



Digitale Selbstermächtigung. Hürden für Privatheit und Autonomie in einer algorithmisch konstruierten Wirklichkeit

Peter Biniok

Zusammenfassung

Digitalisierung und algorithmische Konstruktion der Gesellschaft orientieren sich (derzeit) einseitig vor allem an techno-ökonomischen und machtpolitischen Kriterien. Algorithmisierung und damit verbundene digitale Dynamiken verändern grundsätzliche Handlungs- und Strukturmuster, womit sich Fragen nach Privatheit und Autonomie der Nutzer:innen im Umgang mit Technik neu stellen. Im Beitrag werden Herausforderungen und Chancen digitaler Selbstermächtigung anhand von drei Dimensionen algorithmischer Konstruktion diskutiert: Algorithmen als Besitztümer, Algorithmen als Akteure und Algorithmen als Kontrollmittel. Sozial konstruierte Algorithmen agieren autonom, interagieren mit Nutzer:innen, sortieren und filtern für sie die Wirklichkeit, übernehmen gesellschaftliche Kontrollfunktionen. Selbstermächtigung im Bereich des Digitalen steht diesbezüglich nicht nur für eine Form der praktischen Befähigung, sondern schließt auch Reflexion und Bewertung des eigenen Handelns ein. Selbstermächtigung ist gleichzeitig an fremde Unterstützung gekoppelt und konstituiert sich in einem kollektiven Prozess.

Schlüsselwörter

Algorithmisierung • Souveränität • Digitale Bildung

P. Biniok (✉)

Kompetenzzentrum Innung SHK Berlin, Berlin, Deutschland

E-Mail: peter.biniok@freenet.de

© Der/die Autor(en) 2022

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz*, DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_17

345

1 Einleitung: Soziale Ordnung und Digitalisierung

Gesellschaft befindet sich in einem kontinuierlichen Wandlungsprozess, Technisierung und Digitalisierung eingeschlossen. Die fortwährende Dynamik zieht immer neue Ordnungsleistungen nach sich, damit gesellschaftliches Leben stabil bleibt.

1.1 Gesellschaftliche und technische Konstruktion der Wirklichkeit

Wie Gesellschaft möglich ist und *soziale Ordnung* entsteht und aufrechterhalten bleibt, durch wen und welche Mechanismen also welche Ordnungsleistungen auf welche Weise erbracht werden, wird in der Soziologie vielfältig diskutiert. In diesem Beitrag wird die Prämisse zugrunde gelegt, dass in erster Linie Individuen selbst die soziale Ordnung herstellen und gesellschaftliche Wirklichkeit konstruieren [1, 2]. Durch Interaktion und Kommunikation, d. h. vielfältige Kooperationen, Koordinationsaktivitäten, Aushandlungen usw. bringen Individuen in einem kollektiven Prozess die Gesellschaft in Form von Normen, Prozeduren und Organisationen hervor, die den Individuen als objektive Strukturen und Tatsachen gegenüberstehen und handlungsleitend wirken. Gesellschaft ist so gesehen eine Art *Handlungsstrom*, aus dem spezifische Handlungen in überdauernde Strukturen sedimentieren, die sich weniger langsam verändern als andere. Gemeinsam geteilte und für legitim erachtete Handlungsabläufe, Denkmuster und Wertvorstellungen werden zu Institutionen und bilden einen gesellschaftlichen Handlungsrahmen. Durch Sozialisation erwerben neue Gesellschaftsmitglieder das notwendige Wissen und integrieren sich anhand gesellschaftlicher Vorgaben. Zugleich wird die bestehende soziale Ordnung kontinuierlich hinterfragt und angesichts neuer Entwicklungen, auch technischer Art, reflektiert und verändert. Soziale und technische Veränderungen sind dabei eng miteinander verwoben und bedingen sich wechselseitig.

Neben der Institutionalisierung sozialer Strukturen erfolgt stets auch eine technische Institutionalisierung, also eine technische Konstruktion der Wirklichkeit [3]. Technische Abläufe und Verfahren verfestigen sich ebenso wie Handlungen und Interaktionsbeziehungen in gesellschaftlichen Strukturen, genauer in ‚*Technostrukturen*‘, und stehen den Individuen als objektivierte Gegebenheiten gegenüber. Technikaneignung und Umgang mit Technik wird entsprechend erlernt und folgt technostrukturellen Regulativen. Solche handlungsleitenden Institutionalisierungen sind DIN- und ISO-Normen, technologische Paradigmen (wie der

Verbrennungsmotor), oder dominante Designs (bspw. die QWERTY-Tastatur). Technische Institutionen begrenzen und regeln menschliches Handeln (so als Bestandteil der Verkehrstechnik: Ampeln, Schranken, Schilder) und eröffnen neue Handlungsoptionen, z. B. in Form von Experimentalsystemen (wie das CERN, die Europäische Organisation für Kernforschung). Der Beitrag fokussiert mithin, dem ‚Technopragmatismus‘ folgend, sich stetig wandelnde *soziotechnische* Konstellationen, bestehend aus Mensch und Technik. Insbesondere mit fortschreitender Technisierung kommen den technischen Instanzen immer mehr Handlungsträgerschaft und ein wachsender Anteil am Handlungsstrom zu.

1.2 Digitalisierung und algorithmische Konstruktion der Wirklichkeit

Digitalisierung ist eine *besondere* Form der Technisierung. Der symbolhafte Charakter der Technik bedingt eine neue Qualität im Unterschied zu analogen Werkzeugen und Maschinen. Digitale Technik ist größtenteils nicht sichtbar oder fassbar, oft nur indirekt zugänglich (Reaktionen und Auswirkungen sind vermittelt) und permanent existent mit zahlreichen Rückwirkungen und (unbeabsichtigten) Nebenfolgen. Der Bereich des Digitalen erschließt sich nicht wie bei anderen Techniken materiell-sinnlich. Stattdessen sind Nutzer:innen über Interfaces mit einer schwer nachvollziehbaren Welt aus Bits und Bytes verbunden. Der Zugriff auf diese ‚Blackbox(es)‘ [4, 5] ermöglicht neue Interaktions- und Kommunikationsweisen, die auf einem komplexen Geflecht von Algorithmen und Daten aufbauen. In der digitalen ‚Echtzeitgesellschaft‘ ergänzen sich die Handlungsströme von Mensch und Technik mit *Datenströmen* aus ständig aktualisierten Daten [6, 7]. Die mannigfaltigen Daten sind verknüpfbar und verfolgbar, sie hinterlassen „Spuren“ und bilden im Zeitverlauf ein für die Nutzer:innen intransparentes Referenzsystem.

Im Zuge von Digitalisierung entfalten sich neue Formen der Institutionalisierung, die im Anschluss an die vorstehenden Gedanken als *algorithmische Konstruktion* der Wirklichkeit gefasst werden. Neben gesellschaftliche Sozial- und Technostrukturen treten immer häufiger Algorithmenstrukturen, d. h. durch metrische Prozesse und kalkulatorisches Handeln etablierte und objektivierte Rahmenbedingungen sowie softwarebasierte Interaktions- und Kommunikationsformen. Dabei wird Technik immer stärker als mithandelnde Akteurin relevant. Software und *Algorithmen* bestimmen mehr und mehr soziales Miteinander. Die Herstellung sozialer Ordnung basiert somit zunehmend auf den Ergebnissen algorithmischer Prozesse und sich herausbildender digitaler Institutionen in

Form von Softwareanwendungen, aber auch als Hardware (Smartphone) und als digitale Praxen [8, 9]. Es bildet sich bspw. ein Kontext „des Surfens“, also der Aneignung und Nutzung digitaler Internettechniken heraus. Dieser konstituiert sich durch Technologiefirmen, deren Geräte und Applikationen sowie durch Regeln des digitalen Umgangs miteinander („Netiquette“). Normen und Werte menschlicher Kommunikation verändern sich (von E-Mail über Messenger-Dienste zu Instagram und TikTok), Gesetze werden angepasst und/oder erlassen (Datenschutz-Grundverordnung und ePrivacy-Verordnung), manche wirtschaftliche Organisationen verlieren an Bedeutung und Einfluss (etwa Netscape Communications und MySpace), während andere neu entstehen und den Markt dominieren, wie die sog. „Big Five“ Apple, Google, Microsoft, Facebook und Amazon.

Der institutionelle Kontext algorithmischer Strukturierung ist (noch) *fragil* und befindet sich in Aushandlung, da vielfältige Fragen bis heute nicht geklärt sind. Sind der Einsatz von Algorithmen und das Ergebnis algorithmischer Kalkulationen zu kennzeichnen? Bedarf es einer Kontrolle sozialer Plattformen und wie kann diese aussehen? Inwiefern hat Auskunft über die Verarbeitung personenbezogener Daten zu erfolgen? Wer trägt die Verantwortung in der algorithmischen Entscheidungsfindung? Es deutet sich an: Die algorithmische Konstruktion der Gesellschaft ist stark fragmentiert und schließt bislang nicht an die frühen Demokratieversprechen an [10, 11]. Digitales Leben vollzieht sich partiell (Onliner und Offliner), zensiert (gesperrte Webseiten, Unternehmens-Richtlinien), gefiltert (sowohl durch Algorithmen als auch durch Webseiten- und Profil-Inhaber:innen) und beschränkt bzw. vorstrukturiert (Vorgabe von Zeichenzahlen oder Umfang eines Anhangs). Auf diese Weise entstehen und/oder verstärken sich soziale Unterschiede, Exklusion und Intransparenz. Die Nutzung digitaler Technik birgt die Gefahr, emanzipatorische Potenziale zu verlieren. Die Macht des Digitalen, so die kritische Einstellung, symbolisiere einen ‚technologischen Totalitarismus‘ [12, 13].

1.3 Privatheit und Autonomie auf dem Prüfstand

Daraus leitet sich die These der folgenden Argumentation ab. Digitalisierung und algorithmische Konstruktion der Gesellschaft orientieren sich (derzeit) *einseitig* vor allem an techno-ökonomischen und machtpolitischen Kriterien. Gleichwohl finden sich auch Digitalisierungs- und Algorithmisierungsprozesse, die am Gemeinwohl orientiert sind und sich an den Belangen der Individuen und der Solidargemeinschaft ausrichten. Allerdings verlaufen diese Bemühungen eher im

Hintergrund und sind nicht die dominanten Strukturierungsmomente der digitalen Gesellschaft. Im Folgenden wird insofern eine *kritische* Perspektive auf die algorithmische Konstruktion der Wirklichkeit eingenommen. Damit ist keine immanent technikkritische Positionierung verbunden, die jeglichen Einsatz von Algorithmen und Künstlicher Intelligenz negativ beurteilt. Im Gegenteil sind zahlreiche Digitalisierungs- und Algorithmisierungsprozesse mit positiven Effekten, individuellem Empowerment und der Förderung von Gemeinschaft verbunden.

Allerdings ist es Ziel des Beitrags, auf gesellschaftliche Schieflagen hinzuweisen, die durch vorwiegend positiv konnotierten – auch im öffentlichen Diskurs – und unzureichend reflektierten Technikeinsatz hervorgerufen werden. Algorithmische Medien sind nicht neutral und Daten nicht objektiv. Algorithmisierung und damit verbundene digitale Dynamiken verändern grundsätzliche Handlungs- und Strukturmuster und ziehen problematische Verantwortungsverschiebungen in der Gesellschaft nach sich. Es stellt sich die Frage, wie Privatheit und Autonomie in einer algorithmisch konstruierten Welt gewährleistet und gefördert werden können. Hierzu wird insbesondere der mediale und forschungswissenschaftliche Diskurs aufgearbeitet und die Gefährdungen individueller Privatheit anhand ausgewählter Literatur belegt. *Privatheit* gilt in der eingenommenen Perspektive als, in Auseinandersetzung mit Gesellschaft, herzustellender Zustand und *Selbstermächtigung* folglich als Prozess, durch den dieser Zustand erreicht wird.

In diesem Beitrag geht es weniger um die konkrete Benennung von Instrumenten und Maßnahmen als vielmehr um die differenzierte Betrachtung von Herausforderungen und die Identifikation von möglichen Handlungsfeldern bzgl. Privatheit und Autonomie. Im Folgenden werden zunächst die algorithmische Konstruktion der Wirklichkeit und der Bedarf an Selbstermächtigung der Nutzer:innen und Verbraucher:innen näher erörtert (Abschn. 2). Anschließend werden drei Dimensionen der algorithmischen Konstruktion und mögliche Formen der Selbstermächtigung diskutiert: Algorithmen als Besitztümer (Abschn. 3), als Akteure (Abschn. 4) und als Kontrollmittel (Abschn. 5). Im Resümee wird abschließend auf die Notwendigkeit einer kollektiven Selbstermächtigung hingewiesen (Abschn. 6).¹

¹ Mein Dank gilt an dieser Stelle den drei Reviewer:innen für die konstruktiven Hinweise zum ursprünglichen Manuskript.

2 Algorithmische Konstruktion und Selbstermächtigung

Aus informatischer Perspektive ist ein Algorithmus eine wohl-definierte Berechnungsprozedur, die ausgehend von einem gegebenen Input an Daten einen bestimmten Output an Daten erzeugt. Mit anderen Worten: Algorithmen sind Werkzeuge, mit denen konkrete Berechnungsprobleme in einer Sequenz von Einzeloperationen gelöst werden. In diesem Sinne handelt es sich um eine Art Handlungsanweisung. Dazu muss die soziale Welt kalkulierbar werden: Der Gegenstand oder Prozess wird zum semiotischen Zeichen, dann zum Signal, das jede Bedeutung verliert, und schließlich berechenbar.

2.1 Algorithmische Konstruktion und digitale Vulnerabilitäten

Soziale Phänomene werden durch *Verdatung und Algorithmisierung* in binäre Kategorien überführt – Analoges wird digital. Vice versa werden von Technik Daten als Aussagen über die soziale Welt zur Interpretation durch Menschen rückgemeldet – digitale Werte werden analog. Mit diesem doppelseitigen Transformationsprozess sind spezifische Charakteristika und Herausforderungen verbunden [14]. Drei *Dimensionen* algorithmischer Konstruktion von Wirklichkeit erscheinen für diesen Beitrag zentral.

Erstens werden Algorithmen von Menschen entwickelt. Es existieren Konstrukteure und Konstrukteurinnen, die den Arbeitsbereich und die Funktionalität der Algorithmen festlegen. Insofern fließen spezifische Weltansichten und Deutungen sowie Problemlösungsstrategien in die Softwareentwicklung ein. Darüber hinaus ist der „Arbeitsbereich“ von Algorithmen eingeschränkt, sie funktionieren unter spezifischen Bedingungen für konkrete Fragestellungen. *Zweitens* nehmen Algorithmen an menschlichen Handlungen und Interaktionen teil, indem sie komplexe Kommunikations-, Regelungs- und Entscheidungsprozesse unterstützen und beeinflussen [15, 16]. Algorithmen besitzen Handlungsträgerschaft („Agency“), handeln mit und prägen nicht nur individuelles Verhalten, sondern auch gesellschaftliche Strukturen. *Drittens* erzeugen digitale Techniken Datenspuren. Daten werden erhoben, verarbeitet, weitergeleitet, ausgetauscht und gespeichert. Im Zeitverlauf bildet sich ein komplexes datenbasiertes Referenzsystem in der digitalen Welt heraus. Wer über diese Daten verfügt und bestimmt, ist in der Lage, Machtansprüche geltend zu machen und/oder Macht auszuüben.

Gesamtgesellschaftlich bilden sich eigenständige, digitale Infrastrukturen und Institutionen als neue Basis sozialen Zusammenlebens heraus [17, 18]. Das

bedeutet auch, dass durch Nutzung digitaler Technologien neue *digitale Vulnerabilitäten* entstehen. Neue Angriffsflächen bei Nutzer:innen bieten sowohl die Sorglosigkeit und/oder Überschätzung der eigenen Fähigkeiten im Umgang mit Computertechnik als auch potenzielle Sicherheitsrisiken. Durch ‚Trivialisierung‘ der digitalen Werkzeuge werden die mit der Nutzung verbundenen Gefahren und Risiken ausgeblendet [19]. Eine mögliche Besorgtheit der Nutzer:innen geht dennoch einher mit einem unbesorgten Umgang mit ihren Daten (‚Privacy-Paradox‘). Hinzu kommt, dass gerade beim Einsatz von Digitaltechnik oftmals noch institutionalisierte, sicherheitsfördernde Maßnahmen fehlen [20]. So besteht neben verschiedenen Formen der Cyberkriminalität (Cyber-Grooming, Phishing-Betrug, Identitätsdiebstahl, etc.) die Gefahr, dass Menschen im Rahmen von Datenökonomie und Plattformkapitalismus zu „gläsernen“ Verbraucher:innen werden, wenn Technologiefirmen ihre Netzwerkmacht missbrauchen, um etwa Konsum anzuregen. Ebenso kritisch ist die Möglichkeit einzuschätzen, „gläserne“ Bürger:innen zu erzeugen, etwa im Zuge einer stärkeren Überwachung durch staatliche Organisationen und Geheimdienste, die Computer infiltrieren und Funkzellen abfragen (Stichworte: Bundestrojaner und Vorratsdatenspeicherung).

Digitale Angriffsflächen sind wenig offensichtlich und nur vermittelt erfahrbar. Angriffe erfolgen mittels Algorithmen, Softwareagenten und neuronalen Netzen und basieren auf der Zirkulation von, seien es durch „freiwillige“ Angaben oder durch nicht sichtbare Protokollierung erhobene, Daten der Nutzer:innen und Verbraucher:innen durch die Gesellschaft. Der Einsatz von Algorithmen und deren Funktionsweise sind weitestgehend intransparent und die – wenn auch bedienrichtige – Nutzung von Computertechnik ist oft durch Nicht-Wissen über die zugrunde liegenden Infrastrukturen, Eigentumsrechte und regulativen Hoheitsansprüche gekennzeichnet.

2.2 Digitale Selbstermächtigung entlang dreier Dimensionen

Während die Gewährleistung von Privatheit und Autonomie zum einen seitens wirtschaftlicher Unternehmen oftmals untergraben wird und zum anderen durch staatliche bzw. politische Regulierung lange Umsetzungsphasen durchläuft, sehen sich Nutzer:innen und Akteure und Akteurinnen in eigener Verantwortung, aktiv zu werden und sich zu schützen. Es bedarf einer *digitalen Selbstermächtigung* im Rahmen der Nutzung von digitalen Techniken, um zu einem gewissen Grad digital souverän handeln zu können. Digitale Souveränität umfasst Datenschutz, Privatheitsschutz (Privacy) und Datensicherheit ebenso wie verschiedenste

soziale, technologische und regulative Aspekte, so den Erwerb digitaler Kompetenzen, Privacy-by-Design, Interoperabilität, und vieles mehr [21, 22]. Für digitale Selbstermächtigung sind insbesondere Einblick und Kontrolle in die Arbeit von Algorithmen, in Datenbewegungen und in zugrunde liegende Infrastrukturen wichtig [23]. Selbstermächtigung im Bereich des Digitalen ist nicht nur eine Form der praktischen Befähigung, sondern auch der Reflexion und Bewertung des eigenen Handelns mit Computertechnik, also Aneignung und Distanzierung mit dem Ziel der Hervorbringung, Veränderung und Aufrechterhaltung autonomer digitaler Handlungsweisen. Digitale Selbstermächtigung stellt die Nutzer:innen und Verbraucher:innen in den Mittelpunkt und nicht techno-ökonomische Interessen oder politische Überwachungsmaßnahmen.

Die vorgenommene Identifizierung eines Bedarfs an digitaler Selbstermächtigung ist keine neoliberalistische Forderung, die das Individuum einzig und allein selbstverpflichtet. Es geht um die Stärkung *einer* Facette der Sicherung von Privatheit und Autonomie, eine Facette, die von Nutzer:innen eigenständig bearbeitet werden kann. Darüber hinaus wären bspw. Infrastruktursysteme, die Privatheit fördern, zu schaffen – ganz im Sinne einer gesellschaftlichen Verantwortung für Privatheit (aller) [24]. Die Zuständigkeiten und Verantwortlichkeiten dafür sind weit gestreut, auch wenn es sich oft um ostentative Zuschreibungen handelt und keine konkret umgesetzten Handlungsprogramme. Selbstermächtigung bedeutet auch, von anderen ermächtigt, also durch fremdes Handeln in Autonomie und Souveränität gestärkt zu werden, wie im Falle eines holistischen Datenschutzes [19]. *Fremdermächtigung* und das Engagement staatlicher oder institutioneller Akteurinnen und Akteure haben einen Anteil am souveränen Handeln Einzelner. Das verweist auf die Relevanz eines umfassenden Konzepts von Privatheit, bei dem individuelle Nutzer:innen nur ein Teil der schützenden Figuration sein können. Darüber hinaus sind wirtschaftliche, politische und wissenschaftliche Akteurinnen und Akteure ebenso gefordert, die Privatheit und Autonomie von Nutzer:innen zu ermöglichen. In diesem Beitrag werden die temporären „Grauzonen“ hervorgehoben, in denen Verantwortung durch Andere nicht übernommen und/oder zugeteilt wird und Schutzmaßnahmen für die Individuen mindestens für einen beschränkten Zeitraum ausbleiben.

Im Folgenden werden die drei genannten Dimensionen algorithmischer Konstruktion der Wirklichkeit ausführlicher diskutiert und zugehörige gesellschaftlichen Auswirkungen sowie Ansätze digitaler Selbstermächtigung skizziert (vgl. Tab. 1). Selbstermächtigung erfolgt bestenfalls entlang aller Dimensionen, wobei deren Trennung analytischer Art ist, und die Dimensionen empirisch ineinander übergehen. Kapitel drei „Algorithmen als Besitztümer“ fokussiert Software und Code als Eigentum und stellt digitale Aufklärung und den Erwerb von Hintergrundwissen in den Vordergrund, bspw. über Sektoren, Firmenstrukturen

Tab. 1. Dimensionen algorithmischer Konstruktion

Algorithmen als...	Modus	Imagination und Repräsentation	Selbstermächtigung durch...
...Besitztümer	Geldquelle	Rationalität	...digitale Aufklärung: Hintergrundwissen
...Akteure	Interaktion	Objektivität	...digitale Bildung: Handlungswissen
...Kontrollmittel	Daten	Legitimität	...digitale Achtsamkeit: Folgenwissen

und Kooperationen. „Algorithmen als Akteure“ (Kapitel vier) nimmt die Interaktion mit Software in den Blick und fokussiert Kompetenzerwerb durch digitale Bildung, um den Output von Algorithmen einzuordnen, um also bspw. Suchergebnisse und mediale Öffentlichkeiten zu deuten. Das fünfte Kapitel „Algorithmen als Kontrollmittel“ stellt Daten in den Mittelpunkt und sieht digitale Achtsamkeit (etwa Datensparsamkeit) als zentralen Mechanismus der Selbstermächtigung.

In der vorliegenden Argumentation wird eine Akzentuierung der *Fähigkeiten und Kompetenzen* des Individuums vorgenommen – ganz im Sinne der Fragestellung: Was kann jede:r selbst auf einem niedrigschwelligen Niveau für die eigene Privatheit in der digitalen Sphäre tun? Demzufolge tritt auch die Diskussion der konkreten Verantwortung für Schutzmaßnahmen in den Hintergrund, etwa der staatliche Ausgestaltungsauftrag für Datenschutzregeln und Auffangverantwortung. Individuellen Praktiken der Selbstermächtigung wird ein eher geringer Durchdringungsgrad in der Gesellschaft konstatiert und genau darin liegt die Gestaltungsaufgabe. Diese Gestaltungsaufgabe erfordert allerdings die kollektiven Bemühungen verschiedener Akteurinnen und Akteure und die Institutionalisierung gesellschaftsweit verfügbarer Maßnahmen [20]. Die Zuständigkeiten für Privatheit sind multipel und bilden ein Netz *verteilter Verantwortung*. Dieses Phänomen wird bereits in den nachstehenden Ansätzen zu Selbstermächtigung tangiert und im abschließenden Kapitel aufgegriffen.

3 Algorithmen als Besitztümer: Geldquelle, Rationalität, Aufklärung

Algorithmen und Software sind Besitztümer, Eigentum und Geldquelle. Als Institutionen repräsentieren Algorithmen rationale Problemlösungen. Nutzer:innen

imaginieren eine auf sie selbst ausgerichtete Funktionalität. Diese paradigmatische Repräsentation liegt quer zur intransparenten Inwertsetzung von Nutzer:innen-Daten. Es scheint daher nötig, einen Blick in die Blackboxes der Algorithmen zu werfen und sich im Sinne digitaler Aufklärung mit Hintergrundwissen über digitale Technik auszustatten.

3.1 Geldquelle

Algorithmen sind durch Menschen geschaffene Produkte für wirtschaftliche Unternehmen, staatliche und andere Organisationen. Der Quellcode unterliegt daher in den meisten Fällen spezifischen *Eigentumsrechten* und gilt als Betriebsgeheimnis. Algorithmen haben eine konkrete Zielsetzung, die sich vorrangig über die offiziell artikulierte Funktion definiert. Über den Verkauf von Software generieren Unternehmen einen Gewinn. Ebenso wird mit kostenfrei angebotener Software *Geld* verdient, indem bspw. Werbung in der Software eingeblendet wird und/oder die Daten der Nutzer:innen verwertet werden. Die vordergründige Funktion der Nutzung, bspw. von sozialen Medien wie Facebook, wird so mit einem weitgehenden Geschäftsmodell überlagert. In diesen Funktionschirmen überwiegen die wirtschaftlichen Interessen der Privatunternehmen die sozialen Interessen der Nutzer:innen. Algorithmen und digitale Technik sind sozial konstruiert, beinhalten demzufolge eingeschriebene Handlungsanweisungen und verkörpern vorherrschende Paradigmen, insb. Visionen von Ingenieur:innen, Ideologien globaler Konzerne, und mögliche Stereotype und Rassismen [25, 26].

Dieses ökonomisierte und von datenbasierten Geschäftsmodellen geprägte Technikmilieu ist für Nutzer:innen weitgehend intransparent. *Verantwortung* für eine souveräne Computernutzung wird nicht von den Eigentümer:innen übernommen, sondern diffundiert in den soziotechnischen Konstellationen und verfestigt sich in unausgesprochenen Verhaltensmustern [27]. Einerseits wird die Verantwortung zum Umgang mit personenbezogenen Daten an die Nutzer:innen delegiert, indem überkomplexe Allgemeine Geschäftsbedingungen vorgelegt werden, obwohl Nutzer:innen oft nicht in der Lage sind, sich mit den zahlreichen Regelungen aller Dienstleistungsanbieter:innen auseinanderzusetzen. Andererseits muss Software von Nutzer:innen aufwendig konfiguriert werden, um in einem Privatsphäre-Modus zu arbeiten. Softwareentwickler:innen und Anbieter:innen digitaler Techniken entziehen sich so ihrer Verantwortung. Auch die neuen Regelungen über den Einsatz von Cookies werden mitunter durch schlechte Usability untergraben, sodass die Aus- bzw. Abwahl von Cookies vernachlässigt wird und die Firmen letztendlich doch Daten erheben können.

3.2 Rationalität

Darüber hinaus stellt sich eine weitere Form der Verantwortungsverschiebung ein, wenn Nutzer:innen die Algorithmen als die eigentlichen Handlungsträger ansehen [28]. Die Zuschreibung von Handlungsfähigkeit geht einher mit der Zuweisung von Verantwortung. Die Funktionsausführung der Algorithmen erscheint dann *rational* und die Ergebnisse objektiv. Die dahinterliegenden Strukturen und Eigentümer:innen der Software werden außer Acht gelassen und die multiple Fehleranfälligkeit der Software dürfte in den wenigsten Fällen reflektiert werden. So gelingt es Organisationen ihre Interessen zu technisieren und daraus Profit zu schlagen: das Suchergebnis einer Maschine ist, wie es ist, und gilt als zuverlässig. Die Google-Suchmaschine ist in dieser Hinsicht ein Paradebeispiel für eine algorithmische Institution.

Private Firmen erhalten durch Nutzer:innen einen Vertrauensvorschuss, trotzdem sie die Verantwortung für ihr Handeln auf Nutzer:innen und Technik übertragen. Oft scheint eine gewisse Gutgläubigkeit gegenüber digitalen Technologien zu überwiegen. Dabei kann bspw. bei Suchmaschinen nicht von Suchneutralität ausgegangen werden [16]. Es ist in der Regel kaum möglich, etwas über Prozeduren zur Generierung von Trefferlisten oder Empfehlungen in Erfahrung zu bringen. Die Nutzer:innen sind daher geleitet von einem kurzfristigen Pragmatismus [17]. Sie lassen sich Daten vorsortieren und schauen, ob das Ergebnis in der jeweiligen Situation passt und Gültigkeit besitzt. Ein Urteil über die Qualität der Daten können sie sich kaum bilden. Alle Prozesse der Modellbildung, der Datenauswahl usw. sind ebenso ausgeblendet, wie die eingangs erwähnten Geschäftsmodelle.

3.3 Digitale Aufklärung

Selbstermächtigung der Nutzer:innen wird durch den Erwerb von *Hintergrund- bzw. Kontextwissen* über das Technikmilieu, nicht nur der „Big Five“, möglich. Bislang ist vor allem zu beobachten, dass sich Nutzer:innen proaktiv und auf vielfältige Weise Bedienwissen aneignen. Die Schnittstelle zum digitalen Endgerät scheint jedoch eine „Trennwand“ zu markieren und den Erwerb von Hintergrundwissen zu hemmen. Selbstermächtigung bedeutet das Hinterfragen von digitalen Strukturen und Prozessen.

Hintergrundwissen ist zwar nicht zwingend notwendig, um Techniken zu handhaben. Im Gegenteil: es ist ein grundlegendes Charakteristikum von Technik, als Blackbox zu funktionieren, um die Nutzung zu erleichtern. In Bezug auf die besonderen Merkmale von Digitalisierung (intransparente Referenzsysteme,

Datenprotokollierung, algorithmische Induzierung), wird es jedoch immer wichtiger, die Blackbox der Algorithmen zumindest in Teilen zu verstehen. Welche Firma besitzt welche Software und verdient damit auf welche Weise Geld? Auf welchen Servern werden Bilder und Dokumente gespeichert und welche Verantwortungsprinzipien sind damit verbunden? Nach welchen Regeln arbeiten Filter- und Bewertungsalgorithmen und wie erfolgt Personalisierung?

Letztlich entscheiden Nutzer:innen, welchen Dienst sie zu welchen Konditionen „einkaufen“. Diese Konditionen könnten jedoch transparenter gemacht werden. Insbesondere Klarheit über die hinter den Algorithmen liegenden Wissensmodelle und deren Ausrichtung auf Profit oder Gemeinwohl wäre wichtig. Initiativen und Vereine klären diesbezüglich über Digitaltechnik und spezifische Herausforderungen auf. So wurde bspw. das „kritische Lexikon der Digitalisierung“ [29] herausgegeben und es existiert ein „Deutschland Dialog für digitale Aufklärung“.² Der Staat sieht sich ebenso in der Verantwortung und die „Bundeszentrale für digitale Aufklärung“³ kann u. a. bei Themen wie Fake News und Hassrede zu wichtigen Einsichten und möglichen Handlungsstrategien verhelfen. In der Analyse algorithmischer Entscheidungsfindung ist zudem die Nichtregierungsorganisation „AlgorithmWatch“ sehr aktiv und informiert über die Arbeitsweise von Algorithmen, zuletzt bei „Instagram“.⁴

4 Algorithmen als Akteure: Interaktion, Objektivität, Bildung

Nutzer:innen stehen in Interaktion mit Algorithmen und Software. Die Meldungen und Benachrichtigungen der digitalen Technik werden als objektive Ergebnisse wahrgenommen. Diese Repräsentationen von realer Welt werden kaum hinterfragt und für gültig befunden. Algorithmen beeinflussen so menschliches Handeln. Der Umgang und Dialog mit Technik sollte reflektiert werden, besonders vor dem Hintergrund der begrenzten Arbeitsgebiete von Algorithmen. Digitale Bildung fördert hier den Erwerb von Bedien- und Nutzungswissen.

² Vgl. <https://www.sicher-im-netz.de/deutschland-dialog-für-digitale-aufklärung> (10.10.2020).

³ Vgl. <https://www.bundesregierung.de/breg-de/bundesregierung/staatsministerin-fuer-digitalisierung/bundeszentrale-fuer-digitale-aufklaerung> (06.12.2020).

⁴ Vgl. <https://algorithmwatch.org> (10.10.2020).

4.1 Interaktion

Digitale Technik handelt mit, beeinflusst soziales Handeln und bringt soziale Wirklichkeit hervor [30]. Algorithmen entscheiden, welche Ausschnitte von der Welt auf „Twitter“ in den Meldungen oder bei „Amazon“ in den Kaufempfehlungen zu sehen sind. Grundsätzlich erlaubt Personalisierung, sich zielgerichtet mit relevanten Optionen zu beschäftigen. Gleichzeitig fehlt Nutzer:innen der Zugriff auf derartige Algorithmen, um eben jene Personalisierung zutreffend zu definieren. Soziales wird also nicht dargestellt, sondern vorgefiltert und sortiert. Algorithmen agieren in und für einen kleinen Ausschnitt der Welt. Der Output von Algorithmen wird mitunter jedoch als universell gültig angesehen. In der Konsequenz besteht die Gefahr, diese für jeden User eigens generierten, modellbasierten Konstruktionen als realweltliche *Repräsentationen* misszuverstehen [17]. „Facebook“ als primäre Nachrichtenquelle für Nutzer:innen und damit digitale Institution ist insofern kritisch zu sehen.

Das eher „passive“ Zuschneiden der Welt der Nutzer:innen wird ergänzt durch immer häufigere Handlungsinitiierungen von technischen Agenten. Durch ‚Nudging‘ werden Handlungen von Anwender:innen unbemerkt in vorgegebene Richtungen gelenkt. Update-Aufforderungen und Empfehlungen von Produkten oder Kontakten in sozialen Netzwerken nehmen die Aufmerksamkeit der Nutzer:innen in Anspruch und veranlassen oder erzwingen sogar eine Reaktion. Technologiefirmen werden zu ‚gierigen Institutionen‘ [31], die allumfassende „Besitzansprüche“, d. h. permanente Erreichbarkeit und Verantwortung zur Reaktion, an die Nutzer:innen stellen. Ausgehend von der Programmierung und implementierten Funktionalität beeinflussen Algorithmen unser Verhalten und sind darüber hinaus Teil von Entscheidungsketten und Entscheidungsfindung. ‚Scoring‘ durch Algorithmen regelt Sozialbeziehungen, bspw. in Einstellungsgesprächen oder bei der Bonitätsauskunft. Die Unantastbarkeit der Zahlen und berechneten Werte ist dabei zentrales Moment: eine SCHUFA-Bewertung ist korrekt, auch wenn unklar ist, wie sie entsteht [32].

4.2 Objektivität

Algorithmen werden zu Regelungsmechanismen sozialen Lebens, indem sie gesellschaftliche Komplexität reduzieren. Ihre Berechnungen und Ergebnisse besitzen eine inhärente *Objektivität*. Es scheint, als wäre der Algorithmus intelligent, wenn er Präferenzen identifiziert. Das erscheint bei Algorithmen als Handlungsgrundlage durchaus fragwürdig, da diese anhand der vergangenen

Handlungen (Selektionen) der Nutzer:innen und früheren Referenzen (Webseitenaufrufen, Likes, Einkäufen, etc.) funktionieren. So werden Dysfunktionalitäten diskutiert, etwa in Form von ‚filter bubbles‘ und ‚echo chambers‘, in denen Nutzer:innen durch automatisierte Personalisierung „gefangen“ seien [33].

Algorithmen und deren Ergebnisse sind sehr dynamisch, weil sie von den Entwickler:innen ständig angepasst werden und weil Nutzer:innen durch ihre Aktionen und Handlungen (mitunter absichtsvoll und manipulativ) Daten generieren, die die Ergebnisse der Algorithmen verändern. Ein Kernmoment digitaler Technologien besteht also darin, dass sie sich zu jeder Zeit in Modifikation befinden (können) – auch wenn gerade darauf zugegriffen wird. Die immanente Dynamik der Technik resp. die permanente technische *Unabgeschlossenheit* [34] hat Konsequenzen. Nutzer:innen erlernen nicht einmalig den Umgang mit einer Technik, sondern müssen sich stets umorientieren, neu lernen, neu denken. Objektivität und Erwartungssicherheit, die mit Technik typischerweise verbunden ist, erodieren im digitalen Raum.

4.3 Digitale Bildung

Aus den vorstehenden Bemerkungen lässt sich eine technische *Selbstverantwortlichkeit* der Nutzer:innen ableiten. Selbstermächtigung bedeutet in dieser praktischen Hinsicht die kompetente Handhabung digitaler Technik zu erlernen. Dazu gehört primär die Aneignung des Bedienwissens von Smartphones, Computern, Peripheriegeräten (bspw. Routern). Es bedeutet gleichzeitig auch, eine (Kauf-)Auswahl für bestimmte Geräte treffen zu können, und zwar nach den für die Nutzer:innen wichtigen Kriterien. Dies sollte dem Trend entgegenwirken, dass Technologiefirmen Zwecke für vorhandene Techniken festlegen und deren Dienstbarkeit suggerieren, statt reale Bedarfe zu adressieren. Die souveräne Handhabbarkeit digitaler Technik umfasst zudem intuitive Designs, altersgerechte Menüstrukturen und individuelle Konfigurierbarkeit. Softwareentwickler:innen sind hier gefordert, nutzerzentrierte und subjektorientierte Produkte zu gestalten. In Bezug auf Konstruktion und Implementierung von Software stellen sich die Fragen der Verantwortung für eine nutzer:innenfreundliche Gestaltung. Entwickler:innen sind in Konzernstrukturen eingebunden und programmieren auftragsgemäß [35]. Vorgaben für Softwareprodukte werden insofern intern durch das Management oder extern durch staatliche Vorgaben gemacht. Auch wenn deren Einfluss aktuell gering erscheint, werden Forderungen nach ‚demokratischen Ingenieur:innen‘ laut, die Technikentwicklungen eine selbstermächtigende Richtung geben [36].

Bezüglich der Interaktion mit Algorithmen wäre es wünschenswert, diese und deren Arbeit zu kennzeichnen und sichtbar zu machen. So wären bspw. Suchergebnisse direkt adressierbar und bekämen weniger den Eindruck von Objektivität. Auch der Einsatz alternativer Algorithmen durch Nutzer:innen und die eigenverantwortliche Ent-Personalisierung von Software sollten gefördert werden. Dazu braucht es eine stete Erweiterung und Aktualisierung der Grundkompetenzen digitalen Handelns. Solch eine digitale Bildung kann bereits in der Schule beginnen [37],⁵ wobei der dazu nötige Diskurs über Format und Inhalte eines entsprechenden Schulfachs aktuell eher parteilich aus Informatik-Perspektive geführt wird. Zudem darf ein „Digitalpakt“ nicht lediglich zu einer Digitalisierung überholter Lehrpläne führen. Digitale Bildung ist Bestandteil lebenslangen Lernens und es scheint unerlässlich, Maßnahmen sowohl zielgruppenspezifisch zuzuschneiden, bspw. mit Comics für Kinder⁶ oder Projekten für Senior:innen⁷, also auch Angebote in Volkshochschulen und anderen Bildungseinrichtungen zur Verfügung zu stellen.

Selbstermächtigung wird zudem durch Verbraucher:innenschutzverbände gewährleistet. Die Cyberfibel⁸ etwa vermittelt, wie sich Verbraucher:innen im Alltag vor Bedrohungen schützen können. Nutzer:innen sind darüber hinaus aufgefordert, proaktiv Erfahrungsberichte im Umgang mit Softwareprodukten zur Verfügung zu stellen und so strukturelle Problemlagen aufzudecken. Mit der „Marktbeobachtung Digitales“ (früher Marktwächter „Digitale Welt“) bspw. wird versucht, Verbraucher:innen bei Online-Einkäufen oder bei der Nutzung von Preisvergleichsportalen zu unterstützen und deren Interessen zu schützen.⁹

5 Algorithmen als Kontrollmittel: Daten, Legitimität, Achtsamkeit

Algorithmen produzieren Daten und arbeiten mit Daten, die nicht den Nutzer:innen zur Verfügung stehen, sondern von den Eigentümer:innen der Software in Wert gesetzt werden. Damit sind Tendenzen der Überwachung und Kontrolle verbunden. Über argumentative Legitimation werden von Privatunternehmen und

⁵ Vgl. auch <https://www.netzwerk-digitale-bildung.de> (10.10.2020).

⁶ Vgl. <https://edri.org/our-work/privacy-for-kids-digital-defenders> (10.10.2020).

⁷ Vgl. <https://www.silversurfer-rlp.de/> (10.10.2020).

⁸ Vgl. <https://www.cyberfibel.de> (01.12.2020).

⁹ Vgl. <https://www.vzbv.de/themen/marktbeobachtung/marktbeobachtung-digitales> (10.10.2020).

Regierungen Profile von Nutzer:innen und Bürger:innen angelegt und deren Aktivitäten verfolgt. Dieser informationelle Kapitalismus ist offenzulegen und Nutzer:innen ist mehr digitale Achtsamkeit zu vermitteln.

5.1 Daten

Zunehmend werden unter Einsatz von Algorithmen und aufgrund von Daten und deren Verknüpfungen algorithmenbasierte Entscheidungen getroffen, Scorings und Bewertungen vorgenommen und ‚Big Data‘-Analysen durchgeführt, die die sozialen Ordnungsleistungen und die gesellschaftliche Dynamik tangieren. Ausgehend von der Hoffnung, dass mit dem Aufkommen des World Wide Web und digitaler Kommunikation (dezentrale Vernetzung, peer-to-peer-Kommunikation, eine wertfreie (d. h. ungefilterte und ungebremste) Informationsübertragung und freie Verlinkungen) sich demokratische bzw. demokratisierende Prozesse entfalten, wird nunmehr konstatiert, dass die digitale Welt zunehmend reguliert, hierarchisiert und zentralisiert wird [38].

Ausschlaggebend dafür sei die *Ökonomisierung* der digitalen Welt, die zugleich die infogene Grundversorgung und das Menschenrecht auf Informationszugang gefährde. Digitale Entwicklung scheint gekennzeichnet durch ubiquitäre Technisierung, infrastrukturelle Zentralisierung und scharf asymmetrische Inklusionsordnungen [27]. Nutzer:innen seien im sog. ‚informationellen‘ oder ‚kybernetischen‘ Kapitalismus lediglich Datenlieferanten und würden durch das (auch heimliche) Sammeln von Daten ausgebeutet und von den profitgenerierenden Bedingungen abgeschnitten [39–42]. Die Monopolisierung und Informationsmacht bei einer Handvoll Firmen wie Apple, Microsoft, Google, Amazon und Facebook führe zu rekursiven Steuerungsprozessen menschlichen Handelns, aufbauend auf den durch Nutzer:innen generierten Datenströmen.¹⁰

5.2 Legitimität

Algorithmen sind Kontrollinstanzen. In ihrer Kombination oder Gesamtheit unter zentraler Verwaltung lassen sich Daten kombinieren, Profile erstellen und Überwachungsstrukturen schaffen. Welche Daten der Individuen hierbei an welchen

¹⁰ Ähnlich verhält es sich mit dem Social Credit System in China, bei dem die Daten allerdings aus staatlicher Protokollierung und Überwachung stammen und für die Bewertung der Bürger:innen (und Firmen) in Bezug auf Staatstreue genutzt werden.

Stellen der Gesellschaft verarbeitet werden, ist für Nutzer:innen wenig nachvollziehbar. Zu denken ist diesem Zusammenhang an Predictive Policing, Gesichtserkennung und die neueren Diskussionen über die Steuer-ID in Deutschland. Legitimität für unmittelbare algorithmengesteuerte Kontrolle und Überwachung wird hergestellt u. a. durch Begründung erhöhter *Sicherheit* und erhöhter Sicherheitsbedürfnisse der Bürger:innen.

Mittelbare, also indirekte, Kontrolle durch Technologiefirmen etwa legitimiert sich demgegenüber unter einer funktionsbedingten Argumentation. Ohne Daten wäre eine regelkonforme Nutzung von Software nicht möglich. Damit verbunden ist die stillschweigend Zustimmung der Nutzer:innen. Aufgrund fehlenden Widerspruchs, sei es weil ein Widerspruch nicht als Handlungsoption zur Auswahl steht oder nicht wahr- und/oder ernstgenommen wird, wird der Einsatz der Algorithmen toleriert und so legitimiert. Es sind über die Nutzung hinausgehende „Zwangsformen“, denen sich die Nutzer:innen ausgesetzt sehen, wie die Einwilligung in Datenweitergabe oder Werbemails. Digitale Technik wird in ihrer jetzigen Form als Status Quo anerkannt und Nutzer:innen ordnen sich „freiwillig“ dieser Netzwerkmacht unter [17].

5.3 Digitale Achtsamkeit

Die zentrale Herausforderung für Selbstermächtigung besteht zunächst darin, dass Nutzer:innen digital wachsam sind und die Chancen und Risiken der Nutzung digitaler Technologien vor allem mit Blick auf die Datenspuren und Referenzsysteme abschätzen, also *Folgenwissen* generieren und erwerben.

Daten sind bspw. immer seltener auf den Endgeräten der Nutzer:innen gespeichert, sondern in einer ‚Cloud‘ zentral verfügbar, also auf den Servern und Datenbanken der Dienstleister:innen. Mit Nutzung von Clouds geht die, mit einem Personal Computer gewonnen, Souveränität wieder verloren und es stellen sich Fragen der Sicherheit, des Zugriffs und der Überwachung – auch bereits bei der Übermittlung. Als Alternative gilt die unabhängige Vernetzung von Computern, wie bei der Initiative „Freifunk“.¹¹ Auch der Einsatz von VPN-Servern und des „privaten Modus“ bei Nutzung von Browsern bieten Möglichkeiten gegen Ausspähen, wenngleich diese Instrumente gegenüber professionellen Hackern und Geheimdiensten kaum Schutz bieten. Software und Plattformen sollten von Technologieunternehmen initial auf Privatheit ausgelegt sein, um personenbezogene Daten zu schützen. Nutzer:innen hätten dann später die Möglichkeit, Daten zu

¹¹ Vgl. <https://freifunk.net> (10.10.2020).

spezifischen Zwecken freizugeben. Auch hier zeigen sich Konvergenzen von Selbst- und Fremdermächtigung durch Privacy by Design und Default-Konzepte.

Datensicherheit ist auch Aufgabe des Staates. Öffentliche Rechenzentren könnten hier eine neue Rolle einnehmen [43, 44]. Neben dem Schutz der Privatsphäre der Bürger:innen könnten diese als Wissensbasen dienen und Informationen und Kurse anbieten. Dadurch ergäben sich für Bürger:innen Möglichkeiten, ihr Handeln an professionellem und lokal relevantem Wissen auszurichten. Dass digitale Medien auf solche Zielsetzungen ausgerichtet sein können, zeigt das Projekt „FragDenStaat“.¹² Bürger haben hier die Möglichkeit, Anfragen zu politischen Themen an staatliche Behörden zu stellen. Die Anfragen und Antworten werden gesammelt und stehen der digitalen Öffentlichkeit zur Verfügung. Auf europäischer Ebene gibt es ebenfalls Bemühungen, sich durch „GAIA-X“ eine regional begrenzte Cloud-Infrastruktur zu schaffen und so Datenhoheit aufrecht zu erhalten und Daten zu sichern.

6 Digitale Selbstermächtigung als kollektiver Prozess

Gesamtgesellschaftlich ist zu beobachten, dass sich Handlungen, Werte, Normen und Lebensweisen verstärkt an rationalistischen, ökonomischen und algorithmischen Grundmustern orientieren [32, 45]. Dabei werden eher kaum demokratisierende und emanzipatorische Prozesse angestoßen, sondern in digitalen Technologien werden die sozialen, bspw. milieu- und altersspezifischen, Verhältnisse gespiegelt und digitale Klüfte erzeugt [46]. Privatheit und Autonomie der Nutzer:innen stehen dabei auf dem Prüfstand und Fragen nach digitaler Selbstermächtigung werden aufgeworfen.

6.1 Algorithmische Konstruktion und Gesellschaft

Die algorithmische Konstruktion der Gesellschaft zeigt viele Manifestationen, von denen drei analytisch getrennte, jedoch empirisch eng miteinander verbundene Facetten erörtert wurden. Sozial konstruierte Algorithmen agieren autonom, interagieren mit Nutzer:innen, sortieren und filtern für sie die Wirklichkeit und übernehmen gesellschaftliche Kontrollfunktionen [47, 48]. Damit sind Chancen und Vorteilen verbunden. Algorithmen reduzieren durch Personalisierung Komplexität und ermöglichen bzw. unterstützen auf diese Weise Handeln. Dies erfolgt

¹² Vgl. <https://fragdenstaat.de> (10.10.2020).

jedoch völlig intransparent. Neben reinem Bedien- und z. T. Konstruktionswissen, das sich die Nutzer:innen selbst aneignen, bringen sie kaum etwas über die Grundlagen und Funktionsweisen der Algorithmen oder über den Verbleib der persönlichen Daten in Erfahrung. Algorithmisierung ermöglicht zwar Verschlüsselung und anonyme Kommunikation, es existieren Firewalls, um PCs zu schützen und der Einsatz von Track-Blockern vermindert die Sammlung von Daten. Nutzer:innen haben jedoch selten Wahlmöglichkeiten beim Einsatz digitaler Medien, es werden ihnen lediglich Entscheidungen überlassen. Diese Entscheidungen folgen nicht selten der Maxime, entweder den Bedingungen der privaten Firmen oder staatlichen Stellen zuzustimmen oder die Software oder den Dienst nicht zu nutzen.

Die algorithmische Konstruktion der Gesellschaft hat stark ökonomisch-rationale Züge. Statt zunehmender Kritik, genießen die Internet- und Technologiefirmen einen überraschenden Vertrauensvorschuss, obwohl Grundrechte der Nutzer:innen infrage gestellt werden. In öffentlichen Medien wird Digitalisierung mehrheitlich positiv konnotiert und die (möglichen) Vorteile immer wieder propagiert. Der Diskurs um Datenschutz und verwandte, mit Digitalisierung verbundene, Herausforderungen kommen nur zögerlich in der Öffentlichkeit an. Dabei besteht kein Wissens-, sondern ein Vollzugsdefizit. Das Problem liegt nicht in der wissenschaftlichen Erforschung und Kritik, sondern darin, die Ergebnisse auf der *tagtäglichen* Handlungsebene der Individuen zu artikulieren und zu nutzen.

Eine drängende Frage lautet weiterhin, wie Digitalisierung im Sinne von Bürger:innen und Nutzer:innen gestaltet wird. Es besteht grundsätzlich die Gefahr, dass sich die gesellschaftliche Konstruktion der Wirklichkeit immer weiter am Credo ökonomischer Algorithmisierung orientiert und ein schleichender Wandel einsetzt, der sich in kaum wahrnehmbaren inkrementellen Veränderungen von Normen und Werten äußert und digitale Souveränität erodiert. Es bedarf einer „Sozialisierung“ technischer Routinen statt einer zunehmenden Formalisierung sozialen Handelns. Statt den Lebensalltag der Menschen proaktiv zu informatisieren und digitale Hörigkeit zu forcieren, sollten Informatiker:innen Medien- und Systemgestalter für selbstbestimmte Lebenswelten sein [11].

6.2 Selbstermächtigung und verteilte Verantwortlichkeit

Da weniger auf die freiwillige Selbstkontrolle der Unternehmen und die zeitverzögerte Fremdkontrolle durch staatliche Gesetzgebung zu hoffen ist, stellt digitale Selbstermächtigung ein wichtiges Moment zur Herstellung und Festigung von

Privatheit dar. Dabei geht es nicht um eine neoliberalistische Verantwortungszuweisung, sondern um die Ermöglichung souveräner Entscheidungen, um die Entwicklung eines ‚digitalen Bauchgefühls‘ [49] und um Awareness der ‚menschlichen Firewall‘ – und zwar sowohl durch selbständige Aneignung als auch durch *externe* Unterstützung. Aufgrund asymmetrischer Machtverhältnisse in der Gesellschaft, speziell zwischen individuellen Nutzer:innen und Organisationen, deren Software und Plattformen genutzt werden, ist Selbstermächtigung stets auch gekoppelt an und abhängig von den organisationalen Handlungsparadigmen und Handlungsweisen [50]. Nutzer:innen sind scheinbar frei in ihrer Entscheidung, bspw. Facebook nicht zu nutzen. Andererseits wirken soziale Zwänge, die zur Nutzung ‚verpflichten‘. Verbote in Bezug auf den Betrieb solcher Plattformen sind wenig sinnvoll, da sie an Regulierungs- und Durchsetzungsdefiziten scheitern. Freilich könnte die Masse der Nutzer:innen Firmen unter Druck setzen, dafür scheinen die Gefahren jedoch zu wenig greifbar. Selbstermächtigung kann dann im Minimum bedeuten, soziale Plattformen zu nutzen und über die Folgen Bescheid zu wissen. Zugleich kann Selbstermächtigung bedeuten, freie Software als gleichwertige Alternative wählen zu können. Hierfür könnte der Staat in Verantwortung genommen werden.

Selbstermächtigung darf nicht professionellen Nutzer:innen vorbehalten und *Nischenkompetenz* sein. Selbstermächtigung bedeutet, bildungsferne Nutzer:innen zu berücksichtigen und zu überlegen, wie Mensch-Technik-Interaktionen plastischer gestaltet werden können, bspw. durch Visualisierungen (wie Verkehrsschilder), die beim Verständnis digitaler Prozesse helfen. Software ist für eine souveräne Nutzung zu entwickeln und mit Schutzfunktionen auszustatten. Digitale Bildung an den Schulen ist grundsätzlich sinnvoll, wenngleich auch hier über Formate und Inhalte bislang keine Einigkeit herrscht. Mögliche Schulfächer befreien jedoch nicht von der Notwendigkeit, breite Bevölkerungsschichten lebenslang weiterzubilden. Dazu gehören kompetenzbasierte Schulungsszenarien, bspw. Kurse an Volkshochschulen, und andere gruppenbasierte Formate bei denen auf Altershomogenität oder eben Altersmischungen geachtet wird, und Arbeitsplätze, an denen Awareness entwickelt und Selbstermächtigung gefördert wird. Nötig sind gesellschaftsweite Prozesse der Selbstermächtigung.

Digitale Selbstermächtigung ist ein kollektiver Prozess, der im Sinne einer ‚sozialen Innovation‘ die digitale Ordnung rekonfiguriert. Er erfordert die Bemühungen unterschiedlicher Akteure auf allen gesellschaftlichen Ebenen. Selbstermächtigung ist ein partizipativer Prozess, bei dem Konstruktion und Implementation von Technik an Bedarfen orientiert sind und das Subjekt im Mittelpunkt steht. Darüber hinaus ist die Partizipation weiterer Akteurinnen und Akteure

(aus Zivilgesellschaft, Politik, etc.) mitzudenken, um gemeinsam die soziotechnischen Rahmenbedingungen für souveräne Digitalität entlang der Maximen von Privatheit und Autonomie zu schaffen [51–53]. Wünschenswert sind eine bedarfsorientierte, zielgruppengerechte und gemeinwohlorientierte Konstruktion und ein entsprechender Einsatz digitaler Technik. Wichtig hierbei ist eine Kooperation mit den relevanten Zielgruppen, um Bedarfslagen *und* Dienstleistungen aufeinander abzustimmen. Algorithmen und algorithmenbasierte Entscheidungssysteme sind stets in gesellschaftliche Zusammenhänge eingebettet, die ebenfalls in den Blick zu nehmen sind [14]. So ist neben kompetenten Individuen ein starker Staat nötig, der seine Bürger:innen bspw. durch Gesetzgebung schützt. Digitale Selbstermächtigung konstituiert sich relational zwischen individuellen Voraussetzungen und personenexogenen Faktoren: Selbstermächtigung der Individuen ist nur in einer selbstermächtigenden Gesellschaft möglich. Dabei greifen Grade von Selbst- und Fremdermächtigung in einem Netz verteilter Verantwortung produktiv ineinander.

Literatur

1. Berger, P., Luckmann, T.: Die gesellschaftliche Konstruktion der Wirklichkeit, 19. Aufl. Fischer, Frankfurt a. M. (2003)
2. Strauss, A.L.: Continual Permutations of Action. Routledge, London (2008[1993]).
3. Rammert, W.: Technik – Handeln – Wissen. Springer VS, Wiesbaden (2016[2007]).
4. Passig, K.: Fünfzig Jahre Black Box (2017). <https://www.merkur-zeitschrift.de/2017/11/23/fuenfzig-jahre-black-box>. Zugegriffen: 6. Okt. 2020
5. Geitz, E., Vater, C., Zimmer-Merkle, S. (Hrsg.): Black Boxes – Versiegelungskontexte und Öffnungsversuche. De Gruyter, Berlin (2020)
6. Weyer, J.: Die Echtzeitgesellschaft. Campus, Frankfurt (2019)
7. Lobo, S.: Leben im Datenstrom. Bequemlichkeit schlägt Datensparsamkeit (2016). <https://www.spiegel.de/netzwelt/web/zugriff-auf-daten-bequemlichkeit-schlaegt-sicherheit-kolumne-a-1114091.html>. Zugegriffen: 6. Okt. 2020
8. Orwat, C., et al.: Software als Institution und ihre Gestaltbarkeit. Informatik Spektrum **33**(6), 626–633 (2010)
9. Just, N., Latzer, M.: Governance by algorithms: reality construction by algorithmic selection on the Internet. Media Cult. Soc. **39**(2), 238–258 (2017)
10. Enzensberger, H.M.: Das digitale Evangelium (2000). <https://www.spiegel.de/spiegel/print/d-15376078.html>. Zugegriffen: 6. Okt. 2020
11. Hellige, H.D.: Die Dialektik der informationellen Aufklärung. Ein Rückblick auf den Theoriediskurs von Informatik & Gesellschaft. In: Kühne, C. et al. (Hrsg.) Per Anhalter durch die Turing-Galaxis, S. 55–60. Verlags-Haus Monsenstein und Vannerdat, Münster (2012)
12. Schirrmacher, F. (Hrsg.): Technologischer Totalitarismus. Suhrkamp, Berlin (2015)
13. Han, B.-C.: Psychopolitik. Neoliberalismus und die neuen Machttechniken. Fischer, Frankfurt a. M. (2014)

14. Zweig, K.A.: Algorithmische Entscheidungen: Transparenz und Kontrolle. In: *Analysen und Argumente* 338. Konrad-Adenauer-Stiftung e. V., Berlin (2019)
15. Schmidt, J.-H.: *Social Media*. Springer VS, Wiesbaden (2013)
16. Lewandowski, D.: *Suchmaschinen verstehen*. Springer, Berlin (2015)
17. Stalder, F.: *Kultur der Digitalität*. Suhrkamp, Berlin (2016)
18. Seyfert, R., Roberge, J. (Hrsg.): *Algorithmenkulturen. Über die rechnerische Konstruktion der Wirklichkeit*. Transcript, Bielefeld (2017)
19. Biniok, P.: Maschinenraum, Privatsphäre und Psychopolitik. Holistischer Datenschutz als Kombination von individueller Souveränität und kollektiver Gesetzgebung. *Informatik Spektrum* **43**(3), 220–226 (2020).
20. Karaboga, M., Masur, P., Matzner, T., Mothes, C., Nebel, M., Ochs, C., Schütz, P., Fhom, H.S.: *Selbstdatenschutz*. Fraunhofer ISI, Karlsruhe (2014)
21. SVRV: *Digitale Souveränität. Gutachten des Sachverständigenrats für Verbraucherfragen*. Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz, Berlin (2017).
22. GI (Gesellschaft für Informatik): *Schlüsselaspekte digitaler Souveränität (Arbeitspapier)*. Gesellschaft für Informatik e. V., Berlin (2020).
23. Biniok, P.: *Emanzipierende Infrastrukturen. Wie digitale Teilhabe ausgebaut werden kann*. Rosa-Luxemburg-Stiftung, Berlin (2017)
24. Matzner, T., Masur, P.K., Ochs, C., von Pape, T.: *Do-It-Yourself Data Protection – Empowerment or Burden?* In: Gutwirth, S., Leenes, R., de Hert, P. (Hrsg.): *Data Protection on the Move*, S. 277–305. Springer, Dordrecht (2016)
25. Akrich, M.: *The De-Scriptioin of Technical Objects*. In: Bijker, W.E., Law, J. (Hrsg.) *Shaping Technology/Building Society. Studies in Sociotechnical Change*, S. 205–224. MIT Press, Cambridge/Mass. (1992)
26. Dosi, G.: *Technological paradigms and technological trajectories: A suggested interpretation of the determinants and directions of technical change*. *Res. Policy* **11**(3), 147–162 (1982)
27. Dickel, S.: *Post-Technokratie. Prekäre Verantwortung in digitalen Kontexten*. *Soziale Systeme* **19**(2), 282–303 (2014).
28. Bauman, Z., Lyon, D.: *Daten, Drohnen. Disziplin. Ein Gespräch über flüchtige Überwachung*. Suhrkamp, Berlin (2013)
29. RSL: *Smarte Worte. Das kritische Lexikon der Digitalisierung*. Rosa-Luxemburg-Stiftung, Berlin (2016)
30. Rammert, W., Schulz-Schaeffer, I. (Hrsg.): *Können Maschinen handeln? Soziologische Beiträge zum Verhältnis von Mensch und Technik*. Campus, Frankfurt a. M. (2002)
31. Coser, L.: *Gierige Institutionen. Soziologische Studien über totales Engagement*. Suhrkamp, Berlin (2015)
32. Mau, S.: *Das metrische Wir: Über die Quantifizierung des Sozialen*. Suhrkamp, Berlin (2017)
33. Pariser, E.: *Filter Bubble: Wie wir im Internet entmündigt werden*. Hanser, München (2012)
34. Grenz, T.: *Mediatisierung als Handlungsproblem. Eine wissenssoziologische Studie zum Wandel materialer Kultur*. Springer VS, Wiesbaden (2017)

35. Spiekermann, S., Korunovska, J., Langheinrich, M.: Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers. *Proc. IEEE* **107**(3), 600–615 (2019)
36. Nemitz, P., Pfeffer, M.: Prinzip Mensch. Freiheit und Demokratie im Zeitalter der Künstlichen Intelligenz. Dietz, Bonn, Macht (2020)
37. Müller-Lietzkow, J.: Quo Vadis Digitale Bildung? In: Friedrichsen, M., Bisa, P.-J. (Hrsg.): Digitale Souveränität Vertrauen in der Netzwerkgesellschaft, S. 305–323. Springer VS, Wiesbaden (2016)
38. Egloff, D.: Digitale Demokratie: Mythos oder Realität? Auf den Spuren der demokratischen Aspekte des Internets und der Computerkultur. Westdeutscher Verlag, Opladen (2002)
39. Castells, M.: Jahrtausendwende. Das Informationszeitalter, Bd. 3. Campus, Opladen (2003)
40. Sevignani, S.: Krise der Privatheit. In: Hahn, K., Langenohl, A. (Hrsg.): Kritische Öffentlichkeiten – Öffentlichkeiten in der Kritik, S. 237–254. Springer VS, Wiesbaden (2017)
41. Daniljuk, M.: Die neuen Gatekeeper. Google und Facebook in den kybernetischen Kapitalismus. Rosa-Luxemburg-Stiftung, Berlin, Mit Apple (2016)
42. Zuboff, S.: Das Zeitalter des Überwachungskapitalismus. Campus, Frankfurt a. M. (2018)
43. Jäger, W.: Neue Rolle öffentlicher Rechenzentren für Bürger-Datenschutz und Bürger-Befähigung. In: Friedrichsen, M., Bisa, P.-J. (Hrsg.) Digitale Souveränität Vertrauen in der Netzwerkgesellschaft, S. 23–34. Springer VS, Wiesbaden (2016)
44. Krenn, K., Tiemann, J., Hunt, S.S.: Datenachtsamkeit – ein neuer(licher) Blick auf den Selbstschutz. Fraunhofer-Institut für Offene Kommunikationssysteme, Berlin (2019)
45. Selke, S.: Lifelogging. Digitale Selbstvermessung und Lebensprotokollierung zwischen disruptiver Technologie und kulturellem Wandel. Springer VS, Wiesbaden (2016)
46. Warschauer, M.: Technology and social inclusion. MIT Press, Cambridge/Mass, Rethinking the digital divide (2003)
47. Kurz, C., Rieger, F. Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen. Fischer, Frankfurt a. M. (2011)
48. Lanier, J.: You are not a gadget. A manifesto. Alfred A. Knopf, New York (2010)
49. Müller, L.-S.: Das digitale Bauchgefühl. In: Friedrichsen, M., Bisa, P.-J. (Hrsg.) Digitale Souveränität Vertrauen in der Netzwerkgesellschaft, S. 267–285. Springer VS, Wiesbaden (2016)
50. Rost, M.: Zur Soziologie des Datenschutzes. *DuD – Datenschutz und Datensicherheit* **37**(2) 85–91 (2013).
51. Le Dantec, C., DiSalvo, C.: Infrastructuring and the formation of publics in participatory design. *Soc. Stud. Sci.* **43**(2), 241–264 (2013)
52. Pipek, V., Wulf, V.: Infrastructuring: Toward an Integrated Perspective on the Design and Use of Information Technology. *Journal of the Association for Information Systems* **10**, 447–473 (2009)
53. Hagendorff, T., Geminn, C., Lamla, J., Karaboga, M., Krämer, N., Nebel, M., Uhlmann, M.: Risiken künstlicher Intelligenz für die menschliche Selbstbestimmung. Fraunhofer ISI, Karlsruhe (2020)

Open Access Dieses Kapitel wird unter der Creative Commons Namensnennung 4.0 International Lizenz (<http://creativecommons.org/licenses/by/4.0/deed.de>) veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Kapitel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.

