen und der Festlegung technischer Standards. So war Frankreich federführend bei der Gründung der Global Partnership on AI der OECD und des Paris Call for Stability in Cyber Space. Die EU-Mitgliedsstaaten führten nacheinander den Vorsitz bei den letzten drei Treffen des Internet Governance Forums (IGF), einem wich-

tigen Agenda-Setting-Gremium.[15] Die EU hat sich in der Vergangenheit gemeinsam mit gleichgesinnten Staaten wie den USA für den Schutz des Multi-Stakeholder-Systems der Internet-Verwaltung eingesetzt. Die EU spielt auch eine führende Rolle in der Internet Engineering Taskforce (IETF), demjenigen Standardisierungsgremium, das für die Internet-Protokollsuite (TCP/IP) verantwortlich ist. 42,5 Prozent der IETF-Dokumente sind von europäischen Autor*innen oder Co-Autor*innen (mit)verfasst – deutlich mehr als China (8,4 Prozent), aber weniger als die Vereinigten Staaten (72,98 Prozent).[16] Deutschland und Frankreich sind zwei von sechs ständigen Mitgliedern der International Standards Organization (ISO), dem Gremium, das für die technischen Standards vieler IKT-Produkte und -Dienstleistungen verantwortlich ist. Deutschland allein hält 18 Prozent der ISO-Sekretariate, 19 Prozent der IEC-Sekretariate und 29 Prozent der IEC-Vorsitze, und damit mehr als jedes andere Land. Deutschland und Europa bleiben die normsetzende Supermacht, was zum Teil auf ihre Kapazitäten und die Beherrschung der Prozesse in den oben genannten Institutionen zurückzuführen ist.

Europas Krise der technischen Abhängigkeit durch Offenheit und Resilienz lösen

Zweitens: Wie kann Europa Offenheit und Resilienz als doppelte Grundlagen seiner internationalen Digitalpolitik stärken? Als mächtiger Akteur entlang der globalen Lieferketten hat Europa sowohl zu einem offenen System beigetragen als auch davon profitiert. Das betrifft den freien Fluss von Daten, Diensten, Hardware und Wissen. Daher sind die Abhängigkeit von geopolitischen Hotspots, die Fragmentierung des Internets oder das Streben nach souveräner Ende-zu-Ende-Kontrolle von Basistechnologien eine direkte Bedrohung für Europa. So muss beispielsweise die weltweite Tendenz zur Datenlokalisierung die EU beunruhigen. Sollte die Welt in einen *Daten-Merkantilismus* verfallen, würde dies für Europa – mit seinem derzeitigen Datenmangel und abgeschnitten von den umfangreichen US-amerikanischen oder chinesischen Datenpools – einen massiven Nachteil bedeuten, gerade wenn es versucht, sich zu einer Macht auf dem Gebiet der vernetzten Industrien und des Internets der Dinge zu entwickeln.

15 Vgl. https ://pariscall.international/en/

16 Vgl. Authorstats: Distribution of Documents According to the Countries of their Authors, 31.03.2021, https://www.arkko.com/tools/allstats/d-countryeudistr.html

Vielmehr gilt es, bei den vorhandenen Fähigkeiten anzusetzen. Die EU und ihre Mitgliedsstaaten vereinen immense und unterschätzte Stärken in aufstrebenden Technologien und dominieren mehrere Schlüsselbereiche des digitalen Marktes. Sie sollten die Sicherung ihrer etablierten Kompetenzen ausbauen. Zum Beispiel ist Europa weltweit führend bei Industrie- und Logistikplattformen, Robotik und dem Internet der Dinge. Dagegen spielt Europa bisher in der fortschrittlichen Halbleiterproduktion eine untergeordnete Rolle. Ohne sogenannte EUV-Lithografie zur Herstellung effizienterer Chips werden die autonomen Fahrzeuge, 5G-Technologie und Industrie 4.0 nicht vorangetrieben werden können. Ohne den niederländischen Halbleiter-Lithografie-Ausrüster ASML und die deutschen Optik-Spezialisten Trumpf und Zeiss wird das unmöglich.[17]

Trotz all der versteckten Stärken und sogar der Größe Europas macht es die Struktur seiner industriellen Basis schwierig, den amerikanischen oder chinesischen Ansatz zu replizieren. Vielmehr sollte Europa globale Tech-Beziehungen fördern, die eine Abhängigkeit von einzelnen Anbietern vermeiden – sei es in Form von Gatekeeper-Plattformen, 5G-Technologien oder Chips. In Bezug auf die Datenverwaltung bedeutet dies, Interoperabilität, Portabilität und Nutzer*innenkontrolle von Daten durchzusetzen, damit diese zwischen Anbietern wechseln und innerhalb der Grenzen bewegen können. Europa sollte die Verantwortlichkeiten erweitern und Daten als ein öffentliches Gut behandeln. Bei Geräten und Software bedeutet dies größere politische und finanzielle Investitionen in Open-Source-Technologie für Netzwerkkomponenten und Halbleiter.

Die technologische Resilienz der EU und ihrer Mitgliedsstaaten sowie deren Fähigkeit, Werte zu schaffen, werden dadurch gekennzeichnet sein, dass sie Prioritäten setzen und Bereiche auswählen, die sie dominieren werden, und solche, zu denen sie Bedingungen aushandeln. Mit technologischen Eigenentwicklungen kann sich die EU von risikoreichen Schwachstellen emanzipieren. Die Entwicklung von Open-Source-Software wie O-RAN, einer interoperablen Basis für 5G-Geräte, könnte helfen, das Monopol des chinesischen Tech-Giganten Huawei und dreier anderer Akteure auf dem

17 ZEISS, TRUMPF und Fraunhofer-Forscherteam erhalten den Deutschen Zukunftspreis 2020 für die Entwicklung der EUV-Lithographie, 25.11.2021, https://www.zeiss.com/semiconductor-manufacturing-technology/news-events/press-releases/2020/zeiss-trumpf-and-fraunhofer-research-team-awarded-the-deutscher-zukunftspreis-.html

Gebiet der 5G-Infrastruktur zu brechen. GAIA-X, ein föderierter europäischer Cloud-Standard, zielt darauf ab, mehr Wettbewerb, Datenportabilität und Nutzer*innenkontrolle zu schaffen. Andere könnten entstehen – zum Beispiel in Zusammenarbeit mit den USA bei der Entwicklung der High-End-Chip-Fertigung, die Europas Ökosystem von Halbleiterwerken in ein globales Chip-Konsortium innerhalb des euro-atlantischen Raums einbringt.

Technologischer Vorsprung hängt von Ökosystemen ab, die langlebig sind und weder schnell aufgebaut noch zerstört werden können. Das gilt auch für die USA, die in der Computerindustrie und im Cloud-Computing vorherrschend sind. Aus diesem Grund widmet sich China seit mehr als einem Jahrzehnt groß angelegten Industrialisierungsprojekten, um einheimische Technologiekapazitäten zu schaffen, und ist dabei in Bereichen wie mobile Geräte, soziale Medien und E-Payment-Systeme erfolgreich, sieht sich aber in anderen Bereichen wie der modernen Halbleiterproduktion mit Schwierigkeiten konfrontiert. Die EU und ihre Mitgliedsstaaten müssen gewissenhaft definieren, wo technologische Eigenständigkeit notwendig ist und wo alternativ Strategien zur Schadensbegrenzung, welche Interdependenz und Resilienz erzwingen, besser geeignet sind.

Dazu wird auch eine ehrliche Bewertung der Industriepolitik innerhalb des EU-Rahmens nötig sein. Die Mitgliedsstaaten ziehen es immer noch vor, Technologiebranchen innerhalb ihrer eigenen nationalen Grenzen zu fördern. Schwieriger ist es, eine Innovation außerhalb der eigenen Landesgrenzen zu finanzieren. So stellt sich beispielsweise die Frage, wie Deutschland die deutschen Steuerzahler*innen am besten davon überzeugen kann, dass es sich lohnt, im Namen der europäischen digitalen Souveränität Milliarden für die Unterstützung von Quantenfähigkeiten in Frankreich oder KI in Italien auszugeben.

Regeln mit globalem Anspruch durchsetzen

Drittens: Wie kann Europa seine Fähigkeit, die globalen Regeln der Tech-Governance zu gestalten, durch Konsequenzen ergänzen, die greifen, wenn diese Regeln verletzt werden? Europa spielt eine wichtige Rolle bei der Gestaltung des globalen regulatorischen und normativen Rahmens. Die EU konnte eine Technologiepolitik auf nationaler Ebene entwickeln, zunächst beim Schutz persönlicher Daten und aktuell bei der Bekämpfung illegaler Online-Inhalte oder hinsichtlich KI und Cloud Computing. Und sie hat diese Regeln

dann erfolgreich auf europäischer Ebene kodifiziert. Viele dieser Initiativen sind zu *Goldstandards* für die globale Tech-Regulierung geworden.

Aber Verstöße gegen diese Regeln – sei es in Form von Techno-Autoritarismus wie dem KI-gesteuerten Panoptikum von Xinjiang, Diebstahl von geistigem Eigentum, Cyberangriffen und anderen aktiven Maßnahmen – wurden von Europa oder gleichgesinnten Ländern nicht mit der notwendigen Konsequenz beantwortet. Autoritäre Staaten– wie China, Russland und ihre Partner – wurden nicht rechtzeitig mit angemessenen Maßnahmen konfrontiert. Dazu gehören entsprechende Sanktionen, Exportkontrollen, der Ausschluss vom europäischen Markt, der Ausschluss aus der europäischen Universitäts- und Forschungslandschaft sowie aus Gremien zur Festlegung technischer Standards. Selbst in einem so banalen Bereich wie der digitalen Besteuerung ist die Fähigkeit der EU und ihrer Mitgliedsstaaten, Unternehmen – insbesondere Big-Tech-Unternehmen wie Amazon und Apple – zur Steuerzahlung zu zwingen, an Lobbyarbeit und festgefahrenen Governance-Diskussionen auf OECD- und EU-Ebene gescheitert. Dabei sind bereits zahlreiche geoökonomische Maßnahmen festgeschrieben. Sie reichen von einem EU-weiten Sanktionsinstrumentarium für Cyberangriffe bis hin zu einer Höchststrafe gegen Unternehmen von bis zu 4 Prozent ihres weltweiten Jahresumsatzes bei Verstößen gegen die Datenschutz-Grundverordnung. Aber diese Instrumente wurden noch nie in einer Weise eingesetzt, dass sie zukünftige Verstöße verhindert hätten.

Das bedeutet auch, dass die EU, die europäischen Demokratien und gleichgesinnte Staaten das kollektive Kampfgewicht der Marktgröße, des Marktzugangs und ihrer industriellen Basis nutzen müssen. Sie müssen ihre *Offenheit untermauern*, indem sie Regeln, Werte, Wechselseitigkeit und Zugang als sich gegenseitig verstärkende Instrumente zur Gestaltung eines demokratischen Technologieraums miteinander verbinden. Die OECD-Länder machen rund 50 Prozent des globalen BIP aus; die EU und die USA allein repräsentieren 42 Prozent des globalen BIP und 41 Prozent des globalen Handels.[18] Europa kann neue multilaterale und stärker normative Mechanismen und Ziele in Betracht ziehen, um eine strategisch solide Basis für die Nutzung der kombinierten Marktmacht der EU, der USA, Großbritanniens, Japans und

18 Vgl. Burwell, Frances G.: Engaging Europe: A Transatlantic Digital Agenda for the Biden Administration, in: Atlantic Council, Dezember 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/12/A-Transatlantic-Digital-Agenda-for-the-Biden-Administration.pdf

anderer gleichgesinnter Staaten zu schaffen. Zu den Bemühungen könnte die Angleichung von technologischen und digitalen Marktzugangsinstrumenten gehören, wie Investitionsprüfung, Exportkontrollen, Nutzung geschützten Wissens, Kooperation bei Forschung und Entwicklung und akademische Zusammenarbeit im Dienste von Demokratie, Menschenrechten und wirtschaftlicher Sicherheit. Ein Vorschlag lautet, dass gleichgesinnte Länder ein Koordinationskomitee für multilaterale Exportkontrollen (CoCom)[19] für das 21. Jahrhundert gründen, um den Zugang zu strategischer Technologie für autoritäre Staaten zu beschränken. Europa muss bereit sein, kollektive Maßnahmen zu ergreifen, um Regeln und Konsequenzen als abschreckendes Element durchzusetzen.

Was ist die Killer-App der europäischen Technologiepolitik?

Und schließlich: Wie können die europäischen Demokratien sich mit ihrem Technologieansatz zentral zwischen ihren Partnern positionieren? Die globale Wettbewerbsfähigkeit und Sicherheit Europas wird davon abhängen, den Zugang zu und die Kontrolle über Schlüsseltechnologien wie KI, 5G-Technologie und Halbleiter aufrechtzuerhalten. Digitale Souveränität als merkantilische Abschottung wird wahrscheinlich nicht erfolgreich sein.

Ein alternativer Ansatz wäre der Aufbau von Resilienz durch starke Allianzen, die auf dem Bekenntnis zu gemeinsamen demokratischen Normen und Werten beruhen. Durch den Zusammenschluss mit gleichgesinnten Akteuren bietet sich die Möglichkeit, Schwachstellen zu reduzieren und die Handlungsfähigkeit Europas voranzutreiben. Der Zugang und die Kontrolle über diese Schlüsseltechnologien müssen durch eine Tech-Diplomatie in der gesamten demokratischen Welt erreicht werden, die europäische Werte wie Offenheit, Regeltreue und gezielte Unterstützung von Innovationsunternehmen stärkt.

Hier hat Europa einen Vorteil. Seine geopolitische Stärke resultiert aus seiner Vernetzung. Europas Demokratien sind geopolitisch überdurchschnittlich erfolgreich. Das verdanken sie den Bündnissen, denen sie angehören, allen voran der EU und dem transatlantischen Bündnis, sowie

19 Vgl. Sikorski, Radek: Making the World Great Again: Europe, the United States and China, in: Lisbon Council, January 2021, https://lisboncouncil.net/making-the-world-great-again-europe-the-united-states-and-china/

ihrer Einbettung in die Weltwirtschaft. Europas langjährige Fähigkeit, sich als geeinte Macht in die Mitte des internationalen Systems zu stellen, ist seit langem seine »Killer-App« im Weltgeschehen.

Damit eine europäische digitale Gesamtstrategie Erfolg hat, müssen die EU und die europäischen Demokratien geoökonomische Bündnisse mit gleichgesinnten Staaten vertiefen, um die Regeln für Daten, Algorithmen und Lieferketten mit Zugang zu Märkten, Investitionen und Wissen als Anreiz dafür zu schaffen, eine regelbasierte digitale Ordnung zu entwickeln. Indem sie ein weit verzweigtes Netzwerk von Tech-Allianzen aufbauen, das sich um die EU, das euro-atlantische Bündnis und den breiteren demokratischen Raum gruppiert, können sich die europäischen Staaten am besten positionieren, um diese neue digitale Ära zu meistern.

Bereits 1999 behauptete Lawrence Lessig »Code is Law«[20], also dass Programmierer Wertesysteme in Technologien einschreiben. Über 20 Jahre später lebt Europa in der geopolitischen Landschaft, die diese Wegbereiter geschaffen haben. Einstige Start-ups haben sich zu Super-Giganten entwickelt, die immer mehr Daten und Marktanteile an sich reißen. Heute ist Code mehr denn je Macht. Diese Macht wieder an ein werte- und rechtebasiertes System zu binden, das sich am Gemeinwohl orientiert, könnte der größte Beitrag Europas zum digitalen Zeitalter sein.[21] [22]

20 Lessig, Lawrence: Code and other laws of cyberspace, New York: Basic Books 1999.

21 Vgl.Schaake, Marietje und Tyson Barker: Democratic Source Code, https://www.lawfareblog.com/democratic-source-code-new-us-eu-tech-alliance

22 Übersetzung aus dem Englischen Chris Piallat

Autor*innenverzeichnis

Tyson Barker ist seit 2020 bei der Deutschen Gesellschaft für Auswärtige Programmleiter für Technologie und Außenpolitik. Zuvor arbeitete er beim Aspen-Institut Deutschland als stellvertretender Executive Direktor und war Fellow. Davor war er u.a. als Senior Advisor im Büro für Europäische und Eurasische Beziehungen im US-Außenministerium und als Direktor für transatlantische Beziehungen bei der Bertelsmann Stiftung tätig. Zudem veröffentlicht er auf beiden Seiten des Atlantiks u.a. für Foreign Affairs, Foreign Policy, Politico, The Atlantic, The National Interest und Der Spiegel.

Dr. Ulf Buermeyer (LL.M. [Columbia]) ist Vorsitzender der Gesellschaft für Freiheitsrechte, eines gemeinnützigen Vereins, der mittels strategisch geführter Gerichtsverfahren Grund- und Menschenrechte verteidigt. Gemeinsam mit dem Journalisten Philip Banse gestaltet er den Politik-Podcast »Lage der Nation«. Von seinem Amt als Richter des Landes Berlin ist er derzeit beurlaubt. Die Schwerpunkte seiner wissenschaftlichen Arbeit liegen im Verfassungsrecht, insbesondere im Bereich der Telekommunikationsfreiheiten und der informationellen Selbstbestimmung.

Prof. Dr. Petra Grimm ist seit 1998 Professorin für Medienforschung und Kommunikationswissenschaft an der Hochschule der Medien Stuttgart. Sie ist Leiterin des Instituts für Digitale Ethik und Ethikbeauftragte der Hochschule der Medien. Ihre Forschungsschwerpunkte sind »Digitalisierung der Gesellschaft«, »Ethics by Design«, »Narrative Ethik« und »Narratologie«.

Dr. Stefan Heumann ist Politikwissenschaftler und Mitglied des Vorstands der Stiftung Neue Verantwortung (SNV) e.V., die er in den vergangenen Jahren zum Think Tank für die Gesellschaft im technologischen Wandel weiter-

entwickelt hat. Er arbeitet, spricht und schreibt zu Themen der nationalen und internationalen Digitalpolitik.

Prof. Eric Hilgendorf studierte in Tübingen Rechtswissenschaften, Neuere Geschichte und Philosophie. Seit 2001 ist er Professor für Strafrecht, Informationsrecht und Rechtstheorie an der Universität Würzburg. Zu seinen Hauptarbeitsgebieten gehören das Technikrecht und die Technikregulierung. Hilgendorf war Mitglied der EU High Level Expert Group on AI. Er ist heute Direktor am Bayerischen Forschungsinstitut für Digitale Transformation (bidt) und Mitglied des Bayerischen KI-Rats.

Lorena Jaume-Palasí forscht zur Ethik der Digitalisierung und Automatisierung und in diesem Zusammenhang zur Fragen der Rechtsphilosophie. Sie wurde 2020 in den nationalen Rat für künstliche Intelligenz der Regierung Spaniens berufen und ist Mitglied des internationalen Beirats des STOA Panels des Europäischen Parlaments. 2018 wurde sie mit der Theodor-Heuss-Medaille für die Initiative AlgorithmWatch ausgezeichnet.

Dr. Matthias C. Kettemann (LL.M. [Harvard]) ist Forschungsprogrammleiter am Leibniz-Institut für Medienforschung am Hans-Bredow-Institut und Forschungsgruppenleiter am Humboldt-Institut für Internet und Gesellschaft und dem Sustainable Computing Lab der WU Wien.

Julia Kloiber ist Mitgründerin der gemeinnützigen Organisation Superrr Lab. Sie hat eine Reihe von Initiativen im Bereich Technologie und Gesellschaft gegründet, darunter den Prototype Fund, ein öffentlicher Fund für Public Interest Tech und das Netzwerk Code for Germany. Sie ist Fellow der Mozilla Foundation, berät die Wikimedia im Beirat Offene Wissenschaft und ist im Aufsichtsrat von Digital Service 4 Germany tätig.

Nils Leopold (LL.M. [Rechtsinformatik]) arbeitet im Grundsatzreferat des Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI). Beruflich war er zuvor als Rechtsanwalt, als betrieblicher Datenschutzbeauftragter, als Geschäftsführer einer Bürgerrechtsorganisation, als Leiter Aufsicht über die Privatwirtschaft beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein tätig und hat sich als Referent der Bundestagsfraktion Bündnis 90/Die Grünen mit Datenschutzfragen befasst.

Elisa Lindinger ist ausgebildete Archäologin und arbeitet an der Schnittstelle von Technologie, Kunst und Geisteswissenschaften. Sie ist Mitbegründerin des Superrr Lab. In ihrer Forschung konzentriert sie sich auf Fragen rund um eine gerechte Digitalisierung, die digitale Zivilgesellschaft und die sozialen Auswirkungen neuer Technologien.

Sebastian Müller ist seit 2020 wissenschaftlicher Mitarbeiter am Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health der Universität zu Köln. Dort betreut er den Themenschwerpunkt Gesundheit und Digitalisierung. Seine Forschungsschwerpunkte liegen in den Bereichen Sozialphilosophie, Wirtschaftsphilosophie, Wirtschaftsethik, politische Philosophie und Medizinethik.

Chris Piallat ist seit 2012 Referent für Digital- und Netzpolitik der Bundestagsfraktion Bündnis 90/Die Grünen. Er arbeitet zu allen gesellschaftspolitischen Fragen der Digitalisierung. Neben seiner politischen Beratung arbeitet er als Autor, Redakteur und Sprecher u.a. für die Kulturstiftung des Bundes, die Berliner Gazette und die Heinrich-Böll-Stiftung. Er hat Politikwissenschaften an der Freien Universität Berlin, der Rutgers University (USA) und der Universität Kassel studiert.

Dominik Piétron ist wissenschaftlicher Mitarbeiter am Lehrstuhl »Soziologie der Zukunft der Arbeit« an der Humboldt-Universität zu Berlin. Arbeitsschwerpunkte: Politische Ökonomie des digitalen Kapitalismus, Europäische Datenpolitik, digitale Daseinsvorsorge.

Dr. Julia Pohle ist wissenschaftliche Mitarbeiterin in der Forschungsgruppe »Politik der Digitalisierung« am Wissenschaftszentrum Berlin (WZB). Sie forscht zu nationaler Netzpolitik und globalen Internet Governance-Prozessen.

Prof. Timo Rademacher ist Juniorprofessor für Öffentliches Recht und das Recht der neuen Technologien an der Universität Hannover sowie Mitglied der Jungen Akademie an der Berlin-Brandenburgischen Akademie der Wissenschaften. Er studierte Jura an den Universitäten Heidelberg, Ferrara und Oxford und wurde 2014 in Heidelberg mit einer Arbeit zum Recht der EU promoviert.

Prof. Tilman Santarius forscht und publiziert zu den Themen Klimapolitik, Handelspolitik, nachhaltiges Wirtschaften, globale Gerechtigkeit und digitale Transformation. Er lehrt an der Technischen Universität Berlin und am Einstein Centre Digital Futures und leitet eine Forschungsgruppe zum Thema »Digitalisierung und sozial-ökologische Transformation« am Institut für ökologische Wirtschaftsforschung (IÖW).

Dr. Erik Schilling lehrt Neuere deutsche Literatur und Vergleichende Literaturwissenschaft an der Ludwig-Maximilians-Universität München. Er hat in München, Pavia, Salamanca und Stanford studiert und in Harvard und Oxford geforscht. 2020 wurde er mit dem Heinz Maier-Leibnitz-Preis der DFG ausgezeichnet. Er ist Mitglied der Jungen Akademie an der Berlin-Brandenburgischen Akademie der Wissenschaften und der Leopoldina.

Francesca Schmidt hat 2020 ihr Buch »Netzpolitik. Eine feministische Einführung« veröffentlicht. Sie ist Gründungsmitglied und Vorständin von netzforma* e.V. – Verein für feministische Netzpolitik. Im Gunda-Werner-Institut für Feminismus und Geschlechterdemokratie ist sie Referentin für Feministische Netzpolitik. Sie beschäftigt sich mit digitaler Gewalt, Überwachung, und Künstlicher Intelligenz.

Dr. Nicole Shephard ist freie Sozialwissenschaftlerin, Consultant und Trainerin. Sie arbeitet an der Schnittstelle zwischen Gender und Technologie und beschäftigt sich aus intersektional feministischer Perspektive zum Beispiel mit digitaler Gewalt, Diversity und Inklusion im Technologiesektor oder Überwachung und Privatsphäre.

Malte Spitz ist Generalsekretär der Gesellschaft für Freiheitsrechte. Er veröffentlicht regelmäßig zu datenschutzpolitischen und digitalpolitischen Themen in nationalen und internationalen Medien und hat zwei Bücher dazu verfasst. Er lebt mit seiner Frau und seinen drei Kindern in Berlin. Politisch ist er seit fast 20 Jahren in unterschiedlichen Funktionen bei Bündnis 90/Die Grünen aktiv, seit 2013 als Parteiratsmitglied.

Prof. Dr. Philipp Staab ist Professor für die Soziologie der Zukunft der Arbeit an der Humboldt-Universität zu Berlin und am Einstein Center Digital Future (ECDF). Seine Arbeitsschwerpunkte liegen in den Bereichen Arbeits- und

Industriesoziologie, politische Ökonomie, Wirtschaftssoziologie und soziale Ungleichheit.

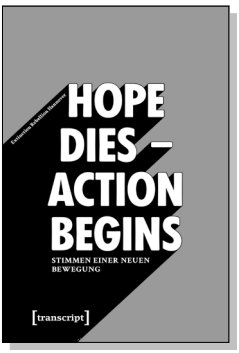
Prof. Christian Stöcker leitet an der HAW Hamburg den Master-Studiengang *Digitale Kommunikation* und mehrere Forschungsprojekte, die sich mit Fragen der Wechselwirkung von digitaler Medientechnologie und Öffentlichkeit befassen. Zuvor arbeitete er über 11 Jahre als Redakteur und Ressortleiter in der Redaktion von SPIEGEL ONLINE. Stöcker verfügt über Abschlüsse in Psychologie (Diplom) und Kulturkritik.

Dr. Thorsten Thiel ist Leiter der Forschungsgruppe »Demokratie und Digitalisierung« am Weizenbaum-Institut für die vernetzte Gesellschaft und wissenschaftlicher Mitarbeiter am Wissenschaftszentrum Berlin.

Dr. Ellen Ueberschär ist seit Juli 2017 Vorstand der Heinrich-Böll-Stiftung, gemeinsam mit Barbara Unmüßig. Sie ist verantwortlich für die Inlandsarbeit der Stiftung sowie für Außen- und Sicherheitspolitik, Europa und Nordamerika, die Türkei und Israel. Zudem verantwortet sie u.a. das Studienwerk, Green Campus, sowie das Querschnittsthema Digitalisierung. Sie ist promovierte Theologin.

Prof. Christiane Woopen ist Professorin für Ethik und Theorie der Medizin an der Universität zu Köln. Dort ist sie Direktorin des Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres). Sie war u.a. Vorsitzende des Deutschen Ethikrates (2012-2016), 2018 – 2019 Co-Sprecherin der Datenethikkommission der Bundesregierung und ist seit 2017 Vorsitzende des Europäischen Ethikrates (EGE).

Politikwissenschaft

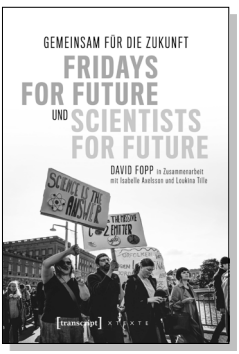


Extinction Rebellion Hannover
»Hope dies – Action begins«: Stimmen einer neuen Bewegung

2019, 96 S., kart.
7,99 € (DE), 978-3-8376-5070-9
E-Book: kostenlos erhältlich als Open-Access-Publikation, ISBN 978-3-8394-5070-3
EPUB: kostenlos erhältlich als Open-Access-Publikation, ISBN 978-3-7328-5070-9

Jan Brunner, Anna Dobelmann, Sarah Kirst, Louisa Prause (Hg.)
Wörterbuch Land- und Rohstoffkonflikte

2019, 326 S., kart., Dispersionsbindung, 1 SW-Abbildung
24,99 € (DE), 978-3-8376-4433-3
E-Book: 21,99 € (DE), ISBN 978-3-8394-4433-7



Angela Nagle
Die digitale Gegenrevolution
Online-Kulturkämpfe der Neuen Rechten von 4chan und Tumblr bis zur Alt-Right und Trump

2018, 148 S., kart.
19,99 € (DE), 978-3-8376-4397-8
E-Book: 17,99 € (DE), ISBN 978-3-8394-4397-2
EPUB: 17,99 € (DE), ISBN 978-3-7328-4397-8

Leseproben, weitere Informationen und Bestellmöglichkeiten finden Sie unter www.transcript-verlag.de

Politikwissenschaft

Sebastian Haunss, Moritz Sommer (Hg.)
Fridays for Future –
Die Jugend gegen den Klimawandel
Konturen der weltweiten Protestbewegung

2020, 264 S., kart.
22,00 € (DE), 978-3-8376-5347-2
E-Book: kostenlos erhältlich als Open-Access-Publikation
PDF: ISBN 978-3-8394-5347-6
ISBN 978-3-7328-5347-2

Helmut König
Lüge und Täuschung
in den Zeiten von Putin, Trump & Co.

2020, 360 S., kart., Dispersionsbindung
29,50 € (DE), 978-3-8376-5515-5
E-Book:
PDF: 26,99 € (DE), ISBN 978-3-8394-5515-9
EPUB: 26,99 € (DE), ISBN 978-3-7328-5515-5

BICC Bonn International Center for Conversion,
HSFK Leibniz-Institut Hessische Stiftung Friedens- und Konfliktforschung, IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg,
INEF Institut für Entwicklung und Frieden
Friedensgutachten 2020
Im Schatten der Pandemie: letzte Chance für Europa

2020, 160 S., kart., Dispersionsbindung, 33 Farbabbildungen
15,00 € (DE), 978-3-8376-5381-6
E-Book: kostenlos erhältlich als Open-Access-Publikation
PDF: ISBN 978-3-8394-5381-0

Leseproben, weitere Informationen und Bestellmöglichkeiten finden Sie unter www.transcript-verlag.de