Felix Sühlmann-Faul

Der goldene Käfig des Digitalkapitalismus

Nichts kostet mehr als kostenlos

oekom

Für G & K und alle weiteren Generationen

Plunging into a newfound
Age of advanced observeillance
A worldwide, foolproof cage
Privacy and intimacy as we know it
Will be a memory
Among many to be passed down
To those who never knew
Living in the pupil of one thousand eyes
Was it overlooked in front of all our faces?
Death: „1000 Eyes“, 1995

Alle im Buch verwendeten Abbildungen sind von Isabell Hornig.

INHALTSVERZEICHNIS

1 Einleitung

Der Protagonist Joe Chip in Philip K. Dicks Roman »Ubik« ist notorisch bankrott. Er befindet sich in seiner Wohnung und möchte diese verlassen. Was Joe gleich erlebt, hat starke Ähnlichkeit mit dem, was wir im digitalisierten Zeitalter häufig erleben:

»Er ging also mit energischen Schritten auf die Wohnungstür zu, drehte den Griff und zog den Riegel zurück. Die Tür ließ sich nicht öffnen. Stattdessen ertönte eine Stimme: ›Fünf Cents, bitte.‹ Chip durchwühlte abermals seine Taschen. Keine einzige Münze mehr, nichts. ›Ich zahle morgen‹, sagte er zu der Tür. Erneut drehte er am Griff, doch das Schloss blieb zu. ›Was ich dir zahle, ist eigentlich ein Trinkgeld. Ich muss dich nicht bezahlen.‹ ›Das sehe ich anders‹, erwiderte die Stimme. ›Bitte werfen Sie einen Blick in den Kaufvertrag, den Sie unterschrieben haben, als Sie diese Wohnung erwarben.‹ In einer Schreibtischschublade fand er den Vertrag; seit der Unterschrift hatte er ihn immer wieder konsultieren müssen. Ganz klar: Für Öffnen und Schließen der Tür war eine Gebühr obligatorisch. Kein Trinkgeld. ›Sie sehen, dass ich recht habe‹, ließ die Stimme selbstgefällig verlauten.«[1]

»Ubik« wurde 1969 veröffentlicht. Wie in einigen Büchern des Autors wirkt es frappierend, wie prophetisch er noch vor der Entwicklung des ersten Mikroprozessors eine Welt beschreibt, die der heutigen sehr ähnlich ist. Ähnlich, aber nicht gleich: Spielte dieser Roman im heutigen Digitalkapitalismus, würde Chip zusätzlich auf diese Probleme stoßen: Er benötigte alle paar Jahre eine neue Tür, da es für die alte keine Software-Updates mehr gibt. Durch fehlende Software-Updates wird die Tür auch zunehmend weniger sicher und sollte es doch ein Update geben, ließe sie sich nur noch sehr langsam öffnen. Ohnehin wäre das Betriebssystem der Tür nicht mit einer einmaligen Zahlung erhältlich, sondern nur als Abonnement. Aber am wichtigsten ist: Die Tür wüsste, wann, von wem und wie oft Joe Besuch hat, wann er seine Wohnung verlässt und wann er sie wieder betritt.

Das ließe sich noch fortsetzen – aber der Hauptunterschied zwischen der Gegenwart und der Situation von Joe Chip ist, dass keine Centbeträge für die Funktion von Geräten bezahlt werden müssen, die zum Eigentum zählen – das wäre einem regulären Leasingvertrag ähnlich. Der unausgesprochene Gesellschaftsvertrag des digitalkapitalistischen Zeitalters verlangt jedoch eine andere Währung. Dieser Vertrag lautet *kostenlose Apps und Dienste gegen persönliche Daten*. Und wir werden vielfach täglich zur Kasse gebeten.

Genauer gesagt handelt es sich nicht um *persönliche*, sondern meist um personenbezogene[2] Verhaltens-[3] und Metadaten[4], die wir unwillentlich und nicht spürbar bei jeder Nutzung des Internets oder von digitalen Endgeräten erzeugen. Laut des digitalkapitalistischen Gesellschaftsvertrags werden die Technologiekonzerne mit Daten der Nutzer*innen für Bequemlichkeit, Unterhaltung, Austausch und Teilhabe finanziert. Und die Endgeräte – Smartphones, Computer, Tablets, smarte Assistenten etc. – die eigentlich unser Eigentum sind, sind ähnlich Joe Chips Haushaltsgeräten eigentlich Leasingobjekte, da diese ebenfalls ohne *Datenspende* nicht funktionieren.

Nun stellt sich die Frage, wo das Problem liegt. Es sind schließlich goldene Zeiten. Videos, Musik, Spiele und andere Konsumchancen sind im Handumdrehen erhältlich – und dazu entweder sehr günstig oder wie gesagt kostenlos. Zu verbergen hat niemand etwas und zu spüren ist diese *Bezahlung* ohnehin nicht – Daten werden ja nicht weniger. Joe Chip wäre sicherlich froh.

Allerdings sind die Zeiten keineswegs golden. Golden ist nur der Käfig, dessen Streben jeden Tag etwas stabiler werden. Nutzer*innen zahlen zwar zunächst mit Daten – letztlich aber mit ihrer Freiheit. Der digitalkapitalistische Gesellschaftsvertrag funktioniert nur durch mehr oder weniger freiwillige Aufgabe unseres Grundrechts auf Datenschutz. Und Datenschutz schützt keineswegs Daten, sondern Menschen. Datenschutz schützt die Privatsphäre, die jedem Menschen ermöglicht, ein freies, selbstbestimmtes Leben nach eigener Vorstellung zu führen. Und der Datendiebstahl, der in jeder Sekunde jeden Tages erfolgt, hebelt diesen Datenschutz aus, infiltriert die Privatsphäre und versklavt die Nutzer*in-

nen, die für Technologiekonzerne eigentlich nur unbezahlte Arbeitskräfte und Erzeuger*innen des zentralen Produktionsmittels des Digitalkapitalismus sind: Daten.

Obwohl dieser Vertrag aus Gewohnheit heute als *normal* empfunden wird, muss diese Normalität radikal hinterfragt werden. Denn die Veräußerung von Daten ist gefährlich. Wenn Menschen mit Daten bezahlen, teilen sie gesichtslosen, intransparenten und machtsüchtigen Konzernen Geheimnisse über sich selbst mit, die teilweise die engsten Freund*innen nicht kennen. Mit jeder *Bezahlung* wird die Macht dieser Konzerne auf unterschiedlichen Ebenen größer, mit jeder *Bezahlung* veräußert jeder/jede Nutzer*in ein Stück ihrer Grundrechte und Freiheiten, jede *Bezahlung* legitimiert ein System, das auf einer utilitaristischen, undemokratischen und pathologischen Ideologie aufbaut.

Das Interesse an Daten rührt u. a. daher, weil sie dazu dienen, das lukrativste Geschäftsmodell des Internets zu ermöglichen: programmatische Werbung. Durch die gesammelten Daten und das dadurch ermittelbare Wissen über die Nutzer*innen kann Online-Werbung sehr zielgerichtet präsentiert werden. Es geht darum, der richtigen Person zum richtigen Zeitpunkt das richtige Produkt oder eine entsprechende Dienstleistung zu zeigen. Mit der Sammlung von Daten verdienen Konzerne wie Meta (Facebook) und Alphabet (Google) ihr Geld, weil sie nicht hauptsächlich Smartphones oder Apps verkaufen, sondern Werbung. Um diese exakte Passung zwischen Werbung und Nutzer*in zu erzeugen, müssen diese Konzerne möglichst viel über sie wissen. Aber auch andere große Tech-Imperien sind an den Daten der Nutzer*innen interessiert: Microsoft, Amazon und Apple gehören ebenfalls zu den zentralen Akteuren im Datenhandel, auch wenn ihre Geschäftsmodelle nicht Online-Werbung umfassen. Trotzdem ist es für die Konzeption von Geschäftsmodellen essenziell, möglichst viel über die Nutzer*innen zu wissen, bspw. um Verhalten vorherzusagen oder Verhalten zu erzeugen. Das zweite lukrative Geschäftsmodell des Internets neben Werbung, der E-Commerce, funktioniert ebenfalls nur auf Basis exakter Analysen von Vorlieben und Verhalten: »Wird oft zusammen gekauft: Kunden, die ›Kopier-/Druckerpapier A4‹ kauften, kauften auch ›3-in-1 Tinten-Multifunktionsdrucker‹« – schon

einmal gelesen? Und nicht zuletzt profitieren alle genannten, großen Technologiekonzerne von Daten für das Training von KI-Systemen.

Seit Mai 2018 gilt europaweit die Datenschutz-Grundverordnung, die den Umgang mit personenbezogenen Daten regelt und damit auch Grundrechte und Privatsphäre schützt. Um personenbezogene Daten verarbeiten zu dürfen, muss den Datenschutzrichtlinien und Allgemeinen Geschäftsbedingungen von Internetdiensten beim Einrichten eines neuen Telefons oder der Nutzung von Apps aber gezwungenermaßen zugestimmt werden. Sonst kann die Soft- oder Hardware nicht genutzt werden. Da es sich dabei um umfangreiche juristische Texte handelt, die häufig absichtlich kompliziert geschrieben sind, wird zumeist einfach zugestimmt – ohne genau zu wissen, was mit den eigenen Daten geschieht. Dadurch wird den Konzernen die Erlaubnis zur Datensammlung und -verarbeitung erteilt. Durch die Zustimmung zur Verarbeitung exponieren die Nutzer*innen jeden Tag, an dem sie das Internet oder digitale Endgeräte verwenden, unweigerlich ihre Privatsphäre und *existieren* als digitalisierte Kopie auf den Servern vieler Unternehmen.

Die Konsequenzen beschränken sich nicht auf die *virtuelle* Welt. Versicherungen und Banken kaufen inzwischen Daten von Nutzer*innen, um Beiträge oder Kreditzinsen zu ermitteln. Auch Bewerbungsverfahren werden inzwischen häufig datengestützt durchgeführt, um in einer frühen Phase der Auswahl möglicher Kandidat*innen genau »auszusieben«. Dabei sind datafizierte Faktoren wie Lebensstil, Kreditwürdigkeit, etwaige Erkrankungen, Freundes- und Bekanntenkreis von erheblicher Bedeutung. Durch die Nutzung von Systemen Künstlicher Intelligenz und Big Data – der Sammlung riesiger Datenmengen – werden auf Basis gesammelter Daten und deren Analyse Schlüsse über die Bankkund*innen oder Bewerber*innen gezogen, auf welche die Betroffenen keinen Einfluss nehmen können – selbst dann nicht, wenn die gezogenen Schlüsse falsch sind. Trotzdem ist es »normal«, dass die Bewerbung oder das Darlehen auf Basis der gesammelten Daten abgelehnt wird.

Auch auf einer anderen Ebene hat die Sammlung von Daten Konsequenzen – nicht nur für das Individuum, sondern für die gesamte Gesellschaft. Denn die genannten überaus mächtigen Konzerne beugen auch

Gesetzgebungsverfahren zu ihren Gunsten, kommodifizieren öffentliche Güter und unterminieren den politischen Apparat. Das gefährdet nicht nur Grundrechte und Selbstbestimmung, sondern auch die Demokratie. Dabei befindet sich die Politik in einer Zwickmühle. Ihre Aufgabe ist es, die Öffentlichkeit vor dem Missbrauch der Daten zu schützen, gleichzeitig ist sie von den Infrastrukturen und Produkten der Technologiekonzerne abhängig und beugt sich an vielen Stellen dieser nicht legitimierten Macht.

Darin spiegelt sich eines der größten Probleme dieser Zeit. Da es immer weniger Möglichkeiten gibt, das Internet oder digitale Endgeräte zu vermeiden, sind die Nutzer*innen den Datensammlungspraktiken ständig ausgeliefert.

Doch nicht alle Dienste und Apps sind gleich: Es gibt durchaus eine gewisse Anzahl datenschutzfreundlicher Software, die sich dadurch auszeichnet, dass sie so wenig wie möglich oder gar keine Daten über die Nutzer*innen sammelt. Doch gibt es für jede Anwendung zumeist eine große Auswahl möglicher Programme oder Dienste. Es muss daher schnell und einfach herauszufinden sein, ob bspw. Firefox die eigenen Daten besser schützt als Edge, für E-Mails eher Posteo oder GMail genutzt werden sollte und welche Entscheidung zu treffen ist, wenn alle Freund*innen WhatsApp nutzen, aber die Privatsphäre bei Signal wahrscheinlich besser geschützt ist.

Zu untersuchen ist daher, wie eine datenschutzsensible *Anna Normalnutzerin* unabhängig, einfach und transparent eine informierte Entscheidung über die Wahl einer App oder eines Dienstes treffen kann – quasi wie mit einem Blick auf den »Nutri-Score« im Supermarkt bei der Auswahl von Lebensmitteln. Das ist eine der Fragestellungen, der in diesem Buch nachgegangen wird. Das Ziel besteht darin, ein dem Nutri-Score ähnliches Bewertungssystem zu entwickeln – den »Priva Score«. Dieses Werkzeug unterstützt die Nutzer*innen bei der Auswahl ihrer Apps und ermöglicht eine informierte Entscheidung. Ohne Datenschutzrichtlinien lesen zu müssen, kann mit einem Blick die Software ausgewählt werden, die im Vergleich zu anderen Produkten die Daten besser schützt. Als Konzeptnachweis werden populäre Sofortnachrichtendienste (Messenger) herangezogen, die anhand ihrer Datenschutzfunktionen miteinander ver-

glichen werden, woraus sich eine Empfehlung ergibt. Für die Auswahl der Funktionen wurden eine Vielzahl von Quellen genutzt und zwei qualitative Interviews mit Fachpersonen geführt.

Dass heutzutage Datenschutz und Privatsphäre mit vielen digitalen Formen des Wirtschaftens im Konflikt stehen, verweist auf den ökonomischen Rahmen. Um diesen Konflikt zu verstehen, werden die folgenden Fragen gestellt: *Welche kulturellen und gesellschaftlichen Prozesse haben dem Digitalkapitalismus den Weg geebnet? Ist der Digitalkapitalismus eine eigenständige und von vorangegangenen Epochen abgrenzbare Form des Kapitalismus? Welche Auswirkungen hat der Digitalkapitalismus auf Individuen, Politik und Gesellschaft?*

Struktur

Das vorliegende Buch umfasst fünf Kapitel. Das erste Kapitel dient dazu, die Relevanz und den Umfang des Themas und die Notwendigkeit eines Werkzeugs wie des Priva Scores festzustellen und zu umreißen. Die analytische Aufarbeitung des Digitalkapitalismus beginnt zunächst in Kapitel 2 mit der Betrachtung dreier zentraler Einflüsse, die dem Digitalkapitalismus den Weg geebnet haben. Diese Einflüsse umfassen grundsätzliche, kulturelle und gesellschaftliche Evolutionen, die aufgrund ihrer Prozesshaftigkeit und gegenseitigen Interdependenz als *Stränge* bezeichnet werden. Diese drei Stränge bilden gemeinsam ein Geflecht, das dem Digitalkapitalismus seine Grundlage liefert. Der erste Strang fokussiert das Zeitalter der Aufklärung, welches zur Abkehr von nicht legitimierter Herrschaft, aber auch zu einer neuen Unterwerfung unter Rationalität und Wissenschaft geführt hat. Dies ermöglichte eine zunehmende Verbindung zwischen Technosphäre und Soziosphäre. Der zweite Strang umfasst ideologische und mythische Wesen. So obskur oder paradox dies angesichts der angeblichen Rationalisierung durch die Aufklärung klingen mag – die Abkehr von tradierter Macht und Unmündigkeit eröffnete *Erklärungslücken*. Diese wurden durch neue göttliche Wesen, Mythen, Magie und Geister gefüllt – z. B. dem *Geist des Kapitalismus*. Aufgearbeitet wird hier ebenfalls die nicht minder mit Täuschung und Magie beladene Ideologie der Technologiekonzerne. Der dritte Strang umfasst den

soziotechnologischen Prozess – die Manifestation und Kolonisierung der Lebenswelt durch Technologie und die wirtschaftshistorischen Hintergründe zur Erklärung einer Überhöhung des gesellschaftlichen Stellenwerts von Technologie.

In Kapitel 3 wird gezeigt, dass es gute Gründe gibt, den Digitalkapitalismus als eigenständige Epoche des Kapitalismus zu verstehen. Daran schließt sich die Analyse von drei Ebenen negativer Einflüsse des Digitalkapitalismus an. Diese umfasst das Plattformgeschäftsmodell zusammen mit dem Faktor Arbeit, die Infiltration der Privatsphäre und ihren Zusammenhang mit Datenschutz. Danach wird gezeigt, wie der Digitalkapitalismus sich auf Demokratie und die Rolle der Politik auswirkt und wie öffentliche Güter, Räume und Gelder durch die Technologiekonzerne vereinnahmt werden. Nicht übersehen werden darf die zentrale Technologie des Digitalkapitalismus – die Künstliche Intelligenz, was das Kapitel 3 beschließt.

Während die eben dargestellten Inhalte eine umfassende *Problembeschreibung* bieten, befasst sich Kapitel 4 mit Hilfestellung für die datenschutzsensible *Anna Normalnutzerin* in Form des Priva Scores und anderer Möglichkeiten der digitalen Selbstverteidigung. Zunächst wird anhand eines Lastenhefts der Priva Score Schritt für Schritt erläutert: im Vergleich zum Vorbild des Nutri-Scores, eine Vorstellung der zu vergleichenden Messengerdienste, ihre Datenschutzfunktionen und die letztendliche Berechnung des Priva Scores einschließlich seiner Bewertung der Messengerdienste.

Kapitel 5 umfasst eine Abgrenzung des Priva Scores von zwei partiell vergleichbaren Konzepten: Einerseits Übersichtstabellen, die seit Kurzem die Handhabung der Nutzerdaten in den App Stores von Google und Apple zeigen sollen, andererseits ein von den Konzernen unabhängiges Konzept namens *App Checker*. Im Anschluss werden die eigentlichen Grenzen des Priva Scores problematisiert: die politökonomischen Randbedingungen und die Rolle der Nutzer*innen in einer stark konsumorientierten Gesellschaft.

Erweiterungsmöglichkeiten des Priva Scores an andere Kategorien von Diensten und Apps werden im Anschluss diskutiert. Der vorletzte

Teil des fünften Kapitels enthält einen Aufruf an die Politik – denn der Priva Score ist ein Konzept für den/die einzelne/n Nutzer*in. Die Verantwortung für den Schutz der Daten auf die individuelle Ebene zu verschieben, ist auch bei anderen Themen nicht zielführend: Die Entscheidung, den individuellen Lebensstil in Hinblick auf die Klimakrise zu reduzieren, liegt auf der individuellen Ebene. Aber es muss einfacher sein, einen nachhaltigen Lebensstil zu verfolgen. Und da führt kein Weg an entschiedenen, politischen Schritten vorbei. Und das gilt auch für die hier thematisierte Problematik – die negativen Auswirkungen des Digitalkapitalismus und seiner dominanten Akteure. Hier müssen politische Lösungen entstehen, um den Individuen den Zwang zu einer *digitalen Selbstverteidigung* zu nehmen. Zuletzt erfolgt ein Schlusswort.

Relevanz des Themas

Welcome, my son
Welcome to the machine
Where have you been?
It's alright, we know where you've been (…)
What did you dream?
It's alright, we told you what to dream.
Pink Floyd: »Welcome to the Machine«, 1975

Der Begriff *Digitalisierung* ist vergleichsweise alt und wurde 1954 zum ersten Mal verwendet.[5] Ursprünglich wurde damit die Umwandlung analoger Informationen in ein maschinenlesbares Format für Archivierungszwecke bezeichnet – bspw. die Erstellung von Lochkarten oder später das Scannen von Büchern. Demgegenüber wird Digitalisierung heute als Bezeichnung für einen der zentralen gegenwärtigen Megatrends verwendet. Oder – in sozialwissenschaftlicher Lesart – als zusammenfassender Begriff für die »(…) globale, gesamtgesellschaftliche, soziotechnische Transformation durch die exponentiell wachsende Leistungsfähigkeit der Mikroelektronik.«[6] Diese zugegebenermaßen etwas sperrige Definition des Autors fokussiert sich darauf, dass die Phänomene, die inzwischen mehr oder weniger zum Alltag gehören – virtuelle Realität, Künstliche Intelligenz,

(teil)autonomes Fahren und dergleichen – letztlich nur durch die in den letzten Jahrzehnten exponentiell gesteigerte Rechenkapazität der Mikroelektronik ermöglicht werden. Es sind also immer noch die Auswirkungen der dritten industriellen Revolution. Eine erste, allgemein sichtbare Veränderung war, dass Personal Computer in den Büros der Industrienationen des Globalen Nordens zum Standardarbeitsgerät wurden. Mit dieser Entwicklung brach gleichzeitig eine neue Epoche des Kapitalismus an.[7]

Heute ist die Menschheit von einer nie dagewesenen Menge Technologie – insbesondere digitaler Technologie – umgeben. Es handelt sich nicht nur um das Zeitalter der Digitalisierung, sondern auch um das Zeitalter eines inzwischen voll entwickelten Digitalkapitalismus. Seine zentrale Sphäre ist das kommerzialisierte Internet, das größtenteils von den zwei Geschäftsmodellen E-Commerce und personalisierte Werbung dominiert wird. Der Erfolg von Online-Werbung begründet sich zunächst darin, dass Formen der klassischen Außenwerbung – Anzeigen, Fernseh- und Radiowerbung – stets einen breiten und ungenauen Streueffekt besitzen. Ob die anvisierte Zielgruppe die Marketingbemühungen wahrnimmt und sich zu einer Kaufentscheidung durchringt, ist häufig nicht direkt nachvollziehbar. Aber über die Nutzung personenbezogener Daten ist es sehr viel effizienter möglich, der gesuchten Zielgruppe Werbung zu zeigen. Ziel personalisierter Werbung ist es, der richtigen Person zum richtigen Zeitpunkt das richtige Produkt oder die richtige Dienstleistung zu offerieren. Durch personenbezogene Daten ist dies mit weniger Streueffekten behaftet, sodass Werbebudgets gezielter eingesetzt werden können. Durch die Datennutzung kann Werbung sehr viel persönlicher in der Ansprache sein und damit mit höherer Wahrscheinlichkeit eine Kaufentscheidung herbeiführen.

Um viele Daten zu sammeln, bieten mehrere große Technologiekonzerne ein digitales Ökosystem[8] von zumeist kostenlosen Diensten an – bspw. Suchmaschinen, E-Mail-Dienste, Office-Anwendungen, Messenger und/oder soziale Netzwerke. Im Zentrum eines Ökosystems steht meist eine Plattform. Diese Dienste bieten den Nutzer*innen sehr viel Wert im Alltag.[9] Kostenlose Navigationsdienste, Cloudspeicher, Office-Software oder Messenger bieten eine hohe *Konsumentenrente*. Jedoch fußen diese

Angebote ausschließlich auf ökonomischen Absichten der Unternehmen, die diese zur Verfügung stellen. Bei Nutzung der Dienste, aber auch nur durch den Besuch von Webseiten hinterlassen Nutzer*innen unweigerlich zahlreiche personenbezogene Daten, Metadaten und Verhaltensdaten, die gesammelt werden. Da diese Daten ein wertvolles Gut sind, werden sie im Rahmen der Datenökonomie[10] gehandelt. Den Großteil des Markts mit personalisierter Werbung teilen sich die Technologiekonzerne Alphabet (Google) und Meta (Facebook).[11] Das bedeutet, dass es quasi kaum einen Weg um diese zwei Konzerne gibt, wenn online Werbung geschaltet werden soll. Weitere Akteure der Datenökonomie stellt eine unüberschaubare Menge kleiner Datenhändler (Data Broker) dar.

Zweck der großen Konzerne wie der kleinen Datenhändler ist es, von Nutzer*innen ein möglichst exaktes Datenabbild zu erzeugen. Je mehr Daten gesammelt werden, desto genauer ist der Zuschnitt von Werbung auf einen Personenkreis möglich. Das ist die Basis des Programmatic Advertising. Dieses Verfahren umfasst den automatisierten softwarebasierten Ein- und Verkauf von Online-Werbeflächen in Echtzeit. Während eine Webseite lädt, läuft im Hintergrund eine Sekundenbruchteile dauernde automatisierte Auktion ab (Real Time Bidding). Bei diesen Auktionen werden Werbeflächen von den Unternehmen, die die Webseite betreiben, angeboten und unter den Firmen, die Werbung dort einblenden lassen wollen, versteigert. Das höchstbietende Unternehmen erhält den Zuschlag. Ob es dabei interessant ist, bei der Auktion mitzubieten, hängt davon ab, wer der/die Nutzer*in ist, welche die Werbung sehen soll.[12] Um ein umfassendes Bild über diese/n Webseitenbesucher*in zu erzeugen, werden drei Arten von zuvor erfassten Daten verknüpft. Das sind

- Daten aus erster Hand von der Webseite selbst: Onlineshops analysieren bspw. Verhalten, Handlungen und Interessen. Kehren Besucher*innen auf die Webseite zurück, sind schon einige Informationen über diese Personen bekannt, wobei die Identifikation bspw. durch Auslesen verschiedener Merkmale des genutzten Endgeräts erfolgen kann: Smartphones, Computer etc. besitzen verschiedene unveränderliche Erkennungsmerkmale wie bspw. die IMEI.

- Daten aus zweiter Hand: Sie stammen von einem Mittler im beschriebenen Vergabeprozess von Werbeflächen und umfassen bspw. statistische Auswertungen von Cookies der Nutzer*in;
- Daten aus dritter Hand: Sie stammen von anderen Websites, die von externen Anbietenden wie den erwähnten Data Broker bereitgestellt werden.[13]

Eine Studie der NGO Irish Council for Civil Liberties (ICCL) offenbart den Umfang dieser Datensammlung und -weitergabe: Allein Google – die größte Firma im beschriebenen Vergabeprozess – verkauft in jeder Minute 19,6 Millionen Datensätze von deutschen Nutzer*innen an über tausend andere Firmen. Was ein/e Nutzer*in aktuell im Internet sucht oder betrachtet, wird von Google individuell in jeder Minute Online-Zeit einmal erfasst.[14] Wie sehr sich das Geschäft rund um Datenerfassung, Datenhandel und die letztendliche exakte Ausrichtung auf Zielgruppen lohnt, zeigt sich darin, dass der Markt für Online-Werbung in Deutschland 2020 laut des Bundesverbands digitale Wirtschaft einen Umsatz von mehr als vier Milliarden Euro erzeugte.[15]

Dass durch die beschriebenen Vorgänge und Geschäftspraktiken durchaus große Probleme für individuelle Nutzer*innen, die gesamte Gesellschaft sowie Politik, Verwaltung und andere staatliche Institutionen entstehen, ist größtenteils nicht direkt zu durchschauen. Die tatsächlichen Vorgänge liegen häufig absichtlich kompliziert hinter einer großen Menge Rauch und Spiegel. Dennoch sind die Konsequenzen real und aus den im Folgenden dargelegten Gründen sehr ernst zu nehmen.

Ein sensibles Gut

Personenbezogene Daten sind sensible Informationen. Daher soll Datenschutz Individuen vor missbräuchlicher Datenverarbeitung schützen und den Schutz des Grundrechts auf informationelle Selbstbestimmung wahren. Datenschutz schützt folglich keineswegs Daten – sondern Menschen und deren Persönlichkeitsrechte. Personenbezogene Daten freiwillig oder unfreiwillig zu offenbaren, bringt eine Vielzahl von Gefahren mit sich, da auf das Recht auf Datenschutz verzichtet wird.

Das Missbrauchspotenzial personenbezogener Daten ist enorm, was folgende Beispiele zeigen: Data Broker verwendeten Nutzerdaten, um Teilnehmer*innen von Black-Lives-Matter-Demonstrationen zu identifizieren. Verschiedene US-amerikanische Geheim- und Sicherheitsabteilungen nutzen diese Daten, um ohne Gerichtsbeschluss Telefone zu tracken. Im Zuge der Untersuchung für die bereits erwähnte Studie der ICCL wurde entdeckt, dass die Daten von vermutlichen Opfern sexueller Gewalt verkauft wurden.[16] An diesen Beispielen zeigt sich, wie sensibel personenbezogene Daten wirklich sind. Demonstrierende, die von ihrem Recht auf Versammlungsfreiheit Gebrauch machen, können über kurze, undemokratische Umwege vom Staatsschutz beobachtet werden. Opfer sexueller Gewalt werden mit erhöhter Wahrscheinlichkeit später wieder Opfer.[17] Der Autor überlässt es der Fantasie der Leser*innenschaft, für welche Personen Daten von Opfern sexueller Gewalt interessant sein könnten.

Interesse an dem Hintergrund von Personen besteht auch in anderen Zusammenhängen. Unternehmen verschiedener Branchen greifen auf die gesammelten Daten von Data Brokern zurück. Dazu zählen Banken – z. B. um das Rückzahlungsrisiko einer Darlehensanfrage zu ermitteln[18], Versicherungen – z. B. um auf Basis gekaufter Gesundheitsdaten einen Score einer Person zu ermitteln, der direkten Einfluss darauf hat, wie teuer eine Lebensversicherung sein wird[19] – oder Unternehmen – z. B. für einen Background-Check von Bewerber*innen. Die persönlichen Kontakte, fragwürdige Interessen, riskante Hobbies oder eine schlechte Einstufung bei Wirtschaftsauskunfteien wie der SCHUFA können deutlichen Einfluss auf Versicherungsbeiträge, Darlehensbedingungen oder die Vergabe von Arbeitsplätzen haben. Die genannten Beispiele, Banken, Versicherungen und Unternehmen, können deutlichen Einfluss auf Schicksale von Individuen haben. Daher sind sie nur bedingt Luxusprobleme. Trotzdem muss an dieser Stelle weiter gedacht werden: Wenn es so einfach ist, auf unsere digitalen Abbilder zuzugreifen – wie ergeht es dann Menschen in Ländern, in denen z. B. Homosexualität noch unter Strafe steht oder die zu einer anderen geächteten Minderheit gehören? Und auch die rein technische Ebene bringt Probleme mit sich: Im Rahmen zunehmender Automatisierung von Entscheidungen wird immer weniger hin-

terfragt, ob die ermittelten Daten einer Person richtig und plausibel sind.[20] Systeme Künstlicher Intelligenz (KI) dehumanisieren Entscheidungsprozesse und durch die Intransparenz der Entscheidungen von KI-Systemen sind Betroffene oft nicht in der Lage, Entscheidungen zu verstehen oder zu beeinflussen. Auch wird ihnen ohnehin meist nicht mitgeteilt, dass der betreffende Prozess zumindest teilweise automatisiert ist.

Sammlung von Daten ohne Einwilligung

Die Datenschutz-Grundverordnung dient einem Interessenausgleich. Je nach Situation lässt sich auf ihrer Grundlage entscheiden, wann der Persönlichkeitsschutz einer betroffenen Person oder das Recht von Unternehmen, mit Daten wirtschaftlich zu arbeiten, überwiegt.[21] Jede Verarbeitung von personenbezogenen Daten stellt eine Einschränkung dieses Persönlichkeitsrechts dar. Daher bedarf es nach Art. 7 der DSGVO einer Einwilligung der betroffenen Person zu dieser Verarbeitung. Aber: Ein Großteil personenbezogener Daten wird bei der Nutzung von digitalen Endgeräten ohne diese notwendige Einwilligung der Nutzer*innen gesammelt.[22]

Apps auf einem Smartphone mit Android als Betriebssystem müssen die Berechtigung der Nutzer*innen erfragen, wenn bspw. Standortdaten, die Kontaktliste oder andere schützenswerte Informationen erfasst werden sollen. Ein Messenger möchte etwa die Kontaktliste nutzen, bei einer Wetter-App kann es sinnvoll sein, den Standort freizugeben. Der Zugriff darauf muss von den Nutzer*innen aktiv erlaubt werden – eigentlich. Eine Untersuchung aus dem Jahr 2019 zeigte jedoch, dass mehr als 1.000 Apps des Google Play Store eine Verweigerung dieser Berechtigungen ignorieren.[23]

Internetbrowser können so eingestellt werden, dass die Nutzer*innen nicht auf ihrem Weg durch das Internet getrackt werden sollen. Dies ist keine Blockierung, sondern eine Bitte, die der Browser an Webseiten übermittelt. Diese Bitte kann daher auch ignoriert werden. Selbst wenn die Bitte, nicht verfolgt zu werden, ignoriert wird, gibt es diverse Methoden, Nutzer*innen online zu identifizieren. Eine Möglichkeit sind Cookies, bei denen es sich um kleine Datenschnipsel handelt, die auf den Endgeräten der Nutzer*innen gespeichert sind und von außen ausgelesen werden können. Cookies erfüllen verschiedene Funktionen. Sie dienen z. B. dazu, Nut-

zer*innen bei einem erneuten Besuch einer Website wiederzuerkennen und die Seite wieder so darzustellen, wie es der/die Nutzer*in zuvor eingestellt hat. Andere Cookies hingegen sammeln Informationen über die Nutzer*innen, z. B. darüber, welche Seiten besucht wurden. Die Cookies werden auf den Wegen durch das Internet mit weiteren Informationen angereichert und enthalten im Laufe der Zeit sehr viele Informationen, die an eine Vielzahl von Data Broker abfließen.[24] Um dies zu verhindern, müssen Nutzer*innen beim Besuch vieler Webseiten zunächst einige Mühe investieren: Wenn sie die Menge an sensiblen Daten, die über sie gesammelt werden können, begrenzen wollen, ist es in der Regel notwendig, die Verwendung von Cookies und Trackern zu verweigern. Das ist meist sehr aufwendig. Und auch wenn dieser Aufwand nicht gescheut wird, verfehlt die Mühe nicht selten ihr Ziel: Nutzer*innen werden teilweise durch die Gestaltung dieser Cookie Banner zu einer unfreiwilligen Einwilligung gedrängt oder die Banner werten eine Ablehnung der Cookies als Einwilligung.[25]

Angenommen, die Cookies wurden erfolgreich abgelehnt. Trotzdem findet eine teilweise sehr direkte Beobachtung und Datafizierung[26] der Nutzer*innen statt. Dies gilt bspw. für Nutzungsdaten. Diese Daten geben Auskunft darüber, wie Nutzer*innen mit einer Website interagieren. Onlinehändler wie Amazon erfassen exakt die Klicks, Mausbewegungen und Verweildauern auf ihren Seiten.[27] Das soziale Netzwerk Facebook trackt die Nutzer*innen auf 18 verschiedene Weisen, darunter auch in Bezug darauf, welche Apps auf dem Endgerät installiert sind, welche Dokumente und Dokumententypen dort gespeichert sind sowie eine Vielzahl von Informationen über andere Geräte, die sich im selben Netzwerk befinden.[28] Diese Daten ergeben insgesamt ein recht umfassendes Bild der Nutzer*innen: Die Verweildauer und Scroll-Bewegungen verraten, welche Produkte bei Amazon besonderes Interesse erwecken. Welche Nutzer*innen zusammenwohnen wird offenbar, wenn häufiger Zugriff auf Facebook derselben Geräte über denselben Internetanschluss stattfindet. Dadurch lässt sich auch ein sozialer Graph erstellen – eine grafische Darstellung des Beziehungsgeflechts von Personen.[29] Facebook verwendet diese Informationen, bspw. um neue Freund*innen vorzuschlagen. Für die Nutzer*innen ist oft nicht nachvollziehbar, warum Facebook dadurch

auch Ex-Freund*innen, Vorgesetzte oder andere Personen, mit denen die Nutzer*innen auf keinen Fall verbunden sein wollen, vorschlägt. Aber das entsteht durch die Analyse des Netzwerks, das Facebook erfasst.[30]

Ein mangelhafter Schutz personenbezogener Daten

Für Nutzer*innen geht jede Freigabe personenbezogener Daten immer mit dem Risiko einher, dass Personen unrechtmäßig Zugang zu vertraulichen, sensiblen oder anderen schützenswerten Daten haben. Und solche Datenlecks (Data Breaches) kommen sehr häufig vor.[31] Data Breaches entstehen in der Regel aus zwei Gründen: Im Fall schlichter Fahrlässigkeit werden Daten von Personen bspw. ungeschützt an öffentlich zugänglichen Stellen im Internet aufbewahrt. Dies geschah z. B. 2019 mit 800 Millionen Datensätzen von Hypothekenkund*innen der First American Financial Bank.[32] Die zweite Variante sind Hackerangriffe. Diese Form der Cyberkriminalität ist nicht hauptsächlich auf Industriespionage fokussiert, sondern auf personenbezogene Daten.[33] Das bislang größte Datenleck durch einen solchen Hackerangriff entstand zwischen 2014 und 2016 beim Internetkonzern Yahoo. Dabei wurden die Daten sämtlicher drei Milliarden Nutzer*innen gestohlen.[34] Für den Erfolg einer solchen Attacke bedarf es häufig nicht einmal besonderer Begabung. Es gibt zwar keinen perfekten Schutz von Daten, aber selbst große Konzerne – seien diese nun Teil der Datenökonomie oder nicht – investieren wenig Geld in Cybersicherheit.[35] Dies mag neben den hohen Investitionen damit zusammenhängen, dass sich Daten im Gegensatz zu physischen Objekten durch Kopieren nicht abnutzen. Es könnte daher rein ökonomisches Kalkül sein, dass Daten nachlässig geschützt werden. Für jede betroffene Person ist der unrechtmäßige Zugang zu ihren Daten aber ein großes Problem. Dies sollte zu denken geben, wenn bspw. der Chrome-Browser von Google so eingestellt ist, dass er automatisch Zugangsdaten speichert.

Ein »Opt-out«

Angesichts der genannten Aspekte wäre es sinnvoll, möglichst wenige Daten offenzulegen. Nur ist ein *Opt-out* – eine Verweigerung der computergestützten Verarbeitung personenbezogener und Metadaten – nicht

mehr möglich.[36] Eine Vielzahl von Behörden wie das Finanzamt, die Zulassungsstelle oder das Bürgerbüro verarbeiten seit Jahrzehnten personenbezogene Daten digital, was im Rahmen der verstärkt vorangetriebenen »E-Verwaltung« weiter ausgebaut wird.[37] Und medizinische Daten sollen zukünftig automatisch in der »elektronischen Patientenakte« hinterlegt werden.[38] Der Nutzung muss erst aktiv widersprochen werden, um nicht an der zentralisierten Verarbeitung der medizinischen Daten teilzunehmen.[39] Reisepässe und Personalausweise enthalten inzwischen biometrische Daten und gehen bei Pass- und Personenkontrollen durch eine Vielzahl von Händen und Scannern. Eindeutig ist, dass als Nutzer*in des Internets eine Vermeidung der großen Technologiekonzerne nicht mehr möglich ist: Selbst, wenn ein/e Nutzer*in Dienste wie Maps, Gmail oder Facebook meidet, stammen Analyse-Tools oder Schriftarten häufig von Google, Werbeanzeigen meist von Google oder Meta.[40] Folglich fließen ohne bewusste Nutzung der Dienste der Digitalkonzerne Daten des/der Nutzer*in nachlässig verschlüsselt[41] in die USA und unterliegen dort – trotz aktueller Bemühungen um neue Datenschutzabkommen[42] – einem im Vergleich zur DSGVO deutlich geringeren Datenschutzniveau.[43]

Die Konsequenz ist eine besondere Form digitaler Spaltung, die sich bspw. darin zeigt, dass Kindertagesstätten und Schulen mit Eltern immer häufiger nur noch mittels spezieller Smartphone-Apps kommunizieren. Eine Verweigerung der Technologie führt dazu, wichtige Informationen im Zweifelsfall nicht zu erhalten. Es gibt daher bei vielen Vorgängen des Alltags keinen Weg mehr, der an der Nutzung des Internets und digitaler Endgeräte vorbeiführt. Das erzeugt inzwischen ein Problem auf Ebene der Teilhabe: Allein in Deutschland gibt es in der Altersgruppe zwischen 16 und 74 Jahren 6 % Offliner, die noch nie das Internet genutzt haben.[44]

Wie wichtig ein Internetzugang ist, hat die Corona-Pandemie gezeigt. Homeschooling und Homeoffice waren spontan gute und die einzigen Möglichkeiten, Bildung und Betriebe am Laufen zu halten – keine Frage. Aber es ist ein zweischneidiges Schwert: Einerseits lässt der Breitbandausbau in Deutschland nach wie vor zu wünschen übrig. Andererseits sind die Nutzer*innen in einem kommerzialisierten Internet einer dauerhaften Überwachung ausgesetzt.

Regulierungsmangel und Corporate Capture

In Artikel 8 der Charta der Grundrechte der Europäischen Union ist zu lesen: »Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden.«[45]

Der Wert personenbezogener Daten für die Rechte und Freiheiten von Individuen steht auf politischer Ebene fest. Dennoch basieren Geschäftsmodelle, ohne die diverse Technologiekonzerne nicht existierten, auf der Nutzung dieser Daten. Und diese Nutzung liegt – wie zuvor gezeigt – häufig außerhalb der zitierten »gesetzlich geregelten legitimen Grundlage«. Das bedeutet, dass die Öffentlichkeit vor dieser Zuwiderhandlung geschützt werden muss. Dies geschieht jedoch nicht in ausreichendem Maß. Denn die Entwicklungen der großen Technologiekonzerne und die entstandene Datenökonomie wurden von politischer Seite zu lange ignoriert oder – wie später gezeigt werden wird – sogar tatkräftig unterstützt.

Wer das Internet kontrolliert, steht fest. Die gesetzgebende Seite steht vor vollendeten Tatsachen und die Sachlage weist inzwischen ein hohes Maß an Komplexität auf. Dadurch fallen Regulierungsmaßnahmen im Sinne der Rechte von Nutzer*innen schwer. Dafür gibt es verschiedene Gründe:

Zunächst sind Gesetzgebungsverfahren zeitintensiv. Das ist im Hinblick auf den zugrunde liegenden Sachverhalt ungünstig. Denn die privatwirtschaftliche Nutzung personenbezogener Daten basiert auf dem Einsatz digitaler Technologien, die mit zunehmender Geschwindigkeit Innovationen in Form von Geräten und Plattformen hervorbringen, deren Aus- und Einwirkungen nicht unmittelbar abzuschätzen sind. Die Wahrscheinlichkeit ist damit groß, dass Gesetze nicht selten ihre Wirkung durch zwischenzeitlich veränderte Rahmenbedingungen verfehlen. Die fachliche Expertise der entscheidenden und beratenden Gremien im Gesetzgebungsprozess ist ebenfalls durch die Geschwindigkeit der technologischen Entwicklung nur bedingt gegeben.

Diese Verzögerungen sind ein Ankerpunkt für die Technologiekonzerne, die u. a. auf die Europäische Kommission und das Europäische Parlament Einfluss nehmen. Es handelt sich um gezielte Lobbyarbeit und

Desinformation der demokratisch legitimierten Entscheidungsträger*innen. Diese Einflussnahme gilt Gesetzesvorlagen wie der Datenschutz-Grundverordnung, die dem Schutz der Öffentlichkeit dienen sollen. Durch dieses *Corporate Capture* werden Gesetzesvorlagen im Sinne der Geschäftsmodelle der Technologiekonzerne verändert und dienen zumindest nur noch in geringerem Umfang dem Gemeinwohl.[46]

Ein weiterer Grund, weshalb Gesetze für den Schutz der Nutzer*innen speziell im Bereich ihrer Daten einen niedrigen Wirkungsgrad erreichen, liegt in der mangelhaften Durchsetzung bzw. Sanktionierung. Das folgende Beispiel kann für eine überaus verzögerte und unzulängliche Einhaltung der rechtlichen Vorgaben angeführt werden: Die Datenschutzbeauftragten der Bundesländer wollen, nachdem die DSGVO bereits seit 2018 in Kraft ist, den Handel mit postalischen (!) Adressen für Briefkastenwerbung unterbinden. Dieser sei mit der DSGVO nicht vereinbar.[47]

Natürlich ist dieser Datenhandel ein Problem, zumal betroffene Personen keinerlei Transparenz haben, in welchen Datenbanken und welcher Form welche Daten vorliegen. Und dadurch lässt sich auch ein Verbot der Nutzung dieser Daten kaum bewerkstelligen. Aber gibt es im Zeitalter des Digitalkapitalismus nicht andere, dringendere Konflikte?

Privacy Paradox

Wenn die politischen Akteure aufgrund der Komplexität oder wegen Beeinflussung von großen Technologiekonzernen die Öffentlichkeit nicht schützen, müssen Nutzer*innen ihre Rechte selbst wahren. Und das Interesse, die eigenen Daten in und außerhalb des Internets zu schützen, ist hoch.[48] Das *Privacy Paradox* besteht darin, dass die wenigsten Nutzer*innen Datenschutz auch aktiv betreiben.

Für diese Lücke zwischen Einstellung und Verhalten gibt es verschiedene Gründe: Bemühungen um den Datenschutz benötigen in der Regel die Anwendung eines gewissen technischen Know-how oder setzen das Lesen und Nachvollziehen langer juristischer Texte voraus. Hinzu kommt, dass Nachlässigkeit gegenüber dem Schutz der eigenen Daten verschiedentlich belohnt wird. Dies zeigt sich bspw. in den Ergebnissen der im Folgenden beschriebenen Untersuchung.

Die Proband*innen einer US-amerikanischen Studie sollten sich vorstellen, Kund*innen eines Supermarkts zu sein. Dieser Supermarkt gibt einen Rabatt auf den Einkaufspreis als Gegenleistung für die Zustimmung, Informationen über die Kund*innen zu sammeln. Ziel der Untersuchung war es, den genauen Punkt zu ermitteln, ab welcher Tiefe der Datensammlung die Befragten dieses Angebot ablehnen. Mit dem Sammeln der Informationen waren 43 % der Befragten grundsätzlich einverstanden. Nur noch 21 % waren es, wenn die Daten dazu genutzt würden, ihr Einkommen zu ermitteln. Nur noch 19 % waren damit einverstanden, dass die Daten dazu genutzt würden, ihre ethnische Herkunft zu ermitteln.[49] Das Interessante daran ist Folgendes: Solcherlei Informationen werden tagtäglich ermittelt und die meisten Nutzer*innen sind damit einverstanden bzw. ignorieren den Umstand, dass bspw. Facebook den Browserverlauf der Nutzer*innen ausliest.[50] Die Allgemeinen Geschäftsbedingungen oder die Datenschutzrichtlinien, die klar benennen, welche Daten von den Nutzer*innen gesammelt werden, sind lang und nicht ohne Weiteres verständlich. Im Vergleich dazu ist der Klick auf *Consent* eine geringe Hürde. Und schließlich erhalten Nutzer*innen als Gegenleistung Zugang zu einer App, einem Spiel oder einem sonstigen Dienst. Das ist die Belohnung dafür, keinen Gebrauch von ihren Grundrechten zu machen und im Zweifelsfall intime Details Konzernen und Datenhändlern preiszugeben. Schuldzuweisungen sollten jedoch vermieden werden. Es ist zwar inzwischen in der Öffentlichkeit kein Geheimnis mehr, dass Meta und andere Technologiekonzerne die Nutzer*innen ausspionieren. Aber Netzwerkeffekte sind eine zentrale Mechanik von Plattformen. Nicht bei einer derzeit sehr populären Social-Media-Plattform dabei zu sein, kann zumindest bei jüngeren Menschen zu einer partiellen digitalen Spaltung auf sozialer Ebene führen. Und auch ältere Nutzer*innen haben wie zuvor beschrieben teilweise keine Wahl, bestimmte Apps nicht zu nutzen.

Zudem muss an dieser Stelle das bekannte soziologische Phänomen einer Diskrepanz zwischen Einstellung und Verhalten mitgedacht werden.[51] Wie beim Thema Umweltbewusstsein besteht ein sehr geringer Zusammenhang zwischen dem in Umfragen gemessenen Wert eines hohen Umweltbewusstseins und dem Handeln im Alltag, das dieser Einstellung

entspricht.[52] Ein starker Zusammenhang zwischen Umweltbewusstsein und entsprechendem Umwelthandeln zeigt sich meist in *Low-Cost*-Situationen, in denen Umwelthandeln nicht mit einem großen Aufwand auf Ebene von Komfort, Zeitaufwand etc. verbunden ist – bspw. Mülltrennung.[53] Übertragen auf das Privacy Paradox bedeutet das, dass der gemessene Wert, Datenschutz als wichtig zu erachten, sich nur dann in eine Handlung übersetzt, wenn der Aufwand dafür niedrig ist. Allerdings stützt diese Überlegung lediglich die These, dass es mit einem hohen Aufwand verbunden ist, im digitalen Alltag den Wunsch nach Schutz der eigenen Daten wirkungsvoll durchzusetzen. Die Differenz zwischen dem Wunsch nach Privatsphäre bzw. Datenschutz und einem entsprechenden Handeln ist in diesem Fall kein verzerrtes Ergebnis durch soziale Erwünschtheit. Vielmehr zeigt sich an dieser Stelle ein Anteil der Taktiken, die Technologiekonzerne für den Erfolg ihrer Geschäftsmodelle nutzen: lange, schwer verständliche allgemeine Geschäftsbedingungen, Datenschutzrichtlinien und andere juristische Texte lassen selbst die motiviertesten Nutzer*innen irgendwann verzweifeln und mit schlechtem Gewissen auf Consent tippen.

Das Dilemma

Nun stellt sich die Frage, wie dieses Dilemma gelöst werden kann. Es wurde gezeigt, dass Datenschutz sehr wichtig ist und auch auf individueller Ebene als wichtig erachtet wird. Die politische Seite greift aus verschiedenen Gründen nur bedingt ein, während mehrere Wirtschaftszweige nur durch Beugung des Datenschutzes und Einschränkung der Privatsphäre existieren. Im Folgenden werden drei zentrale Prozesse dargestellt, welche die Entwicklung des Digitalkapitalismus begünstigt haben. Anschließend wird in Kapitel 3 dargestellt, dass der Digitalkapitalismus im Vergleich zu vorangegangenen Epochen des Kapitalismus als eine eigenständige und neue Epoche angesehen werden kann. Im Anschluss daran werden die zentralen Charakteristiken, die mit dem Digitalkapitalismus einhergehen, beleuchtet: das Plattform-Geschäftsmodell, die Einschränkung von Privatsphäre und Datenschutz sowie die Aushöhlung demokratischer Prozesse und Institutionen. Da Künstliche Intelligenz eine besondere Rolle im Digitalkapitalismus spielt, findet diese ebenfalls Betrachtung.

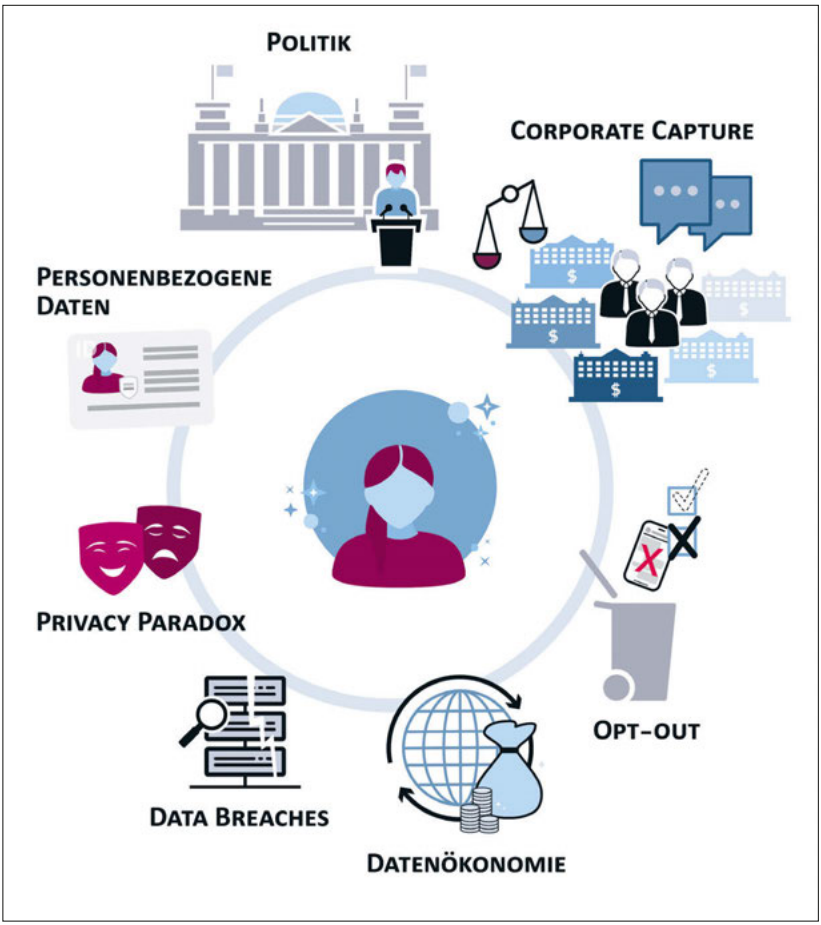

Abb. 1: Zusammenfassende Darstellung des Dilemmas

In Kapitel 4 wird das Werkzeug vorgestellt, das wie der »Nutri-Score« funktioniert, der seit einigen Jahren auf der Verpackung von Lebensmitteln zu finden ist. Dieser Score teilt den Verbraucher*innen mittels eines fünfstufigen Ampelsystems von grün (»A«) bis dunkelrot (»E«) auf einen Blick mit, wie *gesund* das Lebensmittel ist. Berücksichtigt wird das Verhältnis des Fett-, Salz- und Zuckergehalts des Produkts. Dieser Nutri-Score ist eine Vorlage für das Tool, das der Autor erfunden und »Priva

Score« genannt hat. Mittels des Priva Scores ist es Nutzer*innen möglich, die Höhe des Datenschutzstandards eines Internetdiensts oder eine App vor der Nutzung zu vergleichen und mittels eines niedrigschwelligen, transparenten Bewertungsschemas eine informierte Entscheidung zu treffen. Durch den Einsatz dieses Werkzeugs besteht die Möglichkeit, in Bezug auf den Datenschutz und die Privatsphäre zwischen den großen Technologiekonzernen, die den Digitalkapitalismus vorantreiben, und den Nutzer*innen von Diensten und Apps eine bessere Balance zu erreichen. Die Vorteile eines solchen Tools sind vielfältig: Es sind weder technische Kenntnisse noch sonstiges Fachwissen erforderlich, es erübrigt sich das blinde Vertrauen gegenüber Konzernen, dass diese mit teils hochsensiblen Daten verantwortungsvoll umgehen, und es reduziert den Einfluss des zentralen Geschäftsmodells des Digitalkapitalismus bei Nutzung der untersuchten Apps: Sammlung, Verarbeitung und Monetarisierung personenbezogener und Metadaten. Mehr Freiraum wird gewonnen – jedoch sprengt es nicht den goldenen Käfig.[54]

Daher wird am Beispiel von vier verschiedenen Messengerdiensten sowohl die Funktion als auch die Berechnung des Priva Scores demonstriert.

ANMERKUNGEN

1 Dick 1969/2003: 41

2 Zum Beispiel Name, Telefonnummer, Anschrift, E-Mail-Adresse, Geburtsdatum oder die IP-Adresse (Art. 4, Abs.1 DSGVO).

3 Verhaltensdaten beinhalten Informationen über die Handlungen, Gewohnheiten und Verhaltensmuster einer Person oder wie sie bspw. mit einem Produkt oder einem Dienst, einer Plattform etc. interagiert (Zuboff 2019: 74 ff.). Deren Sammlung kann bspw. durch die Aufzeichnung der Online-Aktivitäten einer Nutzerin gesammelt werden oder der körperlichen Bewegungen, gemessen durch eine Smartwatch o. ä. Verhaltensdaten können als eine Art von Metadaten betrachtet werden, da sie Informationen über das Verhalten einer Person liefern und nicht den Inhalt ihrer Kommunikation oder personenbezogene Daten.

Der Begriff Verhaltensdaten wird in diesem Buch trotzdem spezifisch genannt, da Verhaltensdaten eine besondere Form von Daten darstellen. Sie erlauben Einblicke in individuelle Vorlieben, Gewohnheiten und Routinen. So ist es sehr einfach, ein relativ exaktes Profil einer Person zu erstellen, was im Kontext dieses Buchs zumindest als Verletzung der Privatsphäre angesehen werden kann.

4 Daten über Daten: Spracheinstellungen, Aufenthaltsort, Daten über das genutzte Gerät, … (Mayer-Schönberger/Cukier 2013: 93).

5 merriam-webster.com 2023

6 Sühlmann-Faul 2020: 106

7 Morozov 2018

8 Ein Digitales Ökosystem ist ein soziotechnisches System, in dem Unternehmen und Menschen kooperieren, die zwar unabhängig sind, sich von der Teilnahme aber einen gegenseitigen Vorteil versprechen. Ein Digitales Ökosystem hat in seinem Zentrum eine digitale Plattform, die diese Kooperation über Ökosystem-Dienste besonders gut unterstützt (Bartels/Schmitt 2023).

9 Brynjolfsson et al. 2019: 155 ff.

10 Der Begriff wird hier eng gefasst und beschreibt ausschließlich den Austausch und Handel von und mit Daten. Streng genommen umfasst der Begriff die gesamte, zunehmend datenbasierte Form des Wirtschaftens, das sich durch den Einsatz digitaler Technologien verändert

(Deutsche Bundesregierung 2021).

11 Richter 2017

12 Wang et al. 2017: 8 ff.

13 Wang et al. 2017: 11 ff.

14 Irish Council for Civil Liberties/Ryan 2022

15 Online-Vermarkterkreis im Bundesverband Digitale Wirtschaft 2021

16 Irish Council for Civil Liberties/Ryan 2022

17 Bellis et al. 2014

18 McKissick 2022

19 Pasquale 2016: 26

20 Pasquale 2016: 23 ff.

21 Kramer 2020

22 Mattu/Hill 2017a

23 Reardon et al. 2019

24 Seibert 2015

25 Matte et al. 2020

26 Der Begriff »Datafication«, im Deutschen »Datafizierung«, stammt von den Autoren Victor Mayer-Schönberger und Kenneth Cukier (2013). Er beschreibt die seit

dem Beginn der Kommerzialisierung des Internets zunehmende Erfassung, Speicherung und Verarbeitung gesellschaftlicher Vorgänge in Form digitaler Daten (Mayer-Schönberger/Cukier 2013: 78).

27 Véliz 2021: 7 ff.

28 Facebook Inc. 2018: 84 ff.

29 Höller/Wedde 2018: 14 ff.

30 Izusha 2022

31 Eine jeweils aktuelle Liste großer Data Breaches findet sich hier (Kurz-URL von FSF erstellt):

https://t1p.de/diss_databreach

32 Mathews 2019

33 Datenschutzpraxis 2022a

34 Larson 2017

35 Sherman et al. 2018

36 Editorial 2022

37 SPD, Bündnis90/Grüne, FDP 2021

38 Europäische Kommission 2019

39 Bundesministerium für Gesundheit 2023; Leisegang 2023

40 Guinness 2018

41 Dr. Datenschutz 2022

42 The White House 2022

43 Die USA gelten im Sinne der DSGVO als sog. *Unsicheres Drittland*. In diesen Ländern können nach Art. 44 der DSGVO europäischen Nutzer*innen nicht die Rechte und Garantien eingeräumt werden, die ihnen in europäischen Ländern durch die DSGVO zustehen.

44 Destatis 2022b

45 Europäische Union 2012

46 Alter EU (Hrsg.)/LobbyControl (Hrsg.) 2018; OECD 2019

47 Hornung 2022

48 IBM Newsroom 2019

49 Turow et al. 2015

50 Waugh 2014

51 Auch »Awareness-Action Gap«, z. B. Frayling/Dyson 2000, »Value-Action Gap«, z. B. Kollmuss/Agyeman 2002 oder »Knowledge-Attitudes-Practice Gap« bzw. »KAP Gap« Rogers 2003: 70

52 Diekmann/Preisendörfer 2001: 114 ff.

53 ebd.: 117 ff.

54 Rammler bezieht sich mit diesem Begriff auf die Trägheit einer Veränderung im Bereich der Mobilitätskultur. Auch hier herrscht ein Mangel »an der nötigen politischen Klugheit« und eine Veränderung wird durch ökonomische Rahmenbedingungen und kulturelle Pfadabhängigkeiten erschwert (Rammler 2014: 37). Diese Gemengelage herrscht beim vorliegenden Thema ebenfalls: Auf den ersten Blick paradiesische Zustände durch viele kostenlose Apps und Konsumchancen, aber letztendlich der Entzug von Grundrechten und Freiheit.

Die digitale Revolution hat unser Leben tiefgreifend verändert. Unternehmen wie Apple, Google und Meta treiben diese Veränderung voran und steuern zunehmend, wie wir arbeiten und vor allem wie die Wirtschaft funktioniert.

Doch hinter den glänzenden Oberflächen der Konzerne, hinter vermeintlichem Erfindungsgeist und kostenlosen Geschenken lauern Gefahren, besonders wenn es um unsere Demokratie, Gesellschaft und unsere Privatsphäre geht. Denn bezahlt wird der Zauber mit unseren persönlichen Daten, die zum Kapital der Zukunft geworden sind. Dieses Buch taucht tief in diese Themen ein, beleuchtet die Herkunft und die Schattenseiten des Digitalkapitalismus.

Aber es gibt einen Lichtblick: Der Autor stellt den »Priva Score« vor – ein smartes Werkzeug, das Datenschutz im digitalen Alltag erleichtert. Damit wird eine einfache Navigation durch den Datenschutzdschungel möglich, die Privatsphäre bleibt geschützt und eigene Daten unter Kontrolle.

Felix Sühlmann-Faul ist Experte für Digitalisierung und Nachhaltigkeit, promovierter Techniksoziologe, Speaker, Berater und Autor. Er war Versuchsleiter in der Daimler-Kundenforschung und Projektleiter am Institut für Transportation Design. Er berät u. a. den Deutschen Nachhaltigkeitspreis und war beim Aufbau eines deutschlandweiten Forschungsnetzwerks zu Digitalisierung und Nachhaltigkeit beteiligt.

natürlich oekom · nachhaltig seit 1989 ·