

AUS POLITIK UND ZEITGESCHICHTE

Datenökonomie

Shoshana Zuboff

SURVEILLANCE CAPITALISM –
ÜBERWACHUNGS-
KAPITALISMUS

Michael Seemann

EINE BEUNRUHIGENDE
FRAGE AN DEN DIGITALEN
KAPITALISMUS

Markus Spiekermann

CHANCEN UND
HERAUSFORDERUNGEN
IN DER DATENÖKONOMIE

Dirk Heckmann

DATENVERWERTUNG
UND DATENETHIK

Rupprecht Podszun

KARTELLRECHT
IN DER DATENÖKONOMIE

Ingrid Schneider

REGULIERUNGSANSÄTZE
IN DER DATENÖKONOMIE

Wolfe Christl

MICROTARGETING.
PERSÖNLICHE DATEN
ALS POLITISCHE WÄHRUNG

Jörn Lamla

SELBSTBESTIMMUNG
UND VERBRAUCHERSCHUTZ
IN DER DATENÖKONOMIE

APuZ

ZEITSCHRIFT DER BUNDESZENTRALE
FÜR POLITISCHE BILDUNG

Beilage zur Wochenzeitung Das **Parlament**

Datenökonomie

APuZ 24-26/2019

SHOSHANA ZUBOFF

SURVEILLANCE CAPITALISM – ÜBERWACHUNGSKAPITALISMUS

Überwachungskapitalisten wissen alles über uns. Es genügt ihnen jedoch nicht länger, den Informationsfluss *über uns* zu automatisieren, das Ziel besteht nun darin, *uns* zu automatisieren. Doch diese Entwicklung ist nicht unvermeidbar.

Seite 04–09

MICHAEL SEEMANN

EINE BEUNRUHIGENDE FRAGE AN DEN DIGITALEN CAPITALISMUS

Wie verhält es sich im Digitalen mit den gängigen Kapitalismuskriterien Kapital, Arbeit, Markt, Eigentum und Wachstum? Handelt es sich überhaupt noch um Kapitalismus? Und wenn nicht, um was handelt es sich dann?

Seite 10–15

MARKUS SPIEKERMANN

CHANCEN UND HERAUSFORDERUNGEN IN DER DATENÖKONOMIE

Die Datenrevolution ist in vollem Gange und verändert unser aller Leben. Die gewaltigen wirtschaftlichen Potenziale der Datenökonomie werden jedoch vor allem in Deutschland bei Weitem noch nicht ausgeschöpft.

Seite 16–21

DIRK HECKMANN

DATENVERWERTUNG UND DATENETHIK

Wieviel Schutz brauchen personenbezogene Daten in der Datenökonomie, wie sehr „schadet“ der Datenschutz den (redlichen) Geschäftsmodellen in der Digitalwirtschaft, die auf die Verwertung von Daten angewiesen sind?

Seite 22–27

RUPPRECHT PODSZUN

KARTELLRECHT IN DER DATENÖKONOMIE

Die Digitalisierung hat die Marktwirtschaft nicht nur durch neue Produkte oder Dienstleistungen bereichert, sondern ihre Strukturen grundlegend verändert. Das Kartellrecht steht damit vor ungekannten Phänomenen.

Seite 28–34

INGRID SCHNEIDER

REGULIERUNGSANSÄTZE IN DER DATENÖKONOMIE

Wie lässt sich eine Brücke zwischen regulierter kommerzieller Datennutzung und Gemeinwohl schlagen? Sollten Daten dafür eher als privates Gut, öffentliches Gut, Allmendegut oder mittels Treuhandschaft bewirtschaftet werden?

Seite 35–41

WOLFIE CHRISTL

MICROTARGETING. PERSÖNLICHE DATEN ALS POLITISCHE WÄHRUNG

Parteien nutzen umfassende Daten über Wählerinnen und Wähler für politische Kampagnen, insbesondere im Online-Bereich. Welche Rolle spielen Facebook und Klick-Ökonomie? Und was bedeutet das für Öffentlichkeit und Demokratie?

Seite 42–48

JÖRN LAMLA

SELBSTBESTIMMUNG UND VERBRAUCHER- SCHUTZ IN DER DATENÖKONOMIE

Selbstbestimmung wird in der Datenökonomie zu einer Herausforderung. Wir sollten in die Lage versetzt werden, kritisch prüfen zu können, welche Werte in die Entscheidungsarchitekturen digitaler Infrastrukturen eingeschrieben sind.

Seite 49–54

EDITORIAL

Daten sind heute ein wichtiges Wirtschaftsgut; manche bezeichnen sie gar als „Öl des 21. Jahrhunderts“. Die vielfältigen Möglichkeiten, sie in digitaler Form massenhaft zu sammeln, zu verknüpfen, auszuwerten und weiterzuverarbeiten, eröffnen Perspektiven für neue Geschäftsmodelle und enorme Potenziale für wirtschaftliche Gewinnerschöpfung. Davon zeugen nicht nur die Erfolgsgeschichten von „Internetgiganten“ wie Google und Facebook, sondern auch die vielen „Disruptionsgeschichten“ sogenannter Plattformunternehmen wie Uber, Airbnb oder Netflix, die in kürzester Zeit ganze Branchen umgekrempelt haben. Die Datenökonomie birgt aber auch weniger spektakuläre Beispiele für datengetriebene Innovation, etwa in der Logistik oder Landwirtschaft.

Digitale Dienste erleichtern uns in vielerlei Hinsicht das tägliche Leben; überdies sind sie erschwinglich, häufig sogar „kostenlos“. Sie sind zu einer Art Infrastruktur geworden: Wer möchte noch auf Karten-, Wetter-, Chat- oder Video-Apps verzichten? Tatsächlich „zahlen“ wir viele dieser Annehmlichkeiten aber mit unseren persönlichen Daten, die mit den Daten der anderen Userinnen und User einen Schatz bilden, den die entsprechenden Unternehmen höchst profitabel auszunutzen wissen. Angesichts dessen stellt sich die Frage, wem welche Daten „gehören“ (sollten) – und ob Daten als immaterielle und unendlich vervielfältigbare Güter überhaupt eigentumsfähig sind. Wie ließe sich ihr Wert bestimmen?

Neben diesen ökonomischen Aspekten gewinnen Fragen nach dem persönlichen Datenschutz, nach der Wahrung der Privatsphäre und letztlich der individuellen Selbstbestimmung an Dringlichkeit, zumal sich Datensammlungen auch politisch instrumentalisieren lassen. Die Europäische Datenschutzgrundverordnung (DSGVO), die Ende Mai 2018 Geltung erlangte, war mit Blick auf personenbezogene Daten ein wichtiger Schritt. Um Datenverwertung und Datenschutz langfristig in Einklang zu bringen, bedarf es jedoch weiterer, international abgestimmter Schritte – sowie aufgeklärter Bürgerinnen und Bürger.

Johannes Piepenbrink

ESSAY

SURVEILLANCE CAPITALISM – ÜBERWACHUNGSKAPITALISMUS

Shoshana Zuboff

Ich wende mich hier und heute nicht nur als Denkerin, Wissenschaftlerin und Autorin an Sie, sondern auch als Staatsbürgerin und – nicht zuletzt – auch als Mutter. Über die vergangenen beiden Jahrzehnte habe ich die Entstehung und Ausbreitung einer beispiellosen Mutation des Kapitalismus beobachtet, die ich als „Überwachungskapitalismus“ bezeichne. Und ich mache kein Hehl aus meiner Besorgnis hinsichtlich seiner Auswirkungen für unsere Ökonomien, für die Aussichten von Marktdemokratie und Privatsphäre, ja hinsichtlich seiner Bedeutung für die Zukunft des Kapitalismus selbst.

In sieben Jahren eingehender Beschäftigung mit dem Phänomen bin ich zu der Überzeugung gelangt, dass die Folgen des Überwachungskapitalismus weit hinausreichen über die traditionellen Domänen des Kapitalismus und seiner Ökonomien. Die tiefere Wahrheit ist, dass er die Gesellschaft des 21. Jahrhunderts auf eine ebenso menschen- wie demokratiefeindliche Art und Weise umwälzen wird – und das allein um des finanziellen Gewinns aus der Überwachung willen. So entstehen die größten Gefahren aus den überwachungskapitalistischen Ambitionen denn auch unseren Kindern, die schon jetzt – sozusagen als Vorhut – dieses neue Terrain durchstreifen.

Tobten die Titanenkämpfe des 20. Jahrhunderts zwischen Industriekapital und Arbeiterschaft, steht im 21. Jahrhundert das Überwachungskapital der Gesamtheit unserer Gesellschaft gegenüber, bis hinab zur und zum letzten Einzelnen. Der Wettbewerb um Überwachungserträge zielt auf unsere Körper, unsere Kinder, unsere Zuhause, unsere Städte und fordert so in einer gewaltigen Schlacht um Macht und Profit die menschliche Autonomie und demokratische Souveränität heraus. Wir dürfen uns den Überwachungskapitalismus nicht als etwas „irgendwo da draußen“, in den Fabriken und Büros einer vergangenen Ära vorstellen. Vielmehr sind seine Ziele wie sei-

ne Auswirkungen *hier* – seine Ziele wie seine Folgen sind *wir*.

Die Zukunft, die der Überwachungskapitalismus für uns bereithält, kommt auf leisen Sohlen. Wie die flüsternde Schlange im Garten Eden bedient er sich unseres Sehns nach Befreiung von Anonymität, Stress, Ungleichheit und institutioneller Gleichgültigkeit. Seine Perspektive ist die der verlockenden ersten Person; in der Sprache von „Selbst-Ermächtigung“, „Personalisierung“ und „Bequemlichkeit“ versichert er uns, Hilfe sei bereits unterwegs. Lassen Sie mich Ihnen jedoch eines sagen, meine Freunde: Hilfe ist mitnichten unterwegs – aber *wir*. Und zwar unterwegs zu einem umfassenden Verständnis des Überwachungskapitalismus und seiner Gefahren. Ich habe beträchtliche Zeit auf die Benennung des Phänomens verwandt, weil ich weiß, eine solche ist der erste Schritt, diese aus dem Ruder gelaufene Spielart des Kapitalismus an die Kandare zu nehmen, ihr Einhalt zu gebieten, ja sie sogar für rechtswidrig zu erklären zugunsten der Werte und Freiheiten, die es braucht, um die Autonomie des Einzelnen und die demokratische Perspektive für unsere Familien und künftige Generationen zu hegen, zu verteidigen und zu schützen.

Mein neues Buch, „Das Zeitalter des Überwachungskapitalismus“,⁰¹ beschäftigt sich mit drei Themenkreisen: erstens mit den grundlegenden Mechanismen und ökonomischen Imperativen des Überwachungskapitalismus; zweitens mit der beispiellosen, von diesen ökonomischen Imperativen angestoßenen Machtform; und drittens mit den Implikationen beider für die Gesellschaft des 21. Jahrhunderts. Lassen Sie mich hier mit der Frage beginnen: „Was ist Überwachungskapitalismus?“ So kurz ich mich notwendigerweise fassen muss, hoffe ich doch, mit meinen Gedanken einen neuen Diskurs anzustoßen und dass so einige von uns neue Wege zur gemeinsamen Arbeit an einer digitalen Zukunft finden, die wir als Zuhause bezeichnen können.

WAS IST ÜBERWACHUNGSKAPITALISMUS?

Seit Langem schon sind wir uns einig über die Entwicklungsmechanismen des Kapitalismus – dass er außerhalb der Marktdynamik Existierendes in Beschlag nimmt und in ein Marktgut verwandelt. Der Historiker Karl Polanyi sah 1944 in seiner grandiosen Abhandlung „The Great Transformation“ die Ursprünge einer sich selbst regulierenden Marktwirtschaft in drei ebenso erstaunlichen wie kritischen Erfindungen, die er als „Warenfiktionen“ bezeichnete. Die erste davon war, dass unser Menschenleben sich der Marktdynamik unterordnen und – als „Arbeit“ wiedergeboren – kaufen beziehungsweise verkaufen lässt. Die zweite war, dass Natur sich – als „Land“ oder „Grundbesitz“ wiedergeboren – auf den Markt „bringen“ lässt. Die dritte bestand darin, dass Austausch als „Geld“ wiedergeboren werden kann. Das Zeitalter des Überwachungskapitalismus hat seinen Ursprung in einer gar noch verblüffenderen und kühneren Erfindung: Er erklärt Erfahrungen von Privatmenschen zum kostenlosen Rohstoff für Produktion und Verkauf.

Ist menschliche Erfahrung erst einmal für den Markt beansprucht, wird sie zur Berechnung in Verhaltensdaten übertragen und analysiert. Und auch wenn ein Teil dieser Daten der Verbesserung von Produkten oder Dienstleistungen dienen mag, der Rest wird zum proprietären „Verhaltensüberschuss“ (*behavioral surplus*) erklärt. Dieser Überschuss umfasst Daten von erheblichem Vorhersagewert, die weit über alles hinausgehen, was man zur Verbesserung eines Produkts oder einer Dienstleistung braucht. Seien Sie sich darüber im Klaren: Wenn von aus menschlicher Erfahrung extrahiertem Verhaltensüberschuss die Rede ist, bleibt nichts ausgenommen. Ihren Ursprung hatten diese Operationen in dem Verhaltensüberschuss, der aus unserem Online-Verhalten – Browsing, Suche, Social Media – gewonnen wurde, sie erfassen heute jedoch jede Bewegung, jedes Gespräch, jeden Gesichtsausdruck, jeden Laut, jeden Text, jedes Bild, das der ubiquitären, rund um die Uhr arbeitenden Extraktionsarchi-

tektur zugänglich ist oder künftig zugänglich sein wird. Ich habe dieser Architektur den Namen *Big Other* gegeben.

In dieser digitalen Umklammerung wird jedes „smarte“ Gerät, jedes Interface, jeder Touchpoint zum Knotenpunkt eines unermesslichen Nachschubnetzes, das einzig dem Aufspüren, Verfolgen, Herbeiführen und Extrahieren von weiterem Verhaltensüberschuss dient. Triebfeder dieser Jagd ist ein ganz neues, vom Wettbewerb bestimmtes Ringen. In einer Welt allzeit verfügbarer Produkte und Dienstleistungen wenden sich heute Unternehmen dem Verhaltensüberschuss als lang ersehnte Erfolgsroute zu höheren Gewinnen zu. Ergebnis dieser Entwicklung sind ganze Ökosysteme von Verhaltensüberschusslieferanten, da Unternehmen aller Sektoren Mittel und Wege suchen, von dieser universellen Enteignung privater Erfahrung zu profitieren.

In diesen wachsenden Beständen von proprietärem Verhaltensüberschuss finden Sie Ihre Tränen, Ihre zornige Miene, die Geheimnisse, die Ihre Kinder mit ihren Puppen teilen, unsere Frühstücksunterhaltung, unsere Schlafgewohnheiten, den Lärmpegel in unserem Wohnzimmer, die Anordnung der Möbel darin, Ihre zerschlissenen Joggingschuhe, Ihr Zögern beim Anblick eines Pullovers auf einem Ladentisch und die Ausrufezeichen in Facebook-Postings, die man früher einmal völlig arglos und voll Hoffnung in die digitale Entwicklung schrieb. Diese neuen Versorgungsketten sind der Nachschubweg für ein neues „Produktionsmittel“, das uns als „Maschinenintelligenz“ bekannt ist. Hierbei handelt es sich um New-Age-Fabriken, in denen Verhaltensüberschuss zu etwas verarbeitet wird, was ich als „Vorhersageprodukte“ (*prediction products*) bezeichne: Kalkulationen, die ahnen, was wir jetzt, bald oder irgendwann tun. Diese Vorhersageprodukte werden schließlich in rasantem Tempo vom Markt leben absorbiert und in eigens für Vorhaltensvorhersagen konstituierten Märkten gehandelt, die ich „Verhaltensterminkontraktmärkte“ (*behavioral futures markets*) nenne. Aufgrund der Zahl der Unternehmen, die darauf aus sind, Wetten auf unser künftiges Verhalten abzuschließen, haben Überwachungskapitalisten es mittels dieser Handelsoptionen zu immenssem Reichtum gebracht.

Vergessen Sie das Klischee „Wenn es nichts kostet, bist Du das Produkt“. Sie sind mitnichten das Produkt, sondern lediglich die kostenlose

01 Shoshana Zuboff, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, New York 2019 (deutsche Ausgabe: *Das Zeitalter des Überwachungskapitalismus*, Frankfurt/M.–New York 2018).

Quelle für den Rohstoff, der zu marktfähigen Produkten verarbeitet wird. Ich muss dabei an Elefanten denken, die majestätischsten aller Säugetiere: Überwachungskapitalisten sind Wilderer; sie schlagen Profit aus unserem Verhalten und lassen die Bedeutung, die unseren Körpern, unseren Gehirnen, unseren schlagenden Herzen innewohnt, achtlos liegen, was eine gewisse Ähnlichkeit mit dem monströsen Abschlachten von Elefanten um des Elfenbeins willen hat. Nein, Sie sind nicht das Produkt; Sie sind der zurückgelassene Kadaver. Das „Produkt“ zieht man aus dem Verhaltensüberschuss, den man Ihrem Leben entreißt.

URSPRÜNGE

Der Überwachungskapitalismus ist Menschenwerk; er lebt im historischen Kontext; er ist keine technologische Unvermeidbarkeit. Der Überwachungskapitalismus wurde im Trial-and-Error-Verfahren bei Google erprobt und entwickelt – so wie bei Ford seinerzeit die Massenproduktion oder der Management-Kapitalismus bei General Motors. Ersonnen hat man ihn als Lösung für Googles finanzielle Notlage nach dem Platzen der Dotcom-Blase 2000, als das Vertrauen der Investoren in das junge Unternehmen zu schwinden begann. Unter dem wachsendem Druck der Geldgeber entschloss sich die Google-Führung seinerzeit, zur Steigerung der Werbeeinnahmen den exklusiven Zugang zu den Datenlogs seiner Nutzerinnen und Nutzer in Kombination mit der damals schon erheblichen Rechenleistung und den analytischen Fähigkeiten zu nutzen, um daraus Vorhersagen über Klickraten zu erstellen, aus denen sich die Relevanz eingeblendeter Werbung erschließt. Operativ bedeutete dies, dass Google seinen wachsenden Bestand an Verhaltensdaten als *behavioral surplus* einer neuen Verwendung zuführte und gleichzeitig Methoden entwickelte, sich aggressiv nach neuen Quellen für Verhaltensüberschuss umzusehen.

Googles eigenen Wissenschaftlern zufolge entwickelte das Unternehmen neue Methoden der Überschussgewinnung, durch die sich Daten aufspüren lassen, die Nutzer eigentlich bewusst für sich behalten wollen und die darüber hinaus weitreichende Schlüsse auf persönliche Informationen ermöglichen, die Nutzer – bewusst oder unbewusst – nicht zur Verfügung stellen. Dieser zusätzliche Überschuss wird anschließend auf vorhersagekräftige Muster analysiert, wo-

durch sich bestimmte Werbung bestimmten Nutzern zuordnen lässt. Ersonnen und erstmals eingesetzt wurden diese neuen Methoden zwischen 2001 und 2004, und das unter strengster Geheimhaltung. Erst als Google 2004 an die Börse ging, erfuhr die Welt, dass die Einkünfte des Konzerns während dieses Zeitraums um 3590 Prozent gestiegen waren.

Heute ist klar, dass dieser neue Einsatz von Verhaltensdaten ein historischer Wendepunkt war. Das *behavioral surplus* hat sich in seiner Eigenschaft als kostenloser Aktivposten, der sich über die Verbesserung der Dienstleistung hinaus selbst zum Austausch auf dem Markt einsetzen lässt, als bahnbrechend erwiesen. Es geht dabei freilich nicht um einen Austausch mit dem Nutzer, sondern vielmehr mit anderen Unternehmen, die dahintergekommen sind, wie mit der nahezu risikolosen Wette auf das künftige Verhalten eines Nutzers Geld zu verdienen ist. Mit der Managerin Sheryl Sandberg migrierte der Überwachungskapitalismus von Google zu Facebook und entwickelte sich danach rasch zum Standardmodell des Informationskapitalismus für nahezu jedes Internetunternehmen, jedes Startup, ja jede App. Wie eine invasive Spezies ohne natürliche Feinde bemächtigte er sich kraft seiner finanziellen Tüchtigkeit der vernetzten Sphäre und entstellte damit den Traum von der digitalen Technologie als befähigende, emanzipatorische Kraft aufs Entsetzlichste.

Waren in der ersten Phase Online-Werber die dominanten Player der neuen Verhaltensterminkontraktmärkte, beschränkt sich der Überwachungskapitalismus inzwischen ebenso wenig auf die zielgerichtete Online-Werbung, wie die Massenproduktion auf Fords Model T beschränkt blieb. Heute kann jeder an der Monetarisierung wahrscheinlichkeitstheoretischer Informationen über unser Verhalten Interessierte mit dem nötigen Kleingeld auf einer ganzen Reihe von Verhaltensterminkontraktmärkten mit unserem künftigen Verhalten spekulieren.

ENTWICKLUNG

Während es unmöglich ist, sich den Überwachungskapitalismus ohne das Digitale vorzustellen, ist die Vorstellung des Digitalen ohne Überwachungskapitalismus überhaupt kein Problem. Man kann es gar nicht genug betonen: Überwachungskapitalismus ist nicht gleich Technologie.

Digitale Technologien können viele Formen annehmen und auf vielerlei Arten wirken, je nach der gesellschaftlichen und ökonomischen Logik, die sie zum Leben erweckt. Der Überwachungskapitalismus baut auf Algorithmen und Sensoren, Maschinenintelligenz und Plattformen, aber er ist nicht mit diesen gleichzusetzen. Ein Röntgenbild zeigt Knochen und Muskeln, nicht aber das weiche Gewebe, das sie miteinander verbindet. Technologie entspricht in unserem Fall den Knochen und Muskeln, der Überwachungskapitalismus jedoch ist das weiche Gewebe, das die Elemente miteinander verbindet und sie agieren lässt. Er ist der Schatten, der über das Digitale fällt, die verborgene Variable, die erklärt, wie diese einst emanzipatorische Plattform Menschen und Gesellschaft in den Rohstoff für anderer Leute wirtschaftlichen Profit verwandelt hat.

So wie der Überwachungskapitalismus nicht mit Technologie gleichzusetzen ist, hat man ihn sich auch nicht länger auf einzelne Unternehmen oder nur auf den Internetsektor beschränkt vorzustellen. Der Überwachungskapitalismus hat sich auf nahezu alle Bereiche wirtschaftlicher Aktivität ausgebreitet – Versicherungen, Gesundheitssektor, Einzelhandel, Unterhaltung, Transport, Bildung, um nur eine Handvoll zu nennen – und umfasst ein breites Spektrum von Produkten und Dienstleistungen. Was 2001 als Lösung für einen finanziellen Notstand begann, ist heute eine blühende, auf Überwachung gegründete Wirtschaftsordnung: eine Überwachungswirtschaft. So können wir zu unseren Lebzeiten beobachten, wie der Kapitalismus sich verändert: Zunächst ging es um Profite aus Produkten, dann aus Dienstleistungen, schließlich aus Spekulationen und jetzt um Profite aus der Überwachung.

Die Anhäufung von Verhaltensüberschuss ist der Hauptantrieb, um den herum sich die Wettbewerbsdynamik des Überwachungskapitalismus kristallisiert hat. Und hier fangen wir an, einige seiner bestürzenden Imperative zu verstehen. Alles beginnt mit Größenvorteilen (*economies of scale*); sie definieren, was ich den „Extraktionsimperativ“ (*extraction imperative*) nenne. Maschinelles Lernen erfordert Volumen, und die Qualität seiner Ergebnisse verbessert sich stetig mit der Bewegung in Richtung Totalität. Mit zunehmender Intensität des Wettbewerbs um Vorhersageprodukte wird jedoch klar, dass Volumen allein nicht genügt. So sehen sich Überwachungskapitalisten gezwungen, sich nach immer

vorhersagekräftigeren Quellen für Verhaltensüberschuss umzusehen. Ich nenne das den „Vorhersageimperativ“ (*prediction imperative*). Dieser verlangt sowohl Größenvorteile als auch Diversifikationsvorteile (*economies of scope*): Maschinelles Lernen bedarf über das Volumen hinaus auch der Datendiversität, was die notwendigen Nachschuboperationen zum einen in die Offline-Welt treibt – das, was wir als Realität bezeichnen –, zum anderen aber auch tiefer in unsere intime Erfahrungswelt: unsere Stimmen, Gesichter, Persönlichkeiten und Emotionen.

Mit zunehmender Wettbewerbsdynamik reichen schließlich auch Diversifikationsvorteile nicht mehr aus. Überwachungskapitalisten stellen fest, dass man den vorhersagekräftigsten Verhaltensüberschuss durch das zielgerichtete Eingreifen in den Stand der Dinge erhält, indem man Verhalten aktiv in Richtung profitabler Ergebnisse stupst, lockt, treibt. Der Gedanke dahinter ist längst nicht mehr, alles über unser Verhalten in Erfahrung zu bringen; vielmehr geht es darum, es in Richtung eines garantierten kommerziellen Erfolgs zu manipulieren. Dieser neue Grad an Wettbewerbsintensität führt zu etwas, was ich als „Handlungsvorteile“ (*economies of action*) bezeichne. Es genügt nicht länger, den Informationsfluss *über uns* zu automatisieren, das Ziel besteht nun darin, *uns* zu automatisieren.

In dieser Phase sind die Produktionsmittel zunehmend komplexen und umfassenden „Verhaltensmodifikationsmitteln“ (*means of behavioral modification*) untergeordnet. Und hier kommt Big Other ins Spiel, eine nahtlose Umgebung psychologischer Verstärkung, die das Verhalten von Einzelnen, Gruppen, ja ganzen Bevölkerungen ausformen soll. Das Design dieser Prozesse sorgt mit akribischer Sorgfalt für Unwissenheit beziehungsweise Ahnungslosigkeit, indem es das Bewusstsein des Einzelnen umgeht, um jede Möglichkeit zur Selbstbestimmung zu eliminieren. Ein Datenwissenschaftler erklärte mir das folgendermaßen: „Wir können den Kontext um ein bestimmtes Verhalten herum konstruieren und so eine Veränderung erzwingen ... Wir lernen, die Musik zu schreiben, und sorgen dann dafür, dass sie die Leute zum Tanzen bringt.“

Beispiele dafür finden sich überall. In meinem Buch beschreibe ich, wie arglose Pokémon-Go-Spieler zum Essen, Trinken und Einkaufen sanft zusammengetrieben werden in den Restaurants, Bars, Imbissstuben und Geschäften, die für

die Mitwirkung auf den Verhaltensterminkontraktmärkten bezahlen. Ich schildere die skrupellose Enteignung von Verhaltensüberschuss aus Facebook-Profilen zur Einflussnahme auf individuelles Verhalten – vom durch soziale Angst ausgelösten Kauf einer Antipickelsalbe am Freitag um 17.45 Uhr über den Klick auf ein „Ja“ zum Kauf neuer Sportschuhe im Endorphinrausch nach dem langen Sonntagmorgenlauf bis hin zur Stimmabgabe bei der nächsten Wahl als Resultat sozialer Vergleichsdynamiken, die das Unternehmen raffiniert ausgetüftelt hat. Dass Verhaltensmodifikation zum kommerziellen Imperativ geworden ist, räumt endgültig mit der Illusion auf, dass der vernetzten Form so etwas wie eine immanente Moral eigen sei – dass „verbunden“ zu sein doch vom Wesen her prosozial und integrativ sein müsse oder von Natur aus zur Demokratisierung von Wissen neige. Stattdessen nützt man digitales Verbundesein heute schamlos für anderer Leute Marktziele aus.

Diese Macht, Verhalten zum Profit Dritter zu manipulieren, ist ganz und gar selbstverliehen. Sie entbehrt jeglicher demokratischer oder moralischer Legitimation; insofern werden durch sie Entscheidungsrechte usurpiert und Prozesse individueller Autonomie untergraben, die für das Funktionieren einer demokratischen Gesellschaft unabdingbar sind. Die Message hier ist einfach: *Once I was mine. Now I am theirs.*

WIE KOMMEN „DIE“ DAMIT DURCH?

Folge dieser Entwicklung ist, dass der Überwachungskapitalismus für ganz neue Formen sozialer Ungleichheit sorgt. Er operiert mittels beispielloser Asymmetrien an Wissen und daraus erwachsender Macht. Überwachungskapitalisten wissen alles *über uns*; ihre Aktivitäten sind jedoch so angelegt, dass sie *für uns* nicht erkennbar sind. Sie häufen immense Domänen neuen Wissens *über uns* an, nur dass dieses Wissen nicht *für uns* ist; es dient zwar der Vorhersage unserer Zukunft, nur eben für anderer Leute Profit. Solange es den Überwachungskapitalisten und ihren Verhaltensterminkontraktmärkten gestattet ist, zu florieren, stellt der Besitz der neuen Verhaltensmodifikationsmittel den Besitz der Produktionsmittel als Quelle kapitalistischen Reichtums und kapitalistischer Macht im 21. Jahrhundert in den Schatten.

Trotz seiner Herrschaft über das digitale Milieu und seiner illegitimen Macht, sich priva-

te Erfahrung anzueignen und unser Verhalten zu manipulieren, tun die meisten Menschen sich schwer, sich dem Griff des Überwachungskapitalismus zu entziehen, und so mancher überlegt, ob es überhaupt möglich ist. In meinem Buch führe ich die Gründe dafür aus, warum dem so ist; ich beschränke mich hier auf das Folgende: In erster Linie hat der Überwachungskapitalismus Erfolg, weil er uns schlicht keine Wahl lässt; Abhängigkeit und „No Exit“ sind die Dreh- und Angelpunkte seines Erfolgs.

Wir sehen uns in der Falle einer ungewollten Fusion persönlicher Bedürfnisse und ökonomischer Enteignung. Die Kanäle, auf die wir uns hinsichtlich sozialer Interaktion, Arbeit, Bildung, Gesundheit, Zugang zu Produkten und Dienstleistungen und vielem anderem mehr angewiesen sehen, dienen gleichzeitig als Lieferketten für die Überschussströme des Überwachungskapitalismus. Das Resultat ist, dass eine effektive Teilnahme am Sozialleben über die Verhaltensmodifikationsmittel geschieht, was zwangsläufig die Entscheidungsmechanismen aushöhlt, die einst eins mit dem Privaten waren: Ausstieg, Widerspruch und Loyalität (*exit, voice, and loyalty*). Es gibt schlicht keine Möglichkeit, sich Prozessen zu entziehen, die bewusst so gehalten sind, dass sie das individuelle Bewusstsein umgehen und für Ahnungslosigkeit sorgen, zumal wenn es sich dabei um eben die Prozesse handelt, auf die wir zum Bestehen unseres Alltags angewiesen sind. Über die fehlende Möglichkeit des Ausstiegs hinaus fehlt es dem Widerspruch an signifikanten Kanälen, und Loyalität ist nur mehr ein leeres Wort. Teilnahme definiert sich damit eher durch Notwendigkeit, Abhängigkeit, Hilflosigkeit, Resignation, fehlende Alternativen und erzwungene Unwissenheit.

Die Abhängigkeit der Nutzerinnen und Nutzer entspricht somit dem klassischen faustischen Pakt, bei dem unser gefühltes Bedürfnis nach einem effektiven Leben mit der Neigung ringt, den kühnen Übergriffen des Überwachungskapitalismus zu widerstehen. Dieser Konflikt führt zu einer psychischen Abstumpfung, die uns dickfellig macht gegenüber der Realität, getrackt, analysiert, ausgewertet und modifiziert zu werden. Entsprechend neigen wir zu einer zynisch-resignierten Rationalisierung und flüchten uns in Verteidigungsmechanismen wie der berüchtigten Formulierung „Ich habe ja nichts zu verbergen“. Oder wir finden andere Wege, aus Frus-

tration und Hilflosigkeit den Kopf in den Sand zu stecken. So stellt der Überwachungskapitalismus das Individuum des 21. Jahrhunderts vor eine von Grund auf illegitime Entscheidung, mit der es sich erst gar nicht konfrontiert sehen sollte, und deren Normalisierung uns in unseren Ketten tanzen lässt – wobei allzu leicht vergessen wird, dass jemand, der nichts zu verstecken hat, auch nichts ist.

ÜBERWACHUNGSKAPITALISMUS IST MENSCHENWERK

Der Überwachungskapitalismus ist keineswegs unvermeidbar. Er ist ein Menschenwerk, das sich wie schon so viele andere von Menschenhand geschaffene Ungerechtigkeiten im Trojanischen Pferd eines technologischen Determinismus zu verstecken versucht. Es ist entsprechend wichtig, sich vor Augen zu halten, dass jede Unvermeidlichkeitsdoktrin einen waffenfähigen Virus birgt: einen moralischen Nihilismus, der darauf programmiert ist, menschliches Handeln vorherzubestimmen und jeglichen Widerstand ebenso wie jegliche Kreativität aus dem Text menschlicher Möglichkeiten zu löschen.

Die Rhetorik der Unvermeidlichkeit zielt darauf ab, uns zu Hilflosigkeit und Passivität zu verurteilen im Angesicht unerbittlicher Kräfte, die dem bloß Menschlichen gegenüber anscheinend indifferent sind, ja indifferent sein müssen. Hinter dem Gerede von der Unvermeidbarkeit verbirgt sich die Hoffnung, dass wir dem naturalistischen Fehlschluss zum Opfer fallen – dass die Regeln der Überwachungskapitalisten selbstredend richtig und gut sein müssen, weil sie erfolgreich sind. Aber lassen Sie sich nicht täuschen: Der Überwachungskapitalismus und seine Technologien digitaler Enteignung sind nicht „gut“, nur weil sie erfolgreich sind. Sie haben kein Recht auf ein unangefochtenes Eigenleben außerhalb unserer Gemeinschaft. Wir stehen erst am Anfang unseres Weges, nicht am Ende.

In der Ära der Massenproduktion ging es nicht nur um Maschinen, Fabriken, Produktionsverfahren und Management. Sie wurde auch geformt durch die allmähliche Entwicklung neuer Formen kollektiven Handelns im Verein mit politischen und gesellschaftlichen Institutio-

nen, so etwa neuen Gesetzen und Regulierungsregimen, die die prosoziale Dynamik des Kapitalismus verstärkten und seinen schlimmsten Auswüchsen die Zügel anlegten. Auch der Überwachungskapitalismus ist in einem bestimmten sozialen und historischen Kontext entstanden; in eben diesem Kontext wird man ihn anfechten und transformieren. Das Leben im Jahr 2040 wird von neuen Formen kollektiven Handelns und neuen institutionellen Antworten abhängen, die spezifisch sind für unsere Zeit, unsere Herausforderungen und unsere Existenzbedingungen. Diese Entwicklungen bleiben bislang aus; sie existieren noch nicht einmal im Entwurf. Wir werden auf diese – unsere – Zeit zurückblicken und darin den Anfang sehen.

Einer ihrer Kollegen hat Hannah Arendt einmal auf einem Symposium vorgeworfen, sich bei ihrer Analyse des Totalitarismus von persönlichen Werten leiten zu lassen. Ihre Antwort darauf spricht mir aus der Seele, und ich möchte sie deshalb hier abschließend zitieren: „Wenn ich nun diese Bedingungen beschreibe, ohne meiner Entrüstung zu erlauben, sich einzumischen, habe ich dieses besondere Phänomen aus seinem Zusammenhang in der menschlichen Gesellschaft herausgehoben und ihm dabei einen Teil seiner Natur gestohlen, es eines seiner wichtigsten inhärenten Eigenschaften beraubt.“⁰²

So gilt für mich wie vielleicht auch für Sie: Die bloßen Fakten des Überwachungskapitalismus müssen schon deshalb meine Entrüstung erregen, weil sie den Menschen herabwürdigen. Und so beginnt der Kampf um die Zukunft des Menschen mit *unserer* Entrüstung. Wenn die digitale Zukunft uns ein Zuhause sein soll, ist es an uns, sie dazu zu machen.

Dieser Text ist eine Übersetzung der Keynote, die Shoshana Zuboff am 11. Oktober 2018 auf der Konferenz „Zukunft der Datenökonomie“ des Forums Privatheit hielt (www.forum-privatheit.de). Übersetzung aus dem Amerikanischen: Bernhard Schmid, Nürnberg (www.bernhardschmid.de).

SHOSHANA ZUBOFF

ist Wirtschaftswissenschaftlerin und Sozialpsychologin sowie emeritierte Professorin an der Harvard Business School in Boston, USA.

www.shoshanazuboff.com

⁰² Hannah Arendt, Eine Antwort, in: dies./Eric Voegelin, Disput über den Totalitarismus, Göttingen 2015, S. 53–62, hier S. 55.

ESSAY

EINE BEUNRUHIGENDE FRAGE AN DEN DIGITALEN KAPITALISMUS

Michael Seemann

Ein Gespenst geht um (nicht nur) in Europa, es ist das Gespenst des digitalen Kapitalismus. Und wie es sich heutzutage ziemt, kommt er in vielen Formen und Farben: als Informationskapitalismus, Datenkapitalismus, Plattformkapitalismus, Überwachungskapitalismus oder kognitiver Kapitalismus. Der digitalen Kapitalismen gibt es mittlerweile viele, doch zeigen sie alle etwas Ähnliches an: Wir sind Zeuginnen und Zeugen grundlegender Veränderungen. Genau dies führt mich zu einer beunruhigenden Frage: Handelt es sich überhaupt noch um Kapitalismus?

Mit „beunruhigend“ meine ich nicht dieselbe Unruhe, in die sich die Autorinnen und Autoren der unterschiedlichen Digitalkapitalismusbeschreibungen hineinsteigern. Es geht mir nicht darum, zu zeigen, dass die neue, digitale Spielart des Kapitalismus schlimmer ist als alle vorhergehenden. Meine Beunruhigung gilt vielmehr dem Kapitalismus selbst. Ich lege ihm gewissermaßen meine Hand auf die Schulter und frage leise: „Alles in Ordnung mit Dir, Kapitalismus?“ Denn während viele Autorinnen und Autoren in der Digitalversion des Kapitalismus eine weitere Radikalisierung desselben ausmachen, habe ich eher das gegenteilige Gefühl. Ich glaube, dem Kapitalismus geht es nicht gut im Digitalen. Ich will deswegen grundsätzlicher fragen, ob der Kapitalismus in seiner digitalen Spielweise noch die Kriterien erfüllt, mit denen wir dieses System des Wirtschaftens und der Organisation der Gesellschaft beschreiben.

Es gibt verschiedene Kapitalismusdefinitionen, doch alle haben einen mehr oder weniger übereinstimmenden Kern. Demnach erfüllt Kapitalismus die folgenden fünf Kriterien: Er ist geprägt vom Antagonismus zwischen Kapital und Arbeit (zumindest bei Marx), von der Steuerung der Wirtschaft durch den Markt (neoklassische Definition), von Privateigentum an den Produktionsmitteln, dem Vorherrschen einer Eigentumsordnung sowie

dem Prinzip der Akkumulation (oder auch: von Wachstum). Im Folgenden werde ich prüfen, wie es sich im Digitalen mit diesen Kriterien verhält.

KAPITAL

Beginnen wir mit dem Offensichtlichen: dem Privateigentum an den Produktionsmitteln, dem „Kapital“. Gerade hier hat sich durch die Digitalisierung viel getan. Zu Marx' Zeiten waren die Produktionsmittel in erster Linie Land, Gebäude, Maschinen und vielleicht noch Fahrzeuge. Um zu veranschaulichen, wie stark sich die Essenz des Kapitals durch die Digitalisierung geändert hat, braucht man sich nur Folgendes vor Augen zu führen: Uber, das größte Taxiunternehmen der Welt, besitzt keine Fahrzeuge. Alibaba, der wertvollste Einzelhändler der Welt, hat kein eigenes Inventar. Airbnb, der weltweit größte Übernachtungsdienstleister, besitzt keine Immobilien.

Systematischer haben diesen Zusammenhang die Ökonomen Jonathan Haskel und Stian Westlake in ihrem Buch „Capitalism Without Capital“ untersucht. Der Untertitel – „The Rise of the Intangible Economy“ – zeigt auch schon an, dass das Kapital nicht wirklich verschwunden ist.⁰¹ Es hat sich nur dematerialisiert. Zu den materiellen Investitionsgütern, die bereits Marx kannte, traten irgendwann Software, Datenbanken, Design, Marken, Fortbildungen und sonstige nicht anfassbare, immaterielle Werte hinzu. Und sie kamen nicht nur hinzu. In den USA, Großbritannien und Schweden hat der Anteil der Investitionen in immaterielle Werte die Investitionen in materielle Werte längst überflügelt. Die Werte der 500 größten börsennotierten US-amerikanischen Unternehmen sind bereits zu 84 Prozent immateriell.⁰² Die Digitalbranche ist hier Vorreiter und Treiber der Entwicklung.

„Materiell, immateriell, was macht das für einen Unterschied?“, kann man jetzt fragen. Es

sind vier systemische Unterschiede, die Haskel und Westlake herausarbeiten: Immaterielle Güter sind erstens „versunkene Kosten“ (*sunk cost*), das heißt, in immaterielle Werte investiertes Kapital lässt sich schlecht weiterveräußern. Zweitens gibt es häufig Übertragungseffekte, immaterielle Werte „schwappen über“ (*spill-over*). Das heißt, man kann Informationen – und das sind immaterielle Güter immer – nur schwer für sich allein behalten. Drittens lassen sich immaterielle Güter skalieren (*scalable*): Einmal hergestellt, kann ein immaterielles Gut unbegrenzt und ohne Zusatzkosten überall eingesetzt werden. Viertens sind immaterielle Güter synergetisch (*synergy*): Sie ergeben oft erst in der Kombination mit anderen immateriellen Gütern neue Produkte beziehungsweise führen immer wieder zu neuen Anwendungsfällen.

Am spannendsten ist der Spill-over-Effekt. Wir kennen ihn überall dort, wo urheberrechtlich geschützte Werke in Internet getauscht werden. Für industrielle Produzenten kann es aber auch einfach heißen, dass sich die Konkurrenz die Herstellung von einem Produkt anschaut oder eine Software nachbaut. Einige – aber lange nicht alle – immaterielle Investitionen kann man rechtlich schützen lassen. Und hier kommen wir überhaupt erst wieder ins Fahrwasser unseres Kapitalismuskriteriums. Nur immaterielle Investitionen, die man über Urheberrechte, Patente oder Markeneintragung schützen kann, können überhaupt als Privateigentum gelten und tauchen als *assets* in den Bilanzen auf. Aber selbst diese Formen von Privateigentum, also geistigem Eigentum, sind in ihrer Eigentumsstruktur höchst fragwürdig, die Bemessung ihres Wertes ist an der Grenze zur Beliebigkeit. Im Grunde handelt es sich um reine Monopolverwertungsrechte,⁰³ oder, überspitzt ausgedrückt, um Eigentumsbehauptungen.

ARBEIT

Ein wesentlicher Bestandteil jeglicher Kapitalismusdefinition ist die Funktion von Arbeit beziehungsweise die Gegenüberstellung von Arbeit und Kapital als Teile des Produktionsvorgangs.

Der marxischen These nach ist menschliche Arbeit, genauer: gesellschaftlich notwendige Arbeit, dasjenige, was überhaupt den Wert einer Ware innerhalb der Ökonomie erschafft. Da der Arbeiter aber nicht in der vollen Höhe seiner Wertschöpfung entlohnt wird, sondern nur in etwa in der Höhe, die notwendig ist, um seine Arbeitskraft wiederherzustellen (Reproduktion), streicht der Kapitalist diese Differenz (Mehrwert) als Profit ein.

Schauen wir auf den Einsatz von Arbeit und erzieltm Wert in der Digitalwirtschaft, und hier auf das besonders eindruckliche Beispiel der amerikanischen Videothekskette Blockbuster im Vergleich zum Videostreamingdienst Netflix: Netflix machte 2018 mit 5400 Mitarbeiterinnen und Mitarbeitern 15,7 Milliarden US-Dollar Umsatz, während der mittlerweile pleite gegangene Videoverleih in seinem letzten Jahr (2010) mit 25000 Mitarbeiterinnen und Mitarbeitern nur 3,24 Milliarden US-Dollar umsetzte. Das bedeutet, dass Blockbuster mit fünfmal so viel Personal gerade mal ein Fünftel des Umsatzes von Netflix erwirtschaftete, obwohl beide in einem ähnlichen Business sind.⁰⁴ Die Digitalwirtschaft scheint pro Mitarbeiter viel mehr Wertschöpfung zu produzieren als die alte, analoge Wirtschaft.

Gemessen wird dieser Zusammenhang in der Wirtschaftswissenschaft als Arbeitsproduktivität, und wenn wir uns die Zahlen für die Gesamtwirtschaft (zum Beispiel für die G20-Staaten) anschauen, sehen wir in der Tat ein enormes Wachstum der Arbeitsproduktivität, aber nur ein geringes Wachstum der Löhne. Dass diese Differenz bei den Kapitalisten landet, ist also folgerichtig und bereits von dem Wirtschaftswissenschaftler Thomas Piketty beschrieben, der zeigte, wie sich das Wachstum der Anlagevermögen entsprechend von dem Wachstum der Löhne entkoppelt hat.⁰⁵ Unter den arbeitsproduktivsten Firmen der Welt finden wir viele IT-Konzerne. Apple erwirtschaftet fast zwei Millionen US-Dollar Umsatz pro Mitarbeiter. Auch Facebook und Google verdienen auf Platz zwei und drei weit mehr als eine Millionen Dollar pro Mitarbeiter.⁰⁶ Aber alle diese Firmen sind nicht dafür bekannt, dass sie ihre Mit-

⁰¹ Vgl. Jonathan Haskel/Stian Westlake, *Capitalism Without Capital. The Rise of the Intangible Economy*, Oxfordshire 2017.

⁰² Vgl. *The Value of Intangible Assets*, 10. 4. 2019, www.saltare-solutions.com/2018/10/17/the-value-of-intangible-assets.

⁰³ Vgl. Marcel Weiß, Kann es ein Eigentum an Geistigem geben? Nein., 23. 2. 2012, <https://neunetz.com/2012/02/23/kann-es-ein-eigentum-an-geistigem-geben-nein>.

⁰⁴ Vgl. die Wikipedia-Einträge zu Netflix und Blockbuster LLC (abgerufen am 23. 4. 2019).

⁰⁵ Vgl. Thomas Piketty, *Das Kapital im 21. Jahrhundert*, München 2014.

⁰⁶ Vgl. Anaele Pelisson/Dave Smith, *These Tech Companies Make the Most Revenue per Employee*, 6. 9. 2017, www.businessinsider.de/tech-companies-revenue-employee-2017-8.

arbeiterinnen und Mitarbeiter schlecht bezahlen – im Gegenteil. In Bezug auf Marktpreise verdienen vor allem die Entwicklerinnen und IT-Spezialisten Löhne weit über dem Durchschnitt. Aber gemessen am erzielten Umsatz verdienen sie nur „Peanuts“, und aus einer marxischen Ausbeutungslogik heraus betrachtet, zählen sie zu den vielleicht am stärksten ausgebeuteten Menschen der Welt, da der extrahierte Mehrwert so enorm ist.

Wie der gefühlte gesellschaftliche Mehrwert mit dem ökonomischen Mehrwert zusammenhängt, ist allerdings nur schwierig bis unmöglich zu messen. Vor allem, da die Art der Wertschöpfung heute ganz und gar anders vonstattengeht, als Marx es damals beobachtete. In dem Buch „Das Kapital sind wir“ hat der Publizist Timo Daum nicht nur eine interessante Beschreibung der digitalen Ökonomie abgeliefert, sondern eine eigene These zur Wertschöpfung im Digitalen aufgestellt.⁰⁷ Diese geschehe nicht bei der Produktion von Waren, sondern in Form von Innovation. Und wir alle arbeiteten daran mit: Denn wir werden jederzeit vermessen, während wir die digitalen Tools verwenden. Die gesammelten Daten werden dann für die Entwicklung neuer Innovation und Verbesserung der Produkte genutzt. Die Harvard-Ökonomin Shoshana Zuboff schlägt in eine ähnliche Kerbe, allerdings klingt bei ihr die Wertschöpfung wesentlich perfider. Auch bei ihr steht die Überwachung der Nutzerinnen und Nutzer im Mittelpunkt, doch statt um Innovation geht es bei ihr um Manipulation, durch die die großen Internetunternehmen Wert schöpfen (*behavioral surplus*).⁰⁸ Der Digital-Economy-Lecturer Nick Srnicek hingegen beschreibt Daten als eine Art Rohstoff, der erst durch die Verarbeitung wirklich an Wert gewinne. Hier seien es die Programmierer der Auswertungsalgorithmen und vor allem Data Scientists, deren Arbeit den Wert schöpfe.⁰⁹ Der Journalist Paul Mason kam in seinem Buch „Post-Capitalism“ sogar zu dem Schluss, dass sich die kapitalistischen Ökonomien nicht werden halten können, wenn Information statt Arbeit zum zentralen Bestandteil der Wertschöpfung werde.¹⁰

⁰⁷ Vgl. Timo Daum, *Das Kapital sind wir: Zur Kritik der digitalen Ökonomie*, Hamburg 2017.

⁰⁸ Vgl. Shoshana Zuboff, *The Age of Surveillance Capitalism. The Fight for the Future at the New Frontier of Power*, New York 2019. Siehe auch den Beitrag von Zuboff in dieser Ausgabe (Anm. d. Red.).

⁰⁹ Vgl. Nick Srnicek, *Platform Capitalism*, London 2016.

¹⁰ Vgl. Paul Mason, *PostCapitalism. A Guide to Our Future*, London 2015.

Auf die Frage nach der Rolle der Arbeit im Digitalen bleiben wir also mit vielen unterschiedlichen, einander widersprechenden Theorien und Beobachtungen zurück. Einigkeit scheint allein darüber zu bestehen, dass Arbeit im klassischen Sinn zumindest nicht mehr der wesentliche Ort der Wertschöpfung ist.

MARKT

Seit Marx „Das Kapital“ schrieb, ist auch in den Wirtschaftswissenschaften viel passiert. Für viele Ökonominnen und Ökonomen steht heute nicht mehr der Produktionsprozess im Mittelpunkt des Geschehens, sondern der Markt. Und so findet sich kaum eine zeitgenössische Kapitalismusdefinition, die nicht auch auf den Markt rekurrieren würde. Der Markt sei das wesentliche Steuerungsinstrument des Kapitalismus. Indem der Markt Angebot (Produktion) und Nachfrage (Konsumtion) über das Instrument des Preises im Gleichgewicht halte, Sorge er dafür, dass zu jeder Zeit immer ungefähr genauso viel von einer Ware produziert werde, wie gebraucht werde und sich dieses Angebot auch im bezahlbaren Rahmen bewege. So lautet jedenfalls die Theorie, die oft und gerne kritisiert wird, da sie eine ganze Reihe von Annahmen voraussetzt, die in der Realität kaum zu erfüllen sind: völlige Markttransparenz, Menschen als rationale Wirtschaftssubjekte, die Nichtexistenz von Transaktionskosten, die Ausblendung von nicht im Markt abgebildeten Einflüssen und Kosten (Externalitäten) und anderes mehr.

Blendet man diese Ungenauigkeiten gutwillig aus, kann man den Markt auch als „Informationssystem“ verstehen,¹¹ der als Input die Signale von Anbietern und Nachfragern koordiniert. So gesehen, sollte man annehmen, dass der Markt anschlussfähig an die Digitalisphäre sein sollte. Und tatsächlich: Es stellt sich heraus, dass Marktmechanismen sich leicht in Algorithmen nachbauen lassen. Genau das hat zum Beispiel Uber mit seinem „Surge Pricing“ gemacht. Je nach Tages- und Nachtzeit sind unterschiedlich viele Uber-Fahrerinnen und -Fahrer unterwegs, und es gibt unterschiedlich hohe Nachfrage nach Fahrten. Entsprechend wird den Kundinnen und Kunden neben dem Standardpreis auch der Surge-Preis angezeigt. Dieser ist im Zweifels-

¹¹ So zum Beispiel Friedrich August von Hayek, *Der Wettbewerb als Entdeckungsverfahren*, in: ders., *Freiburger Studien*, Tübingen 1969, S. 249–265, hier S. 249.

fall höher als der Standardpreis, aber dafür kommt das Auto sofort. Es handelt sich also um eine Art Marktpreis – mit der Besonderheit, dass er von einem Algorithmus berechnet wurde.

Aus den vielen Millionen Kundenentscheidungen für und gegen den Surge-Preis lassen sich auch eine Menge weiterer Erkenntnisse ziehen. Beispielsweise sind Leute mit niedrigem Smartphone-Akkustand in der Regel bereit, einen höheren Preis für eine sofortige Uber-Fahrt zu bezahlen. Auf dieser Grundlage lässt sich dann auch die „Konsumentenrente“ berechnen, wie ein Team um den Ökonomen Steven Levitt am Beispiel Uber gezeigt hat.¹² Die Konsumentenrente ist, kurz gesagt, die Preisdifferenz zwischen dem Preis, den ich für ein Produkt tatsächlich zahle, und dem, den ich zu bezahlen bereit wäre, wenn der Preis höher wäre. Diese nichtgezahlte Differenz nehme ich als Konsument sozusagen als Bonus mit. Da jeder Konsument eine unterschiedliche Bereitschaft hat, einen höheren Preis zu zahlen, „erhält“ jeder Konsument somit auch eine individuelle Konsumentenrente. Die allgemeine Konsumentenrente errechnet sich somit, wenn man all diese individuellen Differenzen zusammenrechnet. Die Untersuchung von Levitt et al. ergab, dass Uber 2015 eine allgemeine Konsumentenrente in Höhe von 2,9 Milliarden US-Dollar erwirtschaftete. Das ist kein Geld, das in irgendeiner Statistik auftaucht. Es ist Geld, das *nicht* ausgegeben wurde, aber möglicherweise ausgegeben worden wäre, wenn jede Kundin und jeder Kunde einen personalisierten Preis angezeigt bekommen hätte. Und wenn man weiß, dass eine Person mehr Geld zu bezahlen bereit wäre, warum ihr dann nicht diesen Preis anzeigen?

Vergegenwärtigen wir uns, was hier passiert: Wenn der Marktpreis ein Informationssystem ist, und Computer, Internet und Shopsysteme ebenfalls Informationssysteme sind, dann wurde das Erstere durch die Letzteren quasi gehackt. Die IT-Systeme der Anbieter sind einfach intelligenter als der Markt.

EIGENTUM

Eine ebenso schlichte wie elegante Kapitalismusdefinition, die sich sowohl von der marxistischen als auch von der neoklassischen Definition ab-

setzt, ohne mit ihnen inkompatibel zu werden, stammt von den Wirtschaftswissenschaftlern Gunnar Heinsohn und Otto Steiger.¹³ Sie definieren den Kapitalismus als Eigentumsordnung, also eine Gesellschaft, die durch das Konzept Eigentum strukturiert ist. Das hört sich zunächst banal, offensichtlich und wenig ertragreich an, wird aber spannend, wenn man sich die Implikationen des Begriffes „Eigentum“ genauer anschaut.

Während Marx die Ursituation des Kapitalismus in der Produktion verortet und die Neoklassiker dafür den Markttausch heranziehen, sehen Heinsohn und Steiger sie in der Unterscheidung von „Besitz“ und „Eigentum“. Diese Unterscheidung ist selbst keine ökonomische, sondern vor allem eine rechtliche. „Besitz“ ist dabei alles, worüber ich direkte Verfügungsgewalt ausübe. Darin unterscheidet es sich vom Eigentum: Eigentum ist ein Rechtstitel, es ist abstrakte Behauptung. Das heißt, ich kann Gegenstände, die mein Eigentum sind, in den Besitz anderer Menschen geben, ohne dass es aufhört, mein Eigentum zu sein. Allerdings funktioniert das nur dann, wenn eine externe Macht dafür sorgt, dass der Rechtstitel auch durchgesetzt, mir der Gegenstand im Zweifelsfall wieder ausgehändigt wird. Für Eigentum braucht es also einen Staat mit Gewaltmonopol.

Wenn wir uns mit dieser Definition wieder dem Digitalen zuwenden, kommt einem rasch die Online-Musiktauschbörse Napster in den Sinn. 1999 gestartet, machte der Dienst alle Musikdateien auf dem eigenen Computer für alle anderen Napster-User zugänglich. Das Programm hatte eine Suchmaske, mit der man nach jedem beliebigen Song suchen konnte und die daraufhin eine Liste mit Usern anzeigte, die ihn besaßen und teilten. Ein Klick, und der Download startete. Für Musiksammler war es das reinste Eldorado. Für die Musikindustrie war dieses Eldorado jedoch ein *major spill-over*, der totale Kontrollverlust, und das plötzliche Ende ihres Geschäftsmodells. Mit der Kapitalismusdefinition von Heinsohn/Steiger könnte man sagen, dass die Musikindustrie aus der Eigentumsordnung in eine Download-Besitzordnung zurückfiel. Zwar hat die Musikindustrie (und andere Rechteinhaber) viel für Urheberrechtsverschärfungen lobbyiert, aber trotz allem konnte sie die *Peer-to-peer*-Tauschbörsen nicht loswerden.

¹² Vgl. Peter Cohen et al., Using Big Data to Estimate Consumer Surplus: The Case of Uber, National Bureau of Economic Research, NBER Working Paper 22627/2016, www.nber.org/papers/w22627.

¹³ Vgl. Gunnar Heinsohn/Otto Steiger, Eigentum, Zins und Geld. Ungelöste Rätsel der Wirtschaftswissenschaft, Marburg 2002.

Hier nun das Spannende: Dass die Musikindustrie heute wieder ein Geschäftsmodell hat, liegt nicht an einer staatlich garantierten Eigentumsordnung, sondern weil eine ganz eigene, neue Ordnung im Internet entstand: die Ordnung der Plattformen. Als Apple 2002 auf die Musikverlage zukam und ihnen iTunes, die unternehmenseigene digitale Verkaufsplattform für Musik zeigte, stand die Musikindustrie gerade mit dem Rücken zur Wand. Auch die großen Labels hatten es nicht geschafft, den Tauschbörsen ein populäres legales Online-Angebot entgegenzustellen. Apple-Chef Steve Jobs konnte den Verlagen die Bedingungen letztlich jedoch diktieren,¹⁴ weil sein Unternehmen etwas hatte, was sie nicht hatten: Ich nenne es „marktfähige Verfügungsgewalt“. Das heißt, Apple war nicht nur in der Lage, Musik kommerziell und legal anzubieten, sondern auch, sie durch die technische Infrastruktur von iTunes vorzuhalten, ohne dass es einer weiteren Durchsetzungsgewalt (den Staat) bedurfte. Dem Beispiel Apples folgten bald viele weitere Unternehmen, die heute die „Plattform-Ökonomie“ ausmachen. Ihre Plattformen sind in erster Linie Kontroll-Infrastrukturen zur künstlichen Verknappung potenziell unbegrenzter Güter.

Doch die marktfähige Verfügungsgewalt der Plattformen ist schon lange nicht mehr auf tatsächliche Rechtstitel beschränkt. Facebook hat keinerlei Eigentumsrechte an unseren persönlichen Daten, und dennoch basiert sein Geschäftsmodell auf der Ausübung einer marktfähigen Verfügungsgewalt über sie. Die Plattformen setzen bereits eine Form der Kontrolle durch, die die Eigentumsordnung gar nicht braucht, sondern diese lediglich stellenweise abbildet. Das aber bedeutet nichts Geringeres, als dass im Digitalen das Rechtskonzept des Eigentums zumindest infrage steht.

WACHSTUM

Ein Kriterium kommt bei Kapitalismusdefinitionen sowohl aus der marxistischen als auch aus der neoklassischen Schule immer wieder auf, und das ist das Wachstum. Welche Rolle spielt dieses Kriterium in der digitalen Ökonomie?

Der Ökonom Robert J. Gordon argumentiert in seinem Werk „The Rise and Fall of American Growth“,¹⁵ dass heutiges Wirtschaftswachstum trotz aller Zukunftsversprechungen durch die Digitalisierung nicht mehr von tatsächlicher Innovation getrieben sei. Er untermauert diesen Befund anhand der sogenannten Totalen Faktorproduktivität (TFP) – einer volkswirtschaftlichen Kennzahl, die die Faktoren Kapital und Arbeit aus dem Wirtschaftswachstum herausrechnet und somit den Anteil der Wertschöpfung angibt, der nicht durch diese Faktoren erklärbar ist. Gordon sieht in der TFP einen messbaren Effekt von Innovation im Wachstum. Da die TFP in den USA zwischen 1930 und 1970 stetig weit über einem Prozent war, davor und danach aber wesentlich darunter, schließt Gordon daraus, dass die Digitalisierung kaum zu Innovation geführt habe. Er greift damit eine Beobachtung auf, die der Ökonom Robert Solow bereits 1987 formulierte: „You can see the computer age everywhere but in the productivity statistics.“¹⁶

Ich möchte dieser These widersprechen: Meiner Ansicht nach sind die digitalen Innovationen genauso real wie frühere technische Innovationen, sie sind jedoch mit herkömmlichen Maßstäben kaum zu messen. Sowohl das Bruttoinlandsprodukt als auch alle davon abgeleiteten Werte wie Wachstum, Produktivität oder eben die TFP basieren auf der Erhebung davon, wie viel Geld in unterschiedlichen Branchen umgesetzt wird, was heißt: alles, was keine Transaktion verursacht, fließt nicht in die Rechnung ein. Nun gibt es aber viele Gründe, warum sich gerade digitale Innovation oft transaktionsneutral oder gar transaktionsmindernd in den Zahlen niederschlägt:

Erstens wird durch das Internet die Markttransparenz erhöht. Unsere Konsumententscheidungen sind heute viel fundierter als vor dem Internet, was aber auch bedeutet, dass wir weniger Fehlinvestitionen tätigen (und somit weniger Transaktionen). Zweitens hat der erwähnte Spill-over-Effekt dazu geführt, dass wir heute ein weitaus größeres kulturelles Angebot zur Verfügung haben, ohne wesentlich mehr Geld dafür ausgeben zu müssen. Dafür müssen wir Filme nicht illegal streamen, aber allein, dass wir es könnten, zwingt die Anbieter dazu, at-

¹⁴ Vgl. Steve Knopper, iTunes' 10th Anniversary. How Steve Jobs Turned the Industry Upside Down, 26. 4. 2013, www.rollingstone.com/culture/culture-news/itunes-10th-anniversary-how-steve-jobs-turned-the-industry-upside-down-68985.

¹⁵ Vgl. Robert J. Gordon, The Rise and Fall of American Growth. The U.S. Standard of Living Since the Civil War, Princeton 2016.

¹⁶ Vgl. Simon Dudley, The Internet Just Isn't That Big a Deal Yet: A Hard Look at Solow's Paradox, 12. 11. 2014, www.wired.com/insights/2014/11/solows-paradox.

traktive legale Bezahlangebote zu schaffen. Auch dies verursacht ein Minus in der Wachstumsbilanz. Drittens darf man nicht vergessen, auf wie viel kostenloses Wissen wir heute Zugriff haben. Die Wikipedia ist – bis auf ein paar wenige Spendenzahlungen – komplett kostenlos. Netto geht sie allerdings mit einem satten Minus in die volkswirtschaftliche Gesamtrechnung ein, wenn man die vielen Verluste der Lexikonverlage gegenrechnet. Obwohl es vielfach versucht wurde, gibt keine sinnvolle Art, den Wert der Wikipedia zu messen.¹⁷ Einen ähnlichen Effekt haben wir durch die Verwendung von Open Source Software in der Wirtschaft.

Insgesamt werden alle möglichen Prozesse innerhalb der Wirtschaft durch Technologie immer effizienter. Der Einzug von künstlicher Intelligenz und Big Data wird immer wieder mit erheblichen Einsparungen beworben. Einsparungen sind aber nicht getätigte Transaktionen. Es sind Verschlankungen der Bilanz, denen zumindest nicht zwingend eine zusätzliche Investition gegenübersteht. Digitale Innovation spart also mehr Transaktionen ein, als sie zusätzlich schafft. Doch warum gibt es dann überhaupt noch wirtschaftliches Wachstum? Meine These dazu: Ähnlich wie 2007 befinden wir uns in einer Blase, dieses Mal aber mit immateriellen Werten. Ich glaube, Immaterialgüter sind massiv überbewertet – und zwar allein deshalb, weil sie künstlich am *spill-over* gehindert werden, der im Digitalen eigentlich der „Naturzustand“ jeder Information ist. Plattformkontrolle, drakonische Urheberrechtsgesetzgebung und -durchsetzung haben zu einer künstlichen Verknappung von Ideen, Gedanken und kreativen Leistungen geführt, die auf der einen Seite unser aller Leben verarmt, um es uns auf der anderen wieder teuer verkaufen zu können.

Wachstum bedeutete einst, dass mehr Menschen mehr Dinge tun können, dass Produkte billiger wurden, mehr Menschen Zugang zu fließend Was-

ser, Strom, Konsumartikeln bekamen. In der digitalen Ökonomie bedeutet Wachstum lediglich, dass die Konsumentenrente erfolgreicher abgeschöpft wird, dass also mehr Menschen unnötigerweise mehr bezahlen, als sie unter normalen Marktbedingungen müssten. Wachstum bedeutet, dass immaterielle Güter erfolgreicher verknappt wurden.

FAZIT

Alle fünf Kriterien, die ich eingangs identifiziert habe, werden durch die digitale Wirtschaft ad absurdum geführt. Ausführlich lautet die beunruhigende Frage also: Ist ein digitaler Kapitalismus mit nur noch behaupteten Kapital und überflüssiger Arbeit, der nicht mehr durch den Markt gesteuert wird, die Eigentumsordnung hinter sich gelassen hat und dessen kaum noch vorhandenes Wachstum aus der künstlichen Verknappung von Immaterialgütern resultiert, noch Kapitalismus?

Vermutlich nein. Aber was ist er dann? Zunächst stehen wir mit mindestens einem Bein ja noch voll und ganz im guten, alten analogen Kapitalismus. Und was das digitale Bein betrifft: Wir haben Kapitalismus immer nur in Abgrenzung zu Kommunismus oder Sozialismus – bestenfalls noch Anarchismus oder Feudalismus – zu verstehen gelernt. Das, was die Digitalwirtschaft dort tut, ist keines von dem. Wir müssen uns an dieser Stelle der Neuheit der Situation gewahr werden. Dies ist unser aller erste Digitalisierung und somit sollten wir der Möglichkeit Rechnung tragen, dass es sich hier auch um eine komplett neue Form der Ökonomie handelt. Eine, für die wir noch keinen Namen haben und noch gar nicht wissen, wie sie funktioniert. Etwas, das noch im Werden ist. Dieses Etwas ist nicht automatisch besser oder schlechter als der Kapitalismus, nur eben hinreichend anders. „Die alte Welt liegt im Sterben, die neue ist noch nicht geboren: Es ist die Zeit der Monster“, soll der marxistische Philosoph Antonio Gramsci sinngemäß geschrieben haben.¹⁸ Wir haben es hier mit einem Monster zu tun, einem (noch) namenlosen Wesen. Monster sind nicht automatisch böse, aber sie machen uns Angst, weil wir sie nicht verstehen.

MICHAEL SEEMANN

ist Kulturwissenschaftler, Sachbuchautor und Journalist.

www.michaelseemann.de

¹⁷ Siehe zum Beispiel Leonhard Dobusch, Wert der Wikipedia. Zwischen 3,6 und 80 Milliarden Dollar?, 5. 10. 2013, <https://netzpolitik.org/2013/wert-der-wikipedia-zwischen-36-und-80-milliarden-dollar>.

¹⁸ Zit. nach Slavoj Žižek, A Permanent Economic Emergency, in: New Left Review 64/2010, <https://newleftreview.org/issues/ll64/articles/slavoj-zizek-a-permanent-economic-emergency>. Das Zitat ist allerdings umstritten, vermutlich hat Žižek folgende Zeilen frei paraphrasiert: „The crisis consists precisely in the fact that the old is dying and the new cannot be born, in this interregnum a great variety of morbid symptoms appear.“ Antonio Gramsci, „Wave of Materialism“ and „Crisis of Authority“, The Prison Notebooks, New York 1971 (1949/51), S. 275f.

CHANCEN UND HERAUSFORDERUNGEN IN DER DATENÖKONOMIE

Markus Spiekermann

Die rapide Entwicklung neuartiger Informations- und Kommunikationstechnologien – vom Internet der Dinge über Cloud-Computing bis zu künstlicher Intelligenz – zwingt Unternehmen dazu, traditionelle Geschäftsmodelle zu überdenken und zu erneuern. Die Menge an verfügbaren Daten und Informationen durch intelligente Maschinen, Sensoren, Finanztransaktionen, Social Media und viele andere Quellen nimmt exponentiell zu.

Der Begriff „Datenökonomie“ steht dabei für den Grundgedanken, Daten als Wirtschaftsgut zu verstehen und in eigenständigen Geschäftsmodellen zu monetarisieren. Der Bedeutungsanstieg von Daten als Wirtschaftsgut und Treiber für Innovationen und Wachstum zeigt sich im Transformationsprozess unterschiedlichster Domänen sowohl im Bereich der Geschäftsbeziehungen zwischen Unternehmen (B2B) als auch im Bereich der Geschäftsbeziehungen zwischen Unternehmen und Endkunden (B2C). Durch geeignete Analysen können Daten zur Entdeckung neuartiger Zusammenhänge genutzt werden und somit geschäftlich wie auch sozialen Mehrwert liefern.

Im Folgenden werde ich zunächst näher darlegen, was unter Datenökonomie zu verstehen ist. Anschließend werde ich auf die sich verändernde Rolle von Daten als wirtschaftliche Ressource eingehen, um dann die Potenziale und Herausforderungen für Unternehmen in der Datenökonomie zu skizzieren.

WAS IST DATENÖKONOMIE?

Unter *data economy* sind alle Aspekte rund um die Auswertung und wirtschaftliche Nutzung von Daten zu verstehen. Konkret ist dabei der Einfluss der Daten auf die Wirtschaft als Ganzes zu betrachten, was personenbezogene und nicht personenbezogene Daten einschließt. Was die Möglichkeiten der wirtschaftlichen Nutzung angeht, gibt es entscheidende Unterschiede zwischen diesen beiden Daten-

formen, da gerade personenbezogene Daten verschiedenen rechtlichen Regelungen, beispielsweise der Datenschutzgrundverordnung (DSGVO), unterliegen und ein verantwortungsvoller Umgang mit diesem sensiblen Datentyp unabdingbar ist. Wertschöpfungsketten im Bereich der Datenökonomie umfassen die Generierung, die Sammlung, die Speicherung, die Verarbeitung und Analyse bis hin zur abschließenden Verwertung oder Löschung der Daten. Entlang der Wertschöpfungsketten kommen digitale Technologien, Methoden und Algorithmen zum Einsatz, die einen Mehrwert aus den Daten realisieren und neue Geschäftsmodelle, Produktionsmöglichkeiten, Prozessoptimierungen und Verbesserungen in der Kundenbindung ermöglichen.

Die Kommerzialisierung und Monetarisierung von Daten ist bereits voll im Gange. Der Begriff der Datenmonetarisierung ist dabei auf den klassischen Handel mit Daten zurückzuführen. Mit dem Wachstum des Internets und insbesondere Social Media und E-Commerce werden immer mehr Adressdaten von Personen und Unternehmen gehandelt. Heute „zahlen“ die Konsumentinnen und Konsumenten (bewusst oder unbewusst) häufig mit ihren Daten im Tausch gegen zusätzliche Dienstleistungen wie individuelle Produktvorschläge, Navigation oder Kommunikationsfunktionen.

Doch mit Datenökonomie sind nicht nur die wirtschaftliche Verwertung und Vergütungsmodelle von personenbezogenen Daten gemeint. Durch die digitale Transformation und die steigenden Datenmengen – bedingt durch Konzepte der Industrie 4.0 und sich bildenden digitalen Ökosystemen in verschiedenen Industriesektoren wie dem produzierenden Gewerbe, der Agrarwirtschaft und vor allem dem Informations- und Telekommunikationssektor – steigt auch die Verfügbarkeit nicht personenbezogener Daten an. Auftrags-, Maschinen-, Prozess- und Transaktionsdaten werden gesammelt, verarbeitet, verwertet und in den digitalen Wertschöpfungsketten monetarisiert.

Die Charakterisierung von Daten als Schlüsselressource lässt sich dabei als Zeichen einer fundamental neuen Wirtschaftsepoche deuten. So wie das Kapital unsere Gesellschaft von der Agrar- hin zur Industriegesellschaft verändert hat, so werden auch Daten unser aller Leben gewissermaßen auf den Kopf stellen – nur dass diese Veränderungen sowohl wirtschaftlich als auch gesellschaftlich noch tief greifender sein werden. Das autonome Fahrzeug, das selbstständig fährt, oder aber der intelligente Kühlschrank, der eigenständig Milch und andere Produkte bestellt, sind nur zwei lebensnahe Beispiele für viele Veränderungen, die uns bevorstehen.

DATEN ALS WIRTSCHAFTLICHE RESSOURCE

Seit der Einführung der elektronischen Datenverarbeitung und der Automatisierung von Produktionsprozessen in Unternehmen steigt die Bedeutung von Daten für unternehmerischen Erfolg kontinuierlich an. Bereits in den 1960er und 1970er Jahren wurden Informationssysteme zur Unterstützung einzelner Unternehmensfunktionen eingesetzt. Warenwirtschaftssysteme dienten beispielsweise der Unterstützung von Lagerprozessen und den Mitarbeiterinnen und Mitarbeitern bei der Suche nach Artikeln im Lagerbestand. Da der eigentliche Wertbeitrag jedoch ausschließlich durch physische Produkte erzielt wurde, nahmen die Daten eine rein unterstützende Rolle ein.

Mit der Verbreitung datengestützter Planungssysteme in den 1980er und 1990er Jahren, die eine bedarfsgerechte und unternehmensweite Planung von Ressourcen ermöglichten, entwickelten sich Daten zum Befähiger des unternehmerischen Geschäftsprozessmanagements. Daten wurden immer mehr zur strategischen Ressource für die Leistungserbringung von Unternehmen, vor allem in den Bereichen Produktion, Service und Logistik. So stellt beispielsweise das sogenannte *process mining* eine Methodik bereit, um interne Prozesse zu optimieren. Hier ergeben sich insbesondere Potenziale im Bereich der Durchlaufzeiten, der Prozesskosten, der Prozessstabilität, aber auch die Sicherstellung von Compliance-Anforderungen, zum Beispiel was die Einhaltung gesetzlicher Regularien betrifft. Ein anderes Beispiel ist das sogenannte *predictive maintenance*, also die vorausschauende Wartung von Maschinen und Geräten, die auf der Auswertung von Maschinendaten ba-

siert. Umweltdaten können helfen, Ausfälle vorherzusagen, Stillstände zu vermeiden und damit letztendlich Kosten zu sparen.

Ungefähr seit dem Jahrtausendwechsel bieten Unternehmen zunehmend Produkte an, deren Existenz überhaupt nur durch die Verwendung großer und qualitativ hochwertiger Datenmengen möglich ist. Beispiele sind Google Maps, das Transportangebot von Uber, die Leasing- und Fleet-Management-Modelle von Hilti sowie viele weitere Smart Services für unsere persönlichen Lebenslagen. In den vergangenen Jahren ist eine Produktisierung der Daten selbst zu erkennen. Der Kauf und Verkauf von Daten auf sich bildenden Datenmarktplätzen oder Plattformen mit entsprechenden Angeboten werden wie bei klassischen Produkten nach standardisierten Volumen- oder Zeiteinheiten angeboten und abgerechnet. Daten sind nicht länger nur Befähiger und Unterstützer anderer Produkte, sondern mittlerweile das Produkt selbst.

Auf dem Weg in die heutige Datenökonomie lassen sich drei unternehmerische Entwicklungsetappen ausmachen. In einem ersten Schritt wurden klassische Geschäftsmodelle um digitale Prozesse erweitert: Unternehmen digitalisierten ihre Vertriebs- und Kommunikationswege durch die Einführung von E-Commerce-Shops und ermöglichten so einen zusätzlichen digitalen Absatz ihres Wertangebots. In einem zweiten Schritt erstreckte sich die Digitalisierung auf die Produkte selbst: Klassische Produkte wie beispielsweise Bohrmaschinen, Bücher, Zahnbürsten oder Fußbälle wurden um digitale Komponenten erweitert, indem Sensorik zur Generierung von Daten und Funktechnologien zur Datenübertragung verbaut wurden. Hierdurch wurde es Unternehmen auch möglich, einen direkten Kundenkontakt nach dem eigentlichen Verkaufszeitpunkt aufrechtzuerhalten und somit individuell zugeschnittene Zusatzdienstleistungen zu verkaufen. In einem dritten Schritt wurden schließlich rein digitale Geschäftsmodelle entwickelt, die sich durch eine rein digitale Wertschöpfung sowie ein rein digitales Wertangebot und Ertragsmodell auszeichnen: Unternehmen in dieser Ebene konzentrieren ihr Kerngeschäft auf den Umgang mit Daten und Informationen. Dies bezieht sich auf die Generierung, Aggregation und Analyse von Daten. Der Besitz und das Eigentum von physischen Vermögensgegenständen, deren Anschaffung und Wartung im Vergleich zu Daten sehr kostenintensiv

ist, ist hierfür nicht notwendig, was den entsprechenden Unternehmen ein sehr rasches Wachstum und hohe Skalierbarkeit ermöglicht.

Ein Blick auf die Unternehmensgründungen in Deutschland verdeutlicht dies: Die heutige Start-up-Szene wird klar von digitalen Geschäftsmodellen dominiert. 37,8 Prozent der deutschen Unternehmensgründungen basieren auf Softwareentwicklung und anderen Softwareangeboten, weitere 12,9 Prozent auf anderen digitalen Dienstleistungen. Insgesamt setzen 68,4 Prozent der Start-ups auf digitale Geschäftsmodelle. Wenig überraschend sind die meisten jungen Unternehmen in der Informations- und Kommunikationstechnologiebranche angesiedelt. Doch auch in den Branchen Ernährung und Nahrungsmittel, Medizin und Gesundheit, Automobile, Logistik und Verkehr sowie Freizeit und Sport zeigen die digitalen Geschäftsmodelle das unternehmerische Potenzial der Datenökonomie.⁰¹

POTENZIALE

Laut dem Bundesverband der Deutschen Industrie (BDI) beträgt das Wertschöpfungspotenzial der Datenökonomie bis 2025 alleine für Deutschland bis zu 425 Milliarden Euro. Betrachtet man ganz Europa, wird dieses Wertschöpfungspotenzial für die nächsten zehn Jahre auf bis zu 1,25 Billionen Euro geschätzt.⁰² Hierbei zeigen sich unterschiedliche Potenziale in den verschiedenen Branchen, jeweils bedingt durch Datenverfügbarkeit und unterschiedliche Reifegrade der digitalen Transformation. So wird beispielsweise im deutschen Groß- und Außenhandel bis 2025 ein Wertschöpfungspotenzial von 14,4 Milliarden Euro erwartet, in der Metall- und Elektroindustrie 15,1 Milliarden Euro und in der Branche der Informations- und Kommunikationstechnologie sogar 17,2 Milliarden Euro.⁰³

Der Anteil von Digitalinvestitionen an der Gesamtwirtschaftsleistung liegt in Deutschland bei 25 Prozent, hinter den USA (33 Prozent), dem Ver-

einigten Königreich (31 Prozent) und Frankreich (26 Prozent). Ein ähnliches Bild ergibt sich bei der Ausschöpfung von Digitalisierungspotenzialen. Gemessen an 21 Indikatoren – etwa Unternehmensinvestitionen im Hard- und Softwarebereich, E-Commerce oder Social-Media-Nutzung – liegt der Wert des ausgeschöpften Potenzials in Deutschland bei gerade einmal zehn Prozent. Hierbei ist allerdings anzumerken, dass auch andere Länder das in der Digitalisierung liegende Potenzial bisher bei Weitem nicht ausnutzen (USA: 18 Prozent, Vereinigtes Königreich: 17 Prozent, Niederlande: 15 Prozent, Frankreich: 12 Prozent).⁰⁴

Auch auf politischer Ebene wird der Datenökonomie in der Europäischen Union großes Wachstumspotenzial zugesprochen: Die EU-Kommission gibt an, dass das Volumen des EU-Datenmarktes 2015 über 54 Milliarden Euro betrug, zugleich geht sie von einem jährlichen Zuwachs um sieben Prozent aus, sodass es bis 2020 schon 84 Milliarden betragen dürfte. Den Wert der EU-Datenwirtschaft insgesamt beziffert die Kommission für 2015 sogar auf 272 Milliarden Euro, bis 2020 erwartet sie ein Wachstum um etwa 133 Prozent auf 634 Milliarden Euro, was im selben Zeitraum mit der Entstehung von 1,4 Millionen neuen Arbeitsplätzen einhergehen könnte.⁰⁵

Entscheidend dafür, ob der potenzielle Mehrwert aus den Daten tatsächlich realisiert werden kann, wird ein intelligenter Umgang mit den Daten sein. Ein wichtiger Faktor zur Ausschöpfung der vorhandenen Potenziale ist der unternehmensübergreifende Austausch von Daten zur Bildung von sogenannten Datenökosystemen. Datenökosysteme zeichnen sich dadurch aus, dass mehrere Unternehmen an der digitalen Wertschöpfung beteiligt sind und sich neue Verwertungsmöglichkeiten in Form datengetriebener und kundenzentrierter Geschäftsmodelle ergeben, die ein Unternehmen alleine nicht erbringen könnte. Hierbei ist es wichtig, dass alle beteiligten Unternehmen ihre Daten am Markt verfügbar machen, damit am Ende auch alle profitieren können. Dies wird jedoch nur mit geeigneten kontextbezogenen und regulierenden Einschränk-

⁰¹ Vgl. Tobias Kollmann et al., Deutscher Startup Monitor 2018. Neue Signale, klare Ziele, Berlin 2018.

⁰² Vgl. Roland Berger Strategy Consultants/Bundesverband der Deutschen Industrie, Die Digitale Transformation der Industrie. Eine europäische Studie von Roland Berger Strategy Consultants im Auftrag des BDI, München–Berlin 2015.

⁰³ Vgl. Kai Lange, Was McKinsey am deutschen Mittelstand vermisst, 17.8.2017, www.manager-magazin.de/unternehmen/artikel/a-1163125.html.

⁰⁴ Vgl. Bundesministerium für Wirtschaft und Energie (BMWi) (Hrsg.), Weißbuch Digitale Plattformen. Digitale Ordnungspolitik für Wachstum, Innovation, Wettbewerb und Teilhabe, Berlin 2017.

⁰⁵ Vgl. Europäische Kommission, Europäische Datenwirtschaft: EU-Kommission stellt Konzept für Daten-Binnenmarkt vor, Pressemitteilung, 10.1.2017.

kungen, speziell für personenbezogene Daten, sowie geeigneten Ertragsmodellen möglich sein, damit ausreichende Sicherheiten und Anreize für die Unternehmen und Personen bestehen, ihren „Datenschatz“ verfügbar zu machen.

DIGITALE REIFE DER DEUTSCHEN WIRTSCHAFT

Das Fraunhofer-Institut für Software- und Systemtechnik ISST Dortmund hat jüngst mit dem Institut der deutschen Wirtschaft Köln (IW) auf Basis des IW-Zukunftspanels 2018 eine empirische Studie erstellt, um den aktuellen Status der deutschen Industrie und industrienahen Unternehmen hinsichtlich ihrer Fähigkeiten zur Teilhabe an der Datenökonomie zu analysieren. Insgesamt wurden 1235 Unternehmen befragt, um ihren digitalen Reifegrad zu ermitteln.⁰⁶

Die Feststellung des Reifegrades basiert dabei auf den drei aufeinander aufbauenden Dimensionen „Data Resource Management“, „Data Valuation“ und „Data Business“. Die erste Dimension beschreibt die Grundvoraussetzung zur Teilhabe an der Datenökonomie und wird erhoben, indem die unternehmensinternen Strukturen und Prozesse zur Ermöglichung von datenbasierter Wertschöpfung und digitaler Transformation betrachtet werden. Die zweite Dimension beschreibt den wirtschaftlichen und effektiven Umgang mit den Unternehmensdaten. Die dritte Dimension beschreibt die aktive Nutzung und den Austausch von Daten und datenbasierten Produkten über die eigenen Unternehmensgrenzen hinweg.

Die Auswertung der Befragungsdaten mündete in die Einteilung der Unternehmen in sechs Reifestufen. Hierbei wurde festgestellt, dass 84 Prozent der deutschen Unternehmen im Hinblick auf ihre Eignung zur Teilhabe an der Datenökonomie noch einen geringen Reifegrad aufweisen, also allenfalls als „digitale Einsteiger“ gelten können (Stufen 0 und 1). 13,8 Prozent der Unternehmen (Stufe 2) sind „digital fortgeschritten“, das heißt, sie haben die internen Prozesse bereits stärker digitalisiert und die digitale Transformation damit eingeleitet. Nur 2,2 Prozent der Unternehmen sind als „digitale Pioniere“ den zwei oberen Reifestufen zuzuordnen (Stufen 3 bis 5). Sie sehen in Da-

ten die Kernressource ihres Geschäftsmodells und lassen deutliche Fortschritte in den Dimensionen Data Resource Management und Data Valuation erkennen, das heißt, es gibt bereits eine gesteigerte Wahrnehmung von Daten als Vermögenswert und ein Bewusstsein für die Notwendigkeit ihrer monetären und nicht monetären Bewertung.⁰⁷

Weiterhin ergab die Studie, dass fast alle deutschen Unternehmen prognostizieren, dass sich ihre Prozesse innerhalb der nächsten fünf Jahre stärker digitalisieren werden. Etwa zwei von drei befragten Unternehmen erwarten, dass dies eine stärkere Integration externer Daten – etwa von Kunden, Lieferanten oder externen Anbietern – mit sich bringen wird. Der dafür notwendige Handel mit Rohdaten spielt dabei in der Erwartungshaltung der meisten Unternehmen noch eine untergeordnete Rolle. Immerhin 12,9 Prozent erwarten einen stärkeren Zukauf von externen Rohdaten, während nur 6,8 Prozent der Unternehmen den Verkauf von Rohdaten als wahrscheinliche Option sehen. Vor allem kleine und mittlere Unternehmen sind hier noch zurückhaltend. Bei großen Unternehmen kann sich immerhin fast jedes vierte Unternehmen einen verstärkten Verkauf von Rohdaten vorstellen.⁰⁸

WIRTSCHAFTLICHE HERAUSFORDERUNGEN

Um die gewaltigen unternehmerischen und wirtschaftlichen Potenziale der Datenökonomie zu realisieren, gilt es, verschiedene Herausforderungen im Zusammenhang mit der Ressource Daten zu meistern. Aus ökonomischer Sicht stellt sich die zentrale Frage, wie Unternehmen Daten intelligent bewirtschaften sollten, um den potenziellen Mehrwert aus ihrer Nutzung tatsächlich abzuschöpfen. In diesem Zusammenhang sind neben einem Bewusstsein über den Bestand an Daten innerhalb eines Unternehmens und den technischen Implikationen für ihre Erstellung, Speicherung, Verarbeitung und Pflege auch organisatorische und betriebswirtschaftliche Herausforderungen zu beachten. Hier geht es um Fragestellungen wie beispielsweise die Zuordnung von notwendigen Rollen und Verantwortlichkeiten für das Management der Daten innerhalb eines Unternehmens, aber auch um die grundsätzliche Fragestellung, wie man Daten eigentlich ökonomisch bewerten kann.

06 Vgl. Boris Otto et al., *Data Economy. Status Quo der deutschen Wirtschaft & Handlungsfelder in der Data Economy*, Dortmund 2019.

07 Vgl. ebd., S. 12–17.

08 Vgl. ebd., S. 19.

Dass eindeutige Bewertungsverfahren bislang fehlen, liegt vor allem daran, dass Daten sich in ihren Eigenschaften grundsätzlich von materiellen Gütern unterscheiden. Ein wichtiges Charakteristikum materieller Güter ist etwa deren Verschleiß bei der Nutzung. Solche Abnutzungseffekte durch Verwendung in verschiedenen Prozessen und Analysen gibt es bei Daten und Informationen nicht. Zudem werden Güter üblicherweise verbraucht – ein Faktor, der zentral für das Funktionieren unserer Volkswirtschaften ist. Doch auch diese Eigenschaft ist Daten und Informationen nicht zu eigen. Selbst durch Vervielfältigung verlieren Daten nicht an Wert. In diesem Sinne unterscheidet sich auch der Umgang mit diesen digitalen Wirtschaftsgütern von dem mit Gütern, die man anfassen kann.

Es gibt durchaus Versuche, Berechnungsverfahren für die Bewertung von Daten zu entwickeln. Bei Online-Plattformen, deren Hauptressource die Daten der Nutzerinnen und Nutzer sind, liegt es nahe, einfach den Unternehmenswert durch die Nutzerzahl zu teilen: Dividiert man zum Beispiel die 26,2 Milliarden US-Dollar, die Microsoft 2016 bereit war, für die Übernahme der Social-Media-Plattform LinkedIn zu zahlen, durch die damalige Nutzerzahl von 433 Millionen, ergibt das einen Wert von 60,50 US-Dollar pro Datensatz.⁹⁹ Dieser Ansatz hilft jedoch nicht weiter, da er, wenn überhaupt, nur auf Unternehmen anwendbar ist, die ein ähnliches Geschäftsmodell wie LinkedIn verfolgen.

Die Bewertung von Daten ist jedoch eine wichtige Voraussetzung für ihre Monetarisierung und damit für Unternehmen in der Datenökonomie nahezu unerlässlich. Zwar gibt es (noch) keine allgemeingültige Formel, aber die folgenden drei Ansatzpunkte könnten als grundlegende Orientierung weiterhelfen:

Wer als Unternehmerin oder Unternehmer gar keine Idee hat, wie viel die eigenen Daten wert sind, kann sich einem initialen Wert nähern, indem sämtliche Kosten betrachtet werden, die für die Beschaffung beziehungsweise eigene Erstellung, Speicherung, Pflege, Aufbereitung, Verfügbarmachung und Löschung oder Archivierung der Daten angefallen sind. Hieraus lässt sich dann ein Wert für die sogenannten Wiederbeschaffungskosten ermitteln.

Ein weiterer Ansatzpunkt ist der sogenannte Nutzwert. Hierbei werden nicht die Kosten für

die Daten selbst betrachtet, sondern es wird das Potenzial ermittelt, das sich aus der Nutzung der Daten ergibt. So können Faktoren wie Prozessoptimierung und Kosteneinsparungen als Kennwerte herangezogen werden. Dieses Verfahren wird bereits zur Ermittlung anderer immaterieller Vermögenswerte angewendet, beispielsweise bei Lizenzen, Rechten und Patenten.

Gerade in der wachsenden Datenökonomie ergibt sich noch ein dritter Ansatz, den wir sehr gut von anderen Produkten und Dienstleistungen kennen: der Marktansatz. Hierbei müssen sich die Unternehmen die Frage stellen, ob für die von ihnen angebotenen Daten ein Markt existiert und was potenzielle Kundinnen und Kunden bereit sind, für sie zu zahlen. Durch die steigende Verfügbarkeit von Daten auf allen möglichen Plattformen und Marktplätzen gibt es auch immer mehr Vergleichsangebote, die zur Ermittlung eines Marktwertes beziehungsweise eines Referenzwertes genutzt werden können.

RECHTLICHE HERAUSFORDERUNGEN

Was die rechtliche Seite angeht, bewegt sich die Datenökonomie mit all ihren datengetriebenen Geschäftsmodellen noch in einem Ordnungsrahmen aus dem analogen Zeitalter. Eine zentrale rechtliche Frage im digitalen Umfeld ist die nach dem Eigentum und Besitz der Daten. Sie ist aktuell nicht abschließend geklärt und beschäftigt Wissenschaftlerinnen genauso wie Rechtsanwälte in Unternehmen. Je nach Kontext und Branche gelten für verschiedene Datenarten unterschiedliche Verfügungsrechte.¹⁰ Die Frage nach dem Eigentum beziehungsweise den Verfügungsrechten ist für die Unternehmen in der Datenökonomie nicht nur wichtig, um die rechtlich einwandfreie Verwendung interner und externer Daten für neue Geschäftsmodelle sicherzustellen. Sie ist auch entscheidend für die Aufnahme der Datenressourcen in die Bilanz der Unternehmen und der damit verbundenen „Materialisierung“ des Vermögensgegenstandes.

¹⁰ Vgl. Nicola Jentzsch, Dateneigentum – Eine gute Idee für die Datenökonomie?, 30. 1. 2018, www.stiftung-nv.de/de/publikation/dateneigentum-eine-gute-idee-fuer-die-datenoekonomie; Christian Rusche/Marc Scheufen, On (Intellectual) Property and Other Legal Frameworks in the Digital Economy, Institut der deutschen Wirtschaft Köln, IW-Report 48/2018.

⁹⁹ Vgl. James E. Short/Steve Todd, What's Your Data Worth?, in: MIT Sloan Management Review 3/2017, S. 17 ff.

Dies gilt sowohl für personenbezogene Daten als auch für nicht personenbezogene Daten. Während die DSGVO weitgehend regelt, was und vor allem was nicht mit personenbezogenen Daten geschehen darf, ist dies für nicht personenbezogene Daten aktuell unklar. Im Falle der personenbezogenen Daten drohen Unternehmen bei Nichtbeachtung der Regelungen erhebliche Strafzahlungen. Im Falle der nicht personenbezogenen Daten wird derzeit in mehreren Initiativen unter Beteiligung von Ministerien, Unternehmen und Forschungseinrichtungen an Lösungen geforscht, die einen unternehmensübergreifenden Datenaustausch unter Wahrung der sogenannten Datensouveränität ermöglichen.¹¹ Datensouveränität ist dabei als die Fähigkeit einer natürlichen oder juristischen Person zur ausschließlichen Selbstbestimmung hinsichtlich des Wirtschaftsguts Daten zu verstehen. Dies bedeutet, dass ein Unternehmen oder eine Person selbst bestimmen kann, wer, wann und wofür die zur Verfügung gestellten Daten nutzen darf.

Im Kontext der voranschreitenden Entwicklung und vermehrten Nutzung von künstlicher Intelligenz ergeben sich darüber hinaus auch Haftungsfragen: Wer trägt die Verantwortung beziehungsweise wer sollte haften, wenn ein autonomes System Schäden verursacht? Gerade bei dem oft zitierten Anwendungsfall des autonomen Fahrens spielen maschinelle Entscheidungen und die Haftung dafür eine entscheidende Rolle, was als rechtliche Herausforderung der nächsten Zeit anzusehen ist.

TECHNISCHE HERAUSFORDERUNGEN

Die Datenerfassung erfolgt durch immer mehr technische Systeme und Endgeräte. Neben entsprechenden Geräten bei den Verbraucherinnen und Verbrauchern – Smartphones, Smart Watches oder auch Heimassistenzsysteme wie Amazon Alexa oder Google Home – sind dies vor allem Sensoren an den unterschiedlichsten Maschinen und Systemen des Internets der Dinge. Die daraus resultierende Fülle an Daten, oft unter dem Begriff „Big Data“ zusammengefasst, verlangt letztendlich ständig neue Speicherlösungen.

Daneben müssen die großen Datenmengen verwaltet und gesichert werden, was leistungsstarke Architekturen erforderlich macht, um einen schnellen, agilen und anwendungsorientierten Zugriff zu ermöglichen. Mit den neuen Zugriffsmöglichkeiten und der Bereitstellung der Daten für immer mehr interne und externe Nutzerinnen und Nutzer und Systeme steigt auch die Notwendigkeit, sich vor Cyberangriffen, Datenverlust und Systemausfällen zu schützen.

Eine weitere zentrale Herausforderung ist die Standardisierung, sowohl in Bezug auf Datenmodelle als auch auf Datenaustauschformate. Ohne diese Standards kann das Potenzial der verfügbaren Daten für die neu aufkommenden datengetriebenen Geschäftsmodelle nicht abgerufen werden. Und letztendlich gehört auch das Thema der Datenqualität zu den technischen Herausforderungen. Denn eine hohe Qualität der Daten ist die Voraussetzung dafür, dass sie überhaupt sinnvoll analysiert werden können.

FAZIT

Die Datenrevolution ist in vollem Gange und verändert unser aller Leben. Neben den gewaltigen Potenzialen für die wirtschaftliche Nutzung von Daten für neue Geschäftsmodelle, effizientere Prozesse und neue Kundenservices gibt es gleichermaßen Herausforderungen in wirtschaftlicher, technischer und rechtlicher Hinsicht.

Wie meine Ausführungen gezeigt haben, wird das Potenzial bislang jedoch bei Weitem nicht ausgeschöpft, und auch mit Blick auf die verschiedenen Herausforderungen gibt es noch viel zu tun, möchte man mit der internationalen Entwicklung Schritt halten. Der Vergleich mit anderen Ländern verdeutlicht zudem, dass die deutsche Wirtschaft hier zu Lösungen kommen und Themen wie Datensicherheit und Datenschutz, Datensouveränität, Bewertung von Daten und Bildung von Ökosystemen aktiv vorantreiben sollte, um in der Datenökonomie eine gewichtige Rolle spielen und sich gegen die internationale Konkurrenz behaupten zu können.

MARKUS SPIEKERMANN

ist Wirtschaftsinformatiker und leitet die Abteilung „Datenwirtschaft“ am Fraunhofer-Institut für Software- und Systemtechnik ISST in Dortmund.
markus.spiekermann@isst.fraunhofer.de

¹¹ Vgl. etwa Boris Otto et al., *Industrial Data Space: Digitale Souveränität über Daten*, Whitepaper, München 2016.

DATENVERWERTUNG UND DATENETHIK

Dirk Heckmann

Spätestens seit die Europäische Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018 Geltung erlangte, wächst ein neues Bewusstsein für den Umgang mit Daten heran: Wieviel Schutz brauchen (personenbezogene) Daten in der Datenökonomie, wie sehr „schadet“ der Datenschutz den (redlichen) Geschäftsmodellen in der Digitalwirtschaft, die auf die Verwertung von Daten angewiesen sind? Ist unter den Bedingungen der digitalen Transformation sämtlicher Lebensbereiche Datenschutz alleine eine Frage des Rechtsgüterschutzes, den es politisch auszuhandeln gilt, oder hat der Umgang mit persönlichen Daten auch eine ethische Dimension?

DATEN ALS WIRTSCHAFTSGUT

Wenn man unter Wirtschaftsgütern sämtliche Güter versteht, die in einem Arbeitsprozess für die Leistungserstellung notwendig sind (Sachgüter, Dienstleistungen, Rechte), dann gehören hierzu in einer zunehmend digitalisierten Wirtschaft auch Daten. Wie bedeutsam Daten als Wirtschaftsgut sind, zeigt nicht zuletzt die Diskussion um das automatisierte und vernetzte Fahren und die mit diesem einhergehenden Fahrzeug-, Fahrer- und Fahrverhaltensdaten. Dies wirft nicht nur Fragen des Datenschutzes und der Rechte zum Zugriff auf diese Daten, sondern auch ethische Fragen auf. So befasste sich schon die Ethikkommission für automatisiertes und vernetztes Fahren mit diesem Komplex. Sie wurde im September 2016 vom Bundesminister für Verkehr und digitale Infrastruktur eingesetzt und legte im Juni 2017 ihren Abschlussbericht vor.⁰¹ Die im September 2018 eingesetzte Datenethikkommission der Bundesregierung greift diese Überlegungen auf und erweitert das Spektrum auf grundlegende Fragen zu Datenrecht, Datenpolitik und Datenethik.

Selbst die Rechtsprechung bezeichnet inzwischen (etwa im insolvenzrechtlichen Kontext) explizit Daten als Wirtschaftsgut und geht überdies davon aus, dass die zunehmende wirtschaftliche Bedeutung von Datenerhebungen auch auf die Entwicklung des Verständnisses des Daten-

schutzrechts Einfluss nimmt.⁰² Schon das bis 2018 geltende Bundesdatenschutzgesetz (BDSG) ging davon aus, dass es einen Markt für personenbezogene Daten geben soll. Paragraph 29 BDSG gestattete nämlich unter bestimmten Voraussetzungen das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen von Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunftsteilen oder dem Adresshandel diene. Bei alledem stellt sich die Ausgangsfrage: Was sind eigentlich „Daten“?

DATEN ALS RECHTSBEGRIFF

Der Begriff „Daten“ ist in verschiedenen Rechtsgebieten von Relevanz – zu nennen ist natürlich das Datenschutzrecht, aber auch beispielsweise das Strafrecht. Auch deshalb hat sich noch kein einheitlicher Rechtsbegriff des Datums beziehungsweise von Daten herausgebildet. Aufgrund des Vorschlags für eine europäische Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte⁰³ könnte der Begriff der Daten auch im Zivilrecht noch größere Bedeutung erlangen.

Unter Daten im kommunikationswissenschaftlichen und auch im technischen Sinne sind die auf einem Datenträger festgehaltenen Zeichen oder Zeichenfolgen zu verstehen. Zeichen sind dabei zunächst interpretationsfreie Elemente der Sprache oder der Schrift, also etwa ein Symbol, eine Zahl oder ein Buchstabe, die sich mit ihrer Fixierung auf einem materiellen Datenträger von gesprochener Sprache und visueller Beobachtung unterscheiden. Dies umfasst die syntaktische, vom Inhalt der Daten losgelöste Ebene.

Begibt man sich hingegen auf die semantische Ebene, misst man den Daten also eine Bedeutung bei, so handelt es sich streng genommen nicht mehr um Daten, sondern um Informationen. Auf dieser Ebene differenziert beispielsweise das Datenschutzrecht etwa über den Begriff der „personenbezogenen Daten“. Nur wenn personenbezogene Daten vorliegen, ist das Datenschutzrecht anwendbar und entfaltet seine Schutzwirkung für

den Persönlichkeitsschutz. Nach der DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden: „betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen oder zu einer Kennnummer oder ähnlichem identifiziert werden kann (Art. 4 Nr. 1 DSGVO). Dabei ist es nicht zwingend notwendig, dass die Informationen, die zur Identifizierung einer Person erforderlich sind, nur einer einzigen Person zur Verfügung stehen müssen.⁰⁴ Ein Personenbezug ist daher bereits dann herstellbar, wenn die datenverarbeitende Stelle über rechtliche Mittel verfügt, die es ihr erlauben, den Betroffenen anhand der dadurch erhaltenen Informationen zu identifizieren (etwa über gesetzlich geregelte Auskunftsansprüche gegen Dritte).

Demgegenüber hat der Daten-Begriff bislang noch keinen Eingang ins Bürgerliche Gesetzbuch gefunden. Das ist insofern bemerkenswert, als die unstreitige Bedeutung als Wirtschaftsgut eine Einordnung in das Zivilrecht nahelegt. In diese Richtung geht auch die derzeit heftig geführte Diskussion um ein „Dateneigentum“ – also etwa die Fragen, wem die Daten gehören beziehungsweise wem sie zuzuordnen sind.

DATEN ALS GEGENLEISTUNG

Der Einsatz von Daten als Wirtschaftsgut birgt für Unternehmen ein enormes Potenzial. Neben der Produktentwicklung und der Produktverbesserung können sie auch der gezielteren Vermarktung von Produkten dienen, wobei hierdurch noch lange nicht sämtliche Einsatzfelder aufgezählt sind. Dabei muss es nicht immer um Profildaten gehen, wie sie bei Suchmaschinen oder in sozialen Netzwerken generiert werden. Auch für

kleine mittelständische Unternehmen können Daten als Gegenleistung und damit als Wirtschaftsgut interessant sein. Dabei ist zu differenzieren, wie an zwei Anwendungsfällen gezeigt werden kann.

Anwendungsfall 1: Das Unternehmen S vertreibt Gartenteiche. Über dessen Website ist es möglich, die Gartenteiche auch online zu bestellen. Hierbei muss der Kunde seine persönlichen Daten, beispielsweise Name und Adresse, in eine Maske eintragen und den entsprechenden Teich auswählen, damit der Vertrag erfolgreich abgewickelt werden kann. Die Konfiguration der Gartenteiche erfolgt mittels direkter Kommunikation zwischen Unternehmen und Kunde.

Anwendungsfall 2: Das Unternehmen S möchte nun ein Kundenportal mit einem sogenannten Gartenteichkonfigurator einsetzen. Mithilfe des Konfigurators kann der Kunde bestimmte Daten seines Grundstücks, beispielsweise Angaben über Größe, Form und Hangneigung, eingeben. Außerdem soll der Kunde persönliche Angaben machen, beispielsweise über sein Alter und die Anzahl der im Haushalt lebenden Personen. Hier ist insbesondere anzugeben, ob sich darunter Kinder befinden und wie alt diese sind. Auch Angaben zu einer etwaigen Bepflanzung oder Tierhaltung werden gefordert. Aufgrund dieser Daten wird dem Kunden daraufhin der Gartenteich (einschließlich Zubehör und weiterer Services, beispielsweise Sicherungen zum Schutz kleiner Kinder) angeboten, der am besten zu ihm und seinem Grundstück passt. Anhand der Bepflanzung und Tierhaltung sollen die Intervalle für die Reinigung und Wartung des Gartenteichs bestimmt werden. Neben der Erfüllung auf diese Weise avisierter und assoziierter Kundenwünsche möchte S die eingegebenen Daten seiner Kunden auch für andere Zwecke nutzen, beispielsweise, um seine Produkte zu verbessern oder die Produktpalette an die von den Kunden am meisten nachgefragten Gartenteiche auszurichten. Das Unternehmen ist bereit, dem Kunden für die Preisgabe seiner Daten einen Preisnachlass zu gewähren.

Im Anwendungsfall 1 werden die Daten lediglich zur Vertragserfüllung benötigt, sie bilden dagegen nicht selbst den Gegenstand des Vertrags. Die Erhebung der persönlichen Daten des Kunden und die anschließende Nutzung für eigene Geschäftszwecke ist hierbei ohne Weiteres zulässig, da diese für die Begründung und Abwicklung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich sind (Art. 6 Abs. 1 Satz 1 lit. b DSGVO). Würde der Unternehmer S nicht

⁰¹ Vgl. Bericht der Ethikkommission automatisiertes und vernetztes Fahren, Juni 2017, www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.html. Der Verfasser dieses Beitrags war Mitglied dieser Ethikkommission. Er wurde zudem 2018 in die Datenethikkommission der Bundesregierung berufen.

⁰² Vgl. Landgericht Düsseldorf, Urteil vom 9.3.2016 – 12 O 151/15 – ZD 2016, 231, 233 unter Rn. 62.

⁰³ Vgl. Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, 9.12.2015, COM(2015) 634 final.

⁰⁴ Vgl. Europäischer Gerichtshof, Urteil vom 19.10.2016 – C-582/14 – Breyer/Deutschland Tz. 43.

über die Daten seines Kunden verfügen, wüsste er beispielsweise nicht, an wen der Gartenteich geliefert werden sollte, und die Vertragserfüllung wäre unmöglich. Daher sind die Erhebung und die Nutzung dieser Daten, die allein der Vertragserfüllung dienen, datenschutzrechtlich zulässig.

Im Anwendungsfall 2 erlangen die Daten dagegen einen Gegenleistungscharakter, da dem Kunden im Gegenzug zur Preisgabe seiner Daten ein Preisnachlass gewährt werden soll. Die Bereitstellung der Daten bildet somit bereits eine der Hauptleistungen des Vertrags. Aufgrund des Grundsatzes der Vertragsfreiheit ist die Festlegung von Daten als Gegenleistung grundsätzlich möglich. Diese vertragliche Regelung gewährt dem Unternehmen S ein Zugriffsrecht auf die Daten des Betroffenen, das jedoch aufgrund gesetzlicher oder vertraglicher Vorgaben eingeschränkt sein kann.

Zudem stellt sich – beiden Vertragspartnern – die Frage nach dem Wert der Daten, dessen Bestimmung große Schwierigkeiten bereitet. Dies ist unter anderem dem Umstand geschuldet, dass Daten oft erst durch die nachträgliche Verknüpfung mit anderen Daten an Wert gewinnen. Eine erste Herausforderung wird daher sein, den Preisnachlass anhand der zur Verfügung gestellten Daten zu bestimmen. Überdies müssen zur Wirksamkeit des Vertrags seine wesentlichen Inhalte genau festgeschrieben werden. Dies bedeutet, dass genau festgelegt werden muss, welche Daten für die Gewährung des Preisnachlasses zur Verfügung gestellt werden und was mit diesen Daten geschieht.

Weil die Daten im Anwendungsfall 2 für die Vertragsabwicklung als solche nicht erforderlich sind, bedarf es nach dem Grundsatz des Verbots mit Erlaubnisvorbehalt (Art. 6 Abs. 1 DSGVO) der Einwilligung des Betroffenen. Diese ist neben der bloßen Hingabe der Daten – und neben dem (restlichen) Kaufpreis – als Hauptleistung geschuldet, da eine Verarbeitung der Daten nur bei Erteilung der datenschutzrechtlichen Einwilligung möglich ist. Die Einwilligung muss informiert erfolgen, was bedeutet, dass der Betroffene genau über die Art der preisgegebenen Daten und deren beabsichtigte Verarbeitungszwecke aufgeklärt werden muss. Der Verarbeitungszweck ist daher bereits vorab zwingend festzulegen, weshalb das Unternehmen S von Anfang an wissen muss, für welche Zwecke die Daten verarbeitet werden sollen.

Es ist wichtig, die datenschutzrechtlichen Anforderungen einzuhalten, da die DSGVO für Ver-

stöße empfindliche Sanktionen vorsieht. Für die Verarbeitung personenbezogener Daten ohne Einwilligung des Betroffenen können, sofern die Verarbeitung nicht durch eine gesetzliche Grundlage gedeckt ist, Bußgelder bis zu 20 Millionen Euro oder vier Prozent des gesamten weltweit erzielten Jahresumsatzes eines Unternehmens verhängt werden (was freilich nur bei erheblichen Verstößen auch nur annähernd eine solche Größenordnung erreicht).

In diesem Zusammenhang ist zudem zu bedenken, dass sich eine Rückabwicklung des Vertrags, beispielsweise wenn der Gartenteich im genannten Fallbeispiel einen Mangel aufweist, gerade bei Daten als Gegenleistung sehr schwierig gestaltet, da die Daten bereits mit anderen Daten verknüpft sein könnten. Aus technischer Sicht empfiehlt es sich daher, dass der Datensatz stets im Ganzen löschar bleibt. Insgesamt gilt, bereits im Vorhinein all diese Fragestellungen zu bedenken, um nachträgliche Schwierigkeiten vermeiden zu können.

WERT DER DATEN

Dass Daten, vor allem im digitalen Raum, einen ökonomischen Wert haben, ist unbestritten. Nicht nur Sachdaten können einen enormen wirtschaftlichen Wert aufweisen. Auch personenbezogene Daten sind oft Teil der Vermarktungsstrategie von Produkten und Dienstleistungen, auch werden sie als eigener Produktionsfaktor bezeichnet. Sie nehmen damit eine wichtige Rolle im Warenzyklus ein. Der ihnen hierdurch zukommende Wert macht sie zudem für den Datenhandel attraktiv. Den wirtschaftlichen Wert von Daten präzise zu bestimmen, stellt jedoch eine große Herausforderung dar.

Durch die doppelte Nutzbarkeit der Daten für die Entwicklung und Vermarktung von Produkten und Dienstleistungen (*Gebrauchswert* von Daten) entstand auch ein von den Marktmechanismen Angebot und Nachfrage bestimmter Datenhandel. Hierbei werden einzelne (Kunden-)Daten oder Datenpakete entweder zwischen Unternehmen verkauft beziehungsweise gekauft oder diese werden dem Unternehmer von Nutzern im Rahmen der Inanspruchnahme einer IT-Dienstleistung, etwa eines sozialen Netzwerks, zur Verfügung gestellt (*Tauschwert* von Daten).

Der Gebrauchs- und Tauschwert von Daten rechtfertigt es, ihnen einen Warencharakter zuzuschreiben. Die Annahme eines Warencharakters von Daten findet ihre Bestätigung ebenso im Vorschlag für eine europäische Richtlinie über bestimmte ver-

tragsrechtliche Aspekte der Bereitstellung digitaler Inhalte vom 9. Dezember 2015: „In der digitalen Wirtschaft haben Informationen über Einzelpersonen für Marktteilnehmer immer mehr einen mit Geld vergleichbaren Wert. Digitale Inhalte werden häufig nicht gegen Zahlung eines Preises bereitgestellt, sondern gegen Erbringung einer anderen Leistung als Geld, d.h. durch Gewährung von Zugang zu personenbezogenen oder sonstigen Daten.“⁰⁵

DATENSCHUTZRECHT

Nicht nur dem Anbieter des Gartenteichkonfigurators, bei dem (auch) die Kundendaten zum Vertragsgegenstand werden, stellen sich datenschutzrechtliche Herausforderungen.⁰⁶ Auch der Verkäufer beim „klassischen“ Vertrieb über einen Online-Shop könnte sich beispielsweise überlegen, ob er dem Käufer via E-Mail-Newsletter oder Telefonanruf nach ein paar Monaten ein Zubehör- oder Ersatzteil anbieten darf. Dies zeigt, dass im Rahmen der hier maßgeblichen Beleuchtung von Daten als Wirtschaftsgut der klare Fokus auf den Kundendaten liegt. Werden Kundendaten als ökonomisch bedeutsame Gegenleistung angesehen, stellt sich in datenschutzrechtlicher Hinsicht das Problem, wie der Grundsatz informationeller Selbstbestimmung zur Geltung gebracht werden kann.

Der *Grundsatz der Zweckbindung* besagt dabei zunächst, dass die Verarbeitung der Daten nur für die Zwecke erfolgen darf, für die sie auch erhoben wurden und die dem Betroffenen kommuniziert wurden. Daher muss der Zweck auch bereits bei Abschluss des Vertrags festgelegt sein. Greift für die jeweiligen datenschutzrechtlich relevanten Handlungen kein spezifischer Erlaubnistatbestand, sind hierfür nach dem sogenannten Verbot mit Erlaubnisvorbehalt die *Einwilligungen* der Kunden erforderlich. Diese müssen zu ihrer Wirksamkeit zahlreiche Voraussetzungen erfüllen, die im Einzelnen wiederum Probleme bereiten können:

Zunächst muss eine datenschutzrechtliche Einwilligung stets *freiwillig* sein. Dies wäre etwa nicht der Fall, wenn personenbezogene Daten verlangt werden, die grundsätzlich nicht für die Erfüllung des Vertrags erforderlich sind (Art. 7 Abs. 4 DSGVO). Damit sieht die DSGVO ein gegenüber den natio-

nen Vorschriften strengeres *Koppelungsverbot* vor. Dieses soll vor allem für die Konstellationen gelten, in denen eine Einwilligung in die Datenverarbeitung nicht erteilt werden muss, aber der Betroffene bei Verweigerung der Einwilligung auch keinen Vertrag abschließen kann. So sollte es im Ausgangsfall möglich sein, den Kauf auch ohne Konfigurator abzuschließen. Weiterhin muss der Kunde eine *informierte* Einwilligung abgeben können. Ihm müssen alle für die Disposition über seine Daten relevanten Informationen bereitgestellt werden.

Darüber hinaus ist die Einwilligung stets *frei widerruflich* (Art. 7 Abs. 3 DSGVO), hierauf kann der Datengeber auch nicht wirksam verzichten. Sind Daten jedoch nunmehr die Gegenleistung eines Vertrags und wird die Einwilligung nachträglich widerrufen, stellt sich die Frage, wie mit dieser „nachträglichen Nichterfüllung“ umgegangen werden muss. Dies ist juristisch umstritten und höchststrichterlich noch nicht geklärt.

AUF DEM WEG ZUM DATENRECHT

Als die DSGVO vor etwas über einem Jahr Geltung erlangte, war die Aufregung groß: Vom Bürokratiemonster war die Rede, von Rechtsunsicherheit und Überforderung, besonders bei Vereinen und kleinen Unternehmen. Tatsächlich hatten es die verantwortlichen staatlichen Stellen, allen voran die Datenschutzaufsichtsbehörden, zunächst versäumt, frühzeitig aufzuklären, praktische Tipps zur Umsetzung der DSGVO zu geben und Ängste zu nehmen. Als dies dann im Sommer 2018 nachgeholt wurde, hatte das im Ansatz großartige europäische Regelwerk bereits ein schlechtes Image, das es bis heute nicht losgeworden ist. Der gebetsmühlenartig vorgebrachte Hinweis, eigentlich ändere sich kaum etwas an der bisherigen Rechtslage, nutzt in Zeiten verunklarender Panik in den sozialen Netzwerken eher wenig. Dass nunmehr von Beratung statt Strafen bei Erstverstößen die Rede ist, beruhigt nur wenig, weil sich die Verunsicherung mittlerweile verfestigt hat.

Dabei ist das in der DSGVO normierte, aus der bislang geltenden Datenschutzrichtlinie entwickelte Datenschutzrecht so konzipiert, dass es dem Anliegen einer informationellen Selbstbestimmung der Betroffenen Rechnung trägt, die Verantwortlichen in die Pflicht nimmt, Datenverarbeitung transparent zu machen, und die aufsichtsbehördlichen Instrumente stärkt. So verhängte die polnische Datenschutzbehörde mitt-

⁰⁵ Europäische Kommission (Anm. 3), S. 18.

⁰⁶ Ausführlich hierzu Dirk Heckmann/Martin Scheurer, Datenschutzrecht, in: Dirk Heckmann (Hrsg.), juris Praxiskommentar Internetrecht, Saarbrücken 2019, Rn. 182ff.

lerweile ein Bußgeld von über 200 000 Euro an eine Wirtschaftsauskunftei, ein Krankenhaus in Portugal musste 400 000 Euro zahlen, und in Frankreich wurde Google mit dem bislang höchsten Bußgeld in Höhe von 50 Millionen Euro belegt.

Dass der Schutz personenbezogener Daten und der Privatsphäre dennoch nach wie vor lückenhaft ist, hat andere Gründe: Zum einen gehen viele Betroffene selbst sowohl mit ihren Daten als auch mit ihren IT-Systemen sorglos um; zum anderen ist juristisch noch nicht geklärt, ob die massenhafte Erstellung von Nutzerprofilen mit eher rudimentärer Information für die Betroffenen als Teil redlicher Geschäftsmodelle („Daten als Gegenleistung“) rechtmäßig oder gerade wegen der tendenziellen Intransparenz im Hinblick auf die dahinter stehenden Geschäftsinteressen unzulässig ist. Wie präzise und nachprüfbar müssen die Informationen sein, die ein Unternehmen in Bezug auf die hinter dem Geschäftsmodell verborgenen Modi und Zwecke der Datenverarbeitung den Nutzern mitzuteilen hat?

Genau an dieser Stelle schweigt das geltende Datenschutzrecht. Die in der DSGVO verankerten Prinzipien der Zweckbindung und Transparenz laufen ins Leere, soweit ein Unternehmen mit seinem datengetriebenen Geschäftsmodell vordergründig Zwecke wie Werbung und „Verbesserung des Nutzererlebnisses“ angeben kann und nicht zuletzt auch deswegen kaum sanktioniert wird, weil die Nutzer gerade ein solches Geschäftsgebarren fordern oder zumindest hinnehmen. So mag es im Detail kleinere Reformen und Anpassungen des Datenschutzrechts geben. Was – gleichsam als „großer Wurf“ – fehlt, ist die Regulierung eines Datenrechts, das sich nicht auf einen mehr oder weniger wirksamen Datenschutz kapriziert, sondern die gesamte Wertschöpfungskette entlang der Datenerfassung und Datennutzung interessengerecht in den Blick nimmt. Auch und gerade das Datenschutzrecht steht einem maßvoll regulierten Datenverwertungsrecht nicht entgegen. In diese Richtung geht auch die Arbeit der Datenethikkommission der Bundesregierung, die bis Oktober 2019 Eckpunkte für ein ethisch verantwortbares Datenrecht entwickelt.

Zumindest in der Theorie wirkt das geltende Datenschutzrecht der DSGVO konsistent. Was allerdings noch aussteht, ist ein Datenrecht, das auch nicht personenbezogene Daten einbezieht. Ein solches Datenrecht würde Phänomene wie Big-Data-Analysen, Cloud-Computing, die Informationsverarbeitung über die Blockchain und vieles andere mehr realistisch einbinden, ohne die not-

wendige politische Auseinandersetzung um sinnvolle Datennutzung zu unterbinden. Man muss freilich auch konstatieren, dass die Gestaltungsmöglichkeiten des Gesetzgebers im Daten(schutz) recht begrenzt sind, weil Regulierung im Internet auch vor dem Hintergrund internationaler Verflechtungen und autonomer Steuerung der Akteure wenig Durchschlagskraft hat.

Um dies an einem Beispiel zu illustrieren: Sehr viele Services werden heute cloud-basiert angeboten, entsprechende Inhalte auf verteilten Servern bereitgehalten, wo sie die Nutzer orts- und zeitunabhängig abrufen können. Zu den größten Anbietern gehören US-amerikanische IT-Dienstleister, deren Angebote oft wirtschaftlich attraktiv und kundenorientiert sind, sodass sowohl private als auch geschäftliche und gar behördliche Nutzer gerne darauf zugreifen. Weil in den USA aber schon aufgrund vielfältiger Zugriffsmöglichkeiten der Geheimdienste und Sicherheitsbehörden kein dem europäischen Recht vergleichbares Datenschutzniveau herrscht, wird die Nutzung entsprechender Cloud-Services von den Datenschutzbehörden sehr kritisch gesehen. Ein Verbot der Nutzung eines solchen vermeintlich unsicheren Dienstes wird gleichwohl kaum vorgeschlagen, weil es zumindest aus Sicht der Mehrheit der Nutzer keine brauchbare Alternative gibt. Lösungen wie der sogenannte EU-US Privacy Shield (in Ablösung des Safe-Harbor-Abkommens, das der Europäische Gerichtshof 2015 für ungültig erklärt hat) sind zweifelhaft, das Dilemma der unterschiedlichen Rechtskulturen zwischen den USA und der EU im Hinblick auf den Datenschutz bleibt.⁰⁷

Und dies ist durchaus symptomatisch für die Internetnutzung. Bestimmte Verhaltensweisen (wie die Nutzung von Cloud-Services, das Tauschen von Inhalten in sozialen Netzwerken oder die Selbstvermessung über Fitnesstracker) beruhen auf reinen Nützlichkeits- und Bequemlichkeitserwägungen, bei denen das Datenschutzrecht, das Urheberrecht oder der Schutz der Privatsphäre kaum einen Platz finden. Diesen Umstand machen sich viele Anbieter zunutze. Die Menschen nutzen diese Technologien, weil sie nützlich, preiswert, attraktiv und besonders einfach (im Sinne von „plug and play“) gestaltet sind. Die Hersteller forcieren die Verbreitung durch ihre Geschäftsmodelle. Dieses System setzt eine erhebliche, permanente und oft unmerkliche Erhebung, Verarbeitung und Übermittlung personenbezogener Daten voraus: Nur so können nämlich der güns-

⁰⁷ Vgl. ebd., Rn. 702ff.

tige Preis („Daten als Währung“), der hohe Nutzen („Mehrwert durch Datenverknüpfung“) und damit die starke Verbreitung durch Netzwerkbildung („kritische Masse“) gewährleistet werden. Es lässt sich hier durchaus von einer „Plug-and-play-Falle“ sprechen, weil diesem System ein hoher Verführungsgrad innewohnt, der sich auf die Einwilligungsfähigkeit zur Datenverarbeitung auswirkt. Die Datenverknüpfung ist – zum Teil technisch, zum Teil auch durch das Geschäftsmodell bedingt – unmerklich, eine kritische Distanz der Nutzer hierzu weder erwünscht noch praktisch umsetzbar.⁰⁸

Hier gilt es letztlich anzusetzen: Ein wirksamer Datenschutz setzt ein Datenschutzbewusstsein und damit ein hohes, auf ausreichender Sachkenntnis beruhendes Verständnis von Datenverarbeitung voraus. Diese „Digitalkompetenz“ gilt es schon früh in den Schulen und dann über (betriebliche) Fortbildung bis ins hohe Alter zu vermitteln. In der Diskussion um „digitale Bildung“ ist dies ein wichtiger Punkt.

DATENETHIK

Nicht zuletzt mit Blick auf die skizzierten Steuerungsdefizite wird über die Frage rechtlicher Regulierbarkeit hinaus auch diskutiert, ob Geschäftsmodelle, die einen schleichenden Verlust an Privatheit zur Folge haben können, überhaupt ethisch verantwortbar sind: Wie redlich ist es, unzählige Internetnutzer in die „Plug-and-play-Falle“ tappen zu lassen?

Die Ethikkommission für automatisiertes und vernetztes Fahren hat hierzu in ihrem Abschlussbericht eine Regel formuliert: „Erlaubte Geschäftsmodelle, die sich die durch automatisiertes und vernetztes Fahren entstehenden, für die Fahrzeugsteuerung erheblichen oder unerheblichen Daten zunutze machen, finden ihre Grenze in der Autonomie und Datenhoheit der Verkehrsteilnehmer. Fahrzeughalter oder Fahrzeugnutzer entscheiden grundsätzlich über Weitergabe und Verwendung ihrer anfallenden Fahrzeugdaten. Die Freiwilligkeit solcher Datenpreisgabe setzt das Bestehen ernsthaft-

ter Alternativen und Praktikabilität voraus. Einer normativen Kraft des Faktischen, wie sie etwa beim Datenzugriff durch die Betreiber von Suchmaschinen oder sozialen Netzwerken vorherrscht, sollte frühzeitig entgegengewirkt werden.“⁰⁹

Hier wird deutlich, dass sich die Möglichkeit einer Verwertung personenbezogener Daten (hier: Fahrverhaltensdaten, Standortdaten etc.) nicht alleine nach dem Datenschutzrecht richtet, dass es also nicht genügt, eine Einwilligung einzuholen. Vielmehr ist das jeweilige Geschäftsmodell zu hinterfragen. Suchmaschinen und soziale Netzwerke entfalten insofern eine normative Kraft des Faktischen, weil sie eine große Verführungskraft zur Inanspruchnahme des Dienstes entfalten und alsdann eine faktische Abhängigkeit der Nutzer herbeiführen. Zunächst werden kostenfrei attraktive Services zur Verfügung gestellt, die von einer großen Anzahl von Personen weltweit genutzt werden, die letztlich nicht mehr auf diese Nutzung verzichten wollen. Dass diese Leistungen mit den eigenen Daten „bezahlt“ werden, erscheint wiederum unkritisch, weil die Verwertung der Daten zumeist mit dem werbefinanzierten „Privatfernsehen“ verglichen wird.

Dass allerdings die Erzeugung und vielfältige Verwertung von Nutzerprofilen tiefe Einblicke in das Privatleben und die Persönlichkeit gewährt und über die Ermittlung von Nutzerpräferenzen zu Werbezwecken weit hinausgeht, machen sich viele nicht bewusst. Und so erreicht diese flächendeckende Auswertung von Persönlichkeitsmerkmalen eine ethische Dimension. Scheint diese Form der „Selbstausbeutung“ bei der Nutzung von Google und Facebook kaum mehr reversibel, soll etwa beim autonomen Fahren verhindert werden, dass die Betroffenen die Hoheit über die vielfältig damit verbundenen Daten aus der Hand geben. Diese Frage ist zukunftsweisend: Was beim autonomen Fahren schon vielfältig, aber noch einigermaßen überschaubar ist, verliert im Internet der Dinge vollends alle Konturen. Wenn künftig alles mit allem verknüpfbar ist, sind unbegrenzte Möglichkeiten denkbar, (vermeintlich) nützliche Geräte, Anwendungen und Dienste anzubieten, die „das Nutzererlebnis verbessern“. Es kostet nur die Privatheit.¹⁰

⁰⁸ Zur Plug-and-play-Falle vgl. Dirk Heckmann, Persönlichkeitschutz im Internet, in: Neue Juristische Wochenschrift 36/2012, S. 2631–2635.

⁰⁹ Ethikkommission automatisiertes und vernetztes Fahren (Anm. 1), S. 12.

¹⁰ Zu möglichen Schutzkonzepten vgl. Dirk Heckmann, Smart Life – Smart Privacy Management, in: Kommunikation und Recht 1/2011, S. 1–6.

DIRK HECKMANN

ist Inhaber des Lehrstuhls für Öffentliches Recht, Sicherheitsrecht und Internetrecht sowie Leiter der Forschungsstelle für IT-Recht und Netzpolitik an der Universität Passau.

heckmann@uni-passau.de

KARTELLRECHT IN DER DATENÖKONOMIE

Rupprecht Podszun

Das Oberlandesgericht Nürnberg hatte 2016 einen Fall zu entscheiden, der auf den ersten Blick wenig aufregend scheint.⁰¹ Es ging um eine Satzungsbestimmung der Taxizentrale Nürnberg, der fast alle der rund 300 in der Stadt tätigen Taxi-Unternehmen angeschlossen sind. Die Genossenschaft hatte in der Satzung festgelegt, dass geschäftliche Informationen, die Fahrerinnen und Fahrer von der Zentrale erhalten, nicht weitergegeben werden dürfen. Das klingt zunächst nach einer Selbstverständlichkeit: Der Schutz von Betriebsgeheimnissen ist anerkannt. Doch die Taxizentrale stellte klar, dass das Weitergabeverbot auch für Positions- und Bewegungsdaten der Fahrzeuge gelte, wenn die Daten im Zusammenhang mit einem von der Taxizentrale vermittelten Auftrag stünden. Im Klartext: Erhält ein Taxi-Unternehmer einen Auftrag über die Zentrale, darf er nicht an Dritte berichten, wo er sich gerade befindet. Die Folge: Konkurrierende Vermittler wie Mytaxi oder Uber hätten nicht gewusst, wo sich Taxen gerade befinden. Ist es erlaubt, eine solche Satzungsbestimmung zu vereinbaren? Das Oberlandesgericht kippte die unscheinbare Bestimmung und machte damit den Weg frei für die digitalen Vermittlungsdienste. Unter Berufung auf das Gesetz gegen Wettbewerbsbeschränkungen (GWB) konnte der Wettbewerb Fahrt aufnehmen, und innovative, nutzerfreundlich gestaltete Apps traten neben den Anruf bei der Taxizentrale.

Der Rechtsstreit ist symptomatisch für die Verschiebungen im Wettbewerbsgefüge einer datengetriebenen Ökonomie. Daten sind zu einem entscheidenden Wettbewerbsparameter geworden. Neue Angebote drängen in den Markt und treten in Konkurrenz zu etablierten Geschäftsmodellen, was zu Verteilungskämpfen führt, die auch mit rechtlichen Waffen gefochten werden. So willkommen der Wettbewerb ist, so wenig sollte übersehen werden, was eigentlich das Neue ist. Die App-Anbieter vermitteln Aufträ-

ge. Sie senken die Suchkosten und führen auf bequeme Weise Anbieter und Nachfrager zusammen. Die eigentlich relevante Leistung bleibt aber die Beförderung eines Fahrgastes. Das erledigt kein Silicon-Valley-Unternehmen, sondern ein selbstständiger Taxler mit überschaubarem Verdienst.

ENTWICKLUNG DES KARTELLRECHTS: ZÄHMUNG DER TITANEN

Das Beispiel aus Nürnberg zeigt auch, wie sehr sich in kurzer Zeit die Erwartungen an die Ordnung des Wettbewerbs – und diese leistet das Kartellrecht – gewandelt haben. Denn inzwischen wird nach den Regeln zum Schutz des Wettbewerbs nicht mehr primär gerufen, um Schneisen für datenbasierte Geschäftsmodelle zu schlagen. Vielmehr sollen mit rechtlichen Regeln nun die Auswüchse eines Wildwest-Kapitalismus eingefangen werden. Selbst der des Sozialismus unverdächtige „Economist“ rief 2018 nach einer Zähmung der Technologie-Giganten.⁰² Andreas Mundt, der Präsident des Bundeskartellamts, und Margrethe Vestager, scheidende Wettbewerbskommissarin der Europäischen Union, sind zu „Stars“ geworden, das Kartellrecht ist zur Projektionsfläche für eine neue Wirtschaftsordnung geworden. Bundeskartellamt und Europäische Kommission, so scheint es, sind für viele die willkommenen Gegenspieler zu den sogenannten GAFA-Unternehmen geworden: Google, Amazon, Facebook und Apple, jene sensationell erfolgreichen Titanen des Internetzeitalters, die immer mehr Aspekte des Lebens und der Wirtschaft kontrollieren. Können die Kartellbehörden das?

Kartellrecht hat die Aufgabe, den wirtschaftlichen Wettbewerb zu schützen: Unternehmen sollen in Rivalität miteinander in das Ringen um Angebot und Nachfrage eintreten. Sie dür-

fen sich nicht zu Lasten ihrer Abnehmer absprechen; wenn sie wirtschaftlich mächtig sind, dürfen sie ihre Macht nicht missbrauchen. Adam Smith, der vom Moralphilosophen zum ersten modernen Wirtschaftswissenschaftler wurde, hatte solche Grundbedingungen des Funktionierens von Märkten in einer freien Wirtschaft schon in seinem epochemachenden Werk „Der Wohlstand der Nationen“ 1776 erkannt. In rechtliche Regelungen wurden die Erkenntnisse zuerst Ende des 19. Jahrhunderts in Kanada und den USA übersetzt. In den USA waren einzelne Unternehmensgruppen (Trusts), etwa die von John Rockefeller oder J.P. Morgan, so mächtig geworden, dass sie ökonomisch kaum mehr kontrolliert werden konnten. Niedrige Preise für Verbraucherinnen und Verbraucher oder technische Fortentwicklungen sind aber nicht zu erwarten, wenn Unternehmen zu mächtig werden und ihnen die Kontrolle durch den Wettbewerb fehlt. Darum wurden die ersten Wettbewerbsgesetze geschaffen.

Doch der Impuls war nicht nur das Streben nach Effizienz. Von Beginn an war das Kartellrecht auch politisch gedacht. Dem Senator John Sherman, nach dem das amerikanische Antitrustgesetz von 1890 bis heute benannt ist, war auch der Einfluss der Trusts auf das politische Geschäft ein Graus. Ganz ähnlich ist auch die deutsche und europäische Kartellrechtsgeschichte von einem doppelten Impuls geprägt: In Deutschland wurde das GWB auf Drängen der US-amerikanischen Befreier 1958 eingeführt. Parallel wurde im europäischen Recht das Kartellrecht verankert. Einflussreich waren damals die Vorstellungen der ordoliberalen Denker der Freiburger Schule um Walter Eucken und Franz Böhm, die in Wirtschaftsminister Ludwig Erhard einen Partner fanden. Der Freiburger Schule galt Kartellrecht als notwendiger Rechtsrahmen für eine effiziente Wirtschaft, in der sich Unternehmen immer aufs Neue beweisen müssen. Böhm sah den Wettbewerb aber auch als „genialstes Entmachtungsinstrument der Geschichte“⁰³ –

Kartellrecht als ein politisch-sittlich begründeter Rahmen, der Freiheit sichert, auch damit sich ein selbstbewusstes Unternehmertum nicht wieder gleichschalten lässt.

Von dieser ideengeschichtlichen Grundierung löste sich das Kartellrecht im Laufe seiner Anwendungspraxis, es wurde regelrecht entpolitisiert. Insbesondere die in den USA erfolgreiche Chicago School verrückte die Ziele des Kartellrechts und auch die Interventionsschärfe; ab den 1980er Jahren wurde das Kartellrecht einseitig auf die Sicherung niedriger Verbraucherpreise ausgerichtet. Von echten Kartellen, also Preisabsprachen von Wettbewerbern, abgesehen fand eine Durchsetzung in den USA kaum mehr statt. Die Nachweisanforderungen für eine behördliche Intervention in den Wettbewerb stiegen erheblich. Zwar wurde dieser Laissez-faire-Ansatz in Deutschland und Europa nicht in gleicher Weise nachvollzogen. Doch ökonomische Berechnungen (statt rechtlicher Wertungen) und Schutz des Verbrauchers (statt Schutz des Wettbewerbsprozesses) wurden auch hier bedeutsamer. Dieser „more economic approach“ wird erst seit Kurzem wieder kritischer gesehen.⁰⁴

Während das Kartellrecht derzeit in diesem nervösen Selbstfindungsprozess steckt, kommt es zu Disruptionen in der Wirtschaft. Inzwischen gibt es keine Branche mehr, die nicht komplett digitalisiert und damit umgewälzt wird. Darauf war und ist das Kartellrecht nicht vorbereitet, obwohl es seine Aufgabe ist, das Funktionieren der Marktwirtschaft abzusichern.

VERÄNDERUNGEN DES WETTBEWERBS: NEUE PLANWIRTSCHAFT?

Die Digitalisierung hat die Marktwirtschaft nicht nur durch neue Produkte oder Dienstleistungen bereichert, sondern ihre Strukturen grundlegend verändert. Das Kartellrecht steht damit vor ungekannten Phänomenen. Charakteristisch ist die Veränderung des Wettbewerbs durch datengetriebene Plattformen, die in kurzer Zeit in verschiedenen Märkten so gewaltige Macht entfalten, dass traditionelle Strukturen erschüttert und teilweise ersetzt werden.

01 Vgl. OLG Nürnberg, Urteil vom 22. 1. 2016, 1 U 907/14, Taxi-Positionsdaten, in: *Wirtschaft und Wettbewerb (WuW)* 4/2016, S. 194–198.

02 Vgl. *The Economist*, 18. 1. 2018, Cover: „The New Titans – And How to Tame Them“.

03 Franz Böhm, *Demokratie und ökonomische Macht*, in: *Institut für ausländisches und internationales Wirtschaftsrecht (Hrsg.)*, *Kartelle und Monopole im modernen Recht*, Karlsruhe 1961, Bd. 1, S. 2–24, hier S. 22.

04 Vgl. etwa Lina Khan, *Amazon’s Antitrust Paradox*, in: *Yale Law Journal* 3/2017, S. 710–805.

Die bedeutendsten Unternehmen der Welt, gemessen an ihrem Börsenwert, sind Plattformunternehmen. Online-Plattformen führen verschiedene Nutzerinnen und Nutzer zusammen, sei es zur Kommunikation oder zum Matching von Angebot und Nachfrage.⁰⁵ Kennzeichen vieler Plattformen sind die Beziehungen zu mehreren Marktseiten.⁰⁶ Ihre Stärke ziehen sie aus ihrer Datenkenntnis und Netzwerkeffekten: Je mehr Nutzer eine Plattform hat, desto attraktiver wird sie für weitere Nutzer. Plattformen nehmen dann in der Regel eine Vermittlungsfunktion wahr. Darin lässt sich durchaus eine Marktplatzfunktion oder gar die Funktion als Regulator sehen – als eine Instanz, die ihre Regeln selbst setzt.⁰⁷ Durch den Einsatz von Datenmacht gelingt es starken Plattformen, die Transaktionskosten erheblich zu senken und für Nutzer attraktiv zu scheinen. Netzwerkeffekte und Datenzugang erhöhen mit zunehmendem Erfolg die Marktzutrittsschranken für alternative Anbieter. So wird der Wettbewerb auf dem Markt rasch zu einem Wettbewerb um den Markt: Hat eine Plattform eine substanziell große Zahl an Nutzern gewonnen, ist die Marktposition kaum mehr bestreitbar – der Markt kippt: *The winner takes it all*. Für Verbraucher ist es häufig bequem, nur eine Plattform zu nutzen (*single-homing*), statt parallel auf mehreren Plattformen aktiv zu sein (*multi-homing*) oder von einer Plattform zu einer anderen zu wechseln. Ist eine Monopolsituation geschaffen, was für den Wettbewerb die denkbar schlechteste Lösung ist, kann diese durch technische *Lock-in*-Effekte oder vertragliche Regeln abgesichert werden.

Diese „Plattformisierung“ hat die Wirtschaft massiv verändert und den GAFA-Unternehmen volle Kassen beschert. Sie verfügen nun über schier unbegrenzte finanzielle Mittel, nicht zu-

letzt dank dramatisch hoher Skalenerträge.⁰⁸ Was die Wirtschaft so umwälzt, ist für das Kartellrecht schwer zu greifen: Mehrseitige Märkte mit komplexen Wechselbeziehungen und nicht monetäre Währungen wie Daten lassen sich noch kaum darstellen.

Mit diesen Veränderungen geht auch ein anderes Selbstverständnis der Unternehmen einher. Der Investor Peter Thiel hat als Philosophie des Silicon Valley ausgegeben: „Competition is for losers.“⁰⁹ Dieser Satz markiert eine Abkehr vom Wettbewerbsprinzip als Treiber der Marktwirtschaft. Für die Operatoren von Plattformen und Ökosystemen geht es nicht mehr um das dynamische Ringen mit Wettbewerbern. Vielmehr wird der Wettbewerb an die Peripherie gedrängt: Dort kämpfen die klassischen Leistungserbringer darum, überhaupt Zugang zur Plattform oder zum Ökosystem zu erhalten, damit noch die Chance auf eine Vermittlung an den Kunden gegeben ist. Wer bei Google nicht gelistet ist, wer seine Produkte nicht bei Amazon zeigen kann, ist raus.

Die Verteilung knapper Ressourcen (und das leistet die Wirtschaft) wird so neu organisiert: Im Zentrum des neuen Mechanismus stehen datenhungrige Orchestratoren, die nach Datenlage Angebot und Nachfrage zusammenführen. Aus der „unsichtbaren Hand“ (Adam Smith) wird eine Big-Data-Anwendung, aus einem spontanen „Entdeckungsverfahren“ (Friedrich von Hayek)¹⁰ wird ein intelligent designtes Zuteilungssystem. Im Prinzip ist dieses „who gets what and why“¹¹ eine modernisierte Form der Planwirtschaft.

RICHTUNGWEISENDE FÄLLE

Dem steht das freiheitsverpflichtete Konzept des Wettbewerbs entgegen. Es manifestiert sich in einzelnen kartellrechtlichen Fällen. Das Bundeskartellamt und die Europäische Kommission haben im Umgang mit digitalen Unternehmen weltweit Maßstäbe gesetzt. Dabei haben sie im Wesentlichen nur drei Instrumente zur Verfü-

⁰⁵ Vgl. Andreas Engert, Digitale Plattformen, in: Archiv für die civilistische Praxis 2–4/2018, S. 304–376; Rupprecht Podszun/Stephan Kreifels, Digital Platforms and Competition Law, in: Journal of European Consumer and Market Law 1/2016, S. 33–39.

⁰⁶ Grundlegend dazu Jean-Charles Rochet/Jean Tirole, Platform Competition in Two-Sided Markets, in: Journal of European Economic Association 4/2003, S. 990–1029. Siehe auch Bundeskartellamt (BKartA), Marktmacht von Plattformen und Netzwerken, Arbeitspapier, Juni 2016, <https://t1p.de/pddz>.

⁰⁷ Vgl. Heike Schweitzer, Digitale Plattformen als private Gesetzgeber, in: Zeitschrift für europäisches Privatrecht 1/2019, S. 1–12.

⁰⁸ Vgl. Jacques Crémer/Yves-Alexandre de Montjoye/Heike Schweitzer, Competition Policy for the Digital Era, Report for the European Commission, Brüssel 2019, S. 19, <https://t1p.de/bnfa>.

⁰⁹ Peter Thiel, Competition Is for Losers, 12.9.2014, www.wsj.com/articles/peter-thiel-competition-is-for-losers-1410535536.

¹⁰ Friedrich A. von Hayek, Der Wettbewerb als Entdeckungsverfahren, in: ders., Freiburger Studien, Tübingen 1994, S. 249–265.

¹¹ Alvin Roth, Who Gets What and Why, New York 2016.

gung: Sie können ihre Anordnungen auf das Verbot wettbewerbsbeschränkender Absprachen, auf das Verbot des Missbrauchs von Marktmacht und die präventive Kontrolle von Unternehmensübernahmen und -fusionen stützen.¹²

Die Geschichte des digitalen Kartellrechts begann zunächst im Einzelhandel, als es zwischen Online-Handel und klassischen Ladengeschäften zu Verteilungskämpfen kam. Hersteller, insbesondere von Markenprodukten, sahen hier die Möglichkeit, den Vertrieb zu steuern und teilweise selbst zu übernehmen. Das Bundeskartellamt öffnete den Wettbewerb durch einen starken Schutz des ungehinderten Online-Vertriebs.¹³ Rasch rückten aber Plattformbetreiber in den Fokus der Ermittlungen des Amts. Untersucht wurden insbesondere sogenannte Bestpreisklauseln von Hotelbuchungsplattformen.¹⁴ Demnach dürfen Hoteliers weder auf anderen Websites noch selbst günstigere Raten verlangen als auf der Plattform, die sich eine solche Bestpreisklausel einräumen lässt. Das Bundeskartellamt untersagte solche Klauseln weitgehend, da es eine Abschottung von Märkten fürchtete.

Assoziiert wird digitales Kartellrecht aber vor allem mit den großen Missbrauchsfällen: Die Europäische Kommission leitete 2010 ein Verfahren gegen Google ein. Der Vorwurf: Google habe seine Marktmacht bei Online-Suchanfragen – das Unternehmen hält hier in fast allen europäischen Ländern beständig einen Marktanteil von über 90 Prozent – ausgenutzt, um auf anderen Märkten ebenfalls mächtig zu werden, beispielsweise als Preisvergleichsanbieter.¹⁵ Indem der eigene Preisvergleichsdienst Google Shopping gegenüber Konkurrenten wie Idealo in der Suchliste besser platziert werde, falle es Letzte-

ren schwer, überhaupt Nutzer zu erreichen. Ein Link, der nicht auf der ersten Google-Suchseite zu finden ist, wird wesentlich seltener angeklickt. Die Google-Suche, so die Argumentation, sei zum Gatekeeper für Internetangebote geworden. Google könne so eigene Dienste bevorzugen und am Markt durchsetzen.

So plausibel die Argumentation scheinen mag, so schwierig ist der Fall bei genauer juristischer Prüfung. Das Verfahren kam daher nicht vom Fleck. Die EU-Kommission benötigte sieben Jahre bis zu einem Verfahrensabschluss – im Internetzeitalter eine halbe Ewigkeit. Doch die Beendigung des Verfahrens durch die resolute Margrethe Vestager, die den Fall von ihrem Vorgänger übernahm, wurde zu einem Paukenschlag: Die Kommission verhängte eine Rekordgeldbuße von 2,42 Milliarden Euro und untersagte die Bevorzugung eigener Dienste. Ein halbes Jahr später legte sie mit einem Bußgeld von 4,34 Milliarden Euro wegen der Abschottung des Google-Betriebssystems Android nach.¹⁶

Das Bundeskartellamt erarbeitete sich seinen Ruf als Digitalbehörde vor allem 2019 mit der Untersagung der Datenzusammenführung ohne angemessene Einwilligung bei Facebook.¹⁷ Dieses Verfahren endete zwar ohne schwindeleerregende hohe Geldbuße, ist aber in der Herleitung und wohl auch in der Auswirkung spektakulärer. Die Verfügung zielt in das Herz des Geschäftsmodells von Facebook: Das soziale Netzwerk sammelt über die eigene Seite, über die Dienste von Tochtergesellschaften wie Instagram und WhatsApp sowie über Drittseiten mithilfe der sogenannten Facebook Business Tools (von denen die Nutzerinnen und Nutzer kaum etwas merken) Daten und fügt sie zu umfassenden Nutzerprofilen zusammen.¹⁸ Dafür, so das Bundeskartellamt, fehle die datenschutzrechtlich erforderliche Einwilligung der Nutzenden. Durch die Untersagung dieser Praxis erreicht das Amt quasi eine „innere Entflechtung“¹⁹ des Unternehmens.

Rechtlich ist dieses Verfahren richtungsweisend, weil es das Kartellrecht mit dem Datenschutzrecht kombiniert. Damit bringt das Amt

12 Rechtliche Grundlagen sind §§ 1, 19 und 35 ff. GWB, Art. 101 des Vertrags über die Arbeitsweise der Europäischen Union sowie die EU-Fusionskontrollverordnung.

13 Vgl. BKartA, Beschluss vom 26. 8. 2015, B2-98/11, Asics, in: WuW 4/2016, S. 198–205; bestätigt durch Bundesgerichtshof (BGH), Beschluss vom 12. 12. 2017, KVZ 41/17, Preisvergleichsmaschine, in: WuW 3/2018, S. 139 ff. Vgl. auch EuGH, Urteil vom 13. 10. 2011, Rs. C-439/09, Pierre Fabre, in: WuW 1/2012, S. 93–101; EuGH, Urteil vom 6. 12. 2017, Rs. C-230/16, Coty, in: WuW 1/2018, S. 27–31.

14 Vgl. Stephanie Pautke/Jörg-Martin Schultze, Wettbewerbsbeschränkungen im Kontext digitaler Plattformen, in: WuW 1/2019, S. 2–10.

15 Vgl. Europäische Kommission, Beschluss vom 27. 6. 2017, Fall AT.39740, Google Search (Shopping).

16 Vgl. dies., Beschluss vom 18. 7. 2018, Fall AT.40099, Google Android.

17 BKartA, Beschluss vom 6. 2. 2019, B6-22/16, Facebook.

18 Siehe hierzu auch den Beitrag von Wolfie Christl in dieser Ausgabe (Anm. d. Red.).

19 Andreas Mundt, zit. in: BKartA, Pressemitteilung, 7. 2. 2019.

zwei Schlüsselthemen der digitalen Welt zusammen: Datenschutz und Wettbewerb. Der Hebel des durchsetzungsstarken Kartellrechts wird eingesetzt, um den in der Durchsetzung traditionell schwachen Datenschutzregeln zum Durchbruch zu verhelfen. Die dreiköpfige Beschlussabteilung des Bundeskartellamts, die die Entscheidung getroffen hat, stützt sich auf selten angewendete Normen des Kartellrechts und eine ungewöhnliche Linie in der deutschen Rechtsprechung.²⁰ Der Begründungsaufwand, der auf den 309 Seiten der Entscheidung getrieben wird, ist erheblich. Damit steht das von der breiten Öffentlichkeit überwiegend wohlwollend kommentierte Facebook-Verfahren auch sinnbildlich für die Schwierigkeiten, mit traditionellen Rechtsbegriffen die Phänomene der Digitalwirtschaft zu ordnen.

Die wenigsten Vereinbarkeitsprobleme von digitaler Realität und klassischem Recht sind in der formalisierten Fusionskontrolle zu erwarten: Hier haben Unternehmen ihre Übernahmen anzumelden, sobald sie bestimmte Umsatzschwellen überschreiten. Die Behörden prüfen dann – vor Vollzug – ob eine erhebliche Behinderung wirksamen Wettbewerbs nach dem Zusammenschluss zu erwarten ist.²¹ Die Bilanz des Kartellamts und der Europäischen Kommission hat indes einen gravierenden Schönheitsfehler: Die Zukäufe der GAFA-Unternehmen blieben weitgehend unkontrolliert, jedenfalls aber ohne substantielle Beschränkungen. Die Silicon-Valley-Giganten konnten durch Einsatz ihrer Finanzmittel ungehindert weiterwachsen. Das Paradebeispiel liefert die Einverleibung des Messaging-Dienstes WhatsApp ins Facebook-Imperium: 2014 zahlte Facebook 19 Milliarden US-Dollar für den potenziellen Konkurrenten – eine astronomische Summe, die erahnen lässt, für wie bedeutsam die Strategen bei Facebook den Zukauf hielten. Doch der Fall rutschte durch die Maschen der deutschen und der europäischen Fusionskontrolle: Die Umsätze von WhatsApp waren zu

niedrig, um die Transaktion für eine Kontrolle zu qualifizieren. Nur mithilfe eines mühsamen Umwegs konnte die Europäische Kommission die Transaktion doch noch prüfen. Auf gerade einmal 36 Seiten legte die Kommission aber bereits einen Monat nach Eingang der Anmeldung dar, dass keine wettbewerbslichen Bedenken bestehen.²²

WETTBEWERBSORDNUNG 4.0

Die Bemühungen der Wettbewerbsbehörden legen so die Stärken und Schwächen des Kartellrechts offen. Eine „Wettbewerbsordnung 4.0“ ist mit den derzeitigen Regeln nicht zu schaffen. Das verwundert nicht. Eine völlig veränderte Wirtschaft bedarf auch eines neu gestalteten Ordnungsrahmens.

Das gilt zunächst für das Kartellrecht selbst. Der deutsche Gesetzgeber hat dabei bereits eine Pionierrolle eingenommen und etwa eine 400-Millionen-Euro-Kaufpreisschwelle für Fusionsanmeldungen eingeführt: Die WhatsApp-Übernahme wäre nun beim Bundeskartellamt anmeldepflichtig. 2017 wurden zudem Regeln eingeführt, mit denen gezielt auf Schwierigkeiten der Kartellrechtsanwendung auf digitalen Märkten reagiert wird: Märkte ohne finanzielle Gegenleistungen werden nun als Märkte im Sinne des Gesetzes angesehen (§ 18 Abs. 2a GWB). Zudem wurden für mehrseitige Märkte und soziale Netzwerke Kriterien zur Klärung der Frage aufgenommen, wann ein Unternehmen als marktmächtig zu gelten hat, etwa bei Netzwerkeffekten und sehr gutem Datenzugang (§ 18 Abs. 3a GWB).

Mit der in Planung befindlichen zehnten GWB-Novelle werden weitere Schritte erwartet.²³ Die Bundesregierung hat die Vorbereitungen in eine „Wettbewerbskommission 4.0“ verlagert.²⁴ Schon jetzt liegen eine Studie zur Verschärfung der Missbrauchsaufsicht und, auf europäischer Ebene, der Report von drei Sonderberatern der Wettbewerbskommissarin

²⁰ Siehe vor allem BGH, Urteil vom 7.6.2016 – KZR 6/15, Pechstein/ISU, in: WuW 7–8/2016, S. 364–369. Vgl. Torsten Körber, Die Facebook-Entscheidung des Bundeskartellamts – Machtmissbrauch durch Verletzung des Datenschutzrechts?, in: Neue Zeitschrift für Kartellrecht 4/2019, S. 187–195.

²¹ Vgl. §§ 35 ff. GWB sowie Art. 1 und 3 der EU-Fusionskontrollverordnung.

²² Vgl. Europäische Kommission, Entscheidung vom 3.10.2014, Fall M.7217, Facebook/WhatsApp.

²³ Vgl. Koalitionsvertrag zwischen CDU, CSU und SPD, 12.3.2018, Zeilen 1938 ff. und 2755 ff., www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf.

²⁴ Vgl. Bundesministerium für Wirtschaft und Energie (BMWi), Kommission Wettbewerbsrecht 4.0, 2018, <https://t1p.de/xhzi>.

vor.²⁵ Fünf Fragen stehen für die GWB-Reform im Vordergrund:

Die vielleicht schwierigste Frage ist, *erstens*, ob bei einer sich abzeichnenden Monopolisierung frühzeitiger eingegriffen werden kann. Dazu wären neue Aufgreiffilter und neue Missbrauchstatbestände erforderlich. Dann ließe sich das Kippen einzelner Märkte möglicherweise verhindern.²⁶

Ein weiteres Problem stellt sich, *zweitens*, in der Fusionskontrolle: Wie kann es Unternehmen untersagt werden, potenzielle Wettbewerber aufzukaufen (sogenannte *killer acquisition*)? Während das Ziel klar erscheint, ist die rechtliche Umsetzung in Ermangelung harter, rechtssicher anzuwendender Kriterien unklar.

Eine zusätzliche Thematik hängt, *drittens*, an der Bedeutung der Daten für den Wettbewerb. Zum einen wird nach Möglichkeiten gesucht, Unternehmen Zugang zu Daten zu vermitteln, die sie für den Markteintritt benötigen. Kann Google verpflichtet werden, Daten mit anderen Unternehmen zu teilen, wie etwa in einem „Daten-für-Alle-Gesetz“ gefordert?²⁷ Praktisch dürfte das außerordentlich schwierig sein. Zum anderen ist die Frage, inwiefern Unternehmen – entgegen dem kartellrechtlichen Verbot des Austausches von sensiblen Daten – Daten *poolen*, also zusammenführen und gemeinsam nutzen dürfen. Das Bundeskartellamt hat in einer Entscheidung zu einer Stahlhandelsplattform eher strenge Kriterien für ein solches Datensharing aufgestellt.²⁸

Viertens wird – angesichts des „siebenjährigen Krieges“ der EU-Kommission gegen Google – geprüft, wie die Kartellrechtsanwendung beschleunigt und vereinfacht werden kann.²⁹ Dazu zählt auch die Frage, inwieweit Beweis-

standards gesenkt werden können. Das Erbe der Laisser-faire-Ökonomen muss mühsam überwunden werden, auch in den Instrumenten und Einstellungen unterhalb der gesetzlichen Ebene.

Fünftens hat das deutsche Facebook-Verfahren die Diskussion eröffnet, wie das Kartellrecht im Zusammenspiel mit anderen Rechtsgebieten anzusehen ist. Überschneidungen mit Verbraucher- und Datenschutzrecht liegen auf der Hand. Das führt zu Abstimmungsbedarf. Eine Schlüsselfrage in der Gesetzgebung ist, ob das Bundeskartellamt künftig auch Befugnisse zur Durchsetzung im Verbraucherrecht erhält. Anders als in fast allen anderen EU-Ländern gibt es in Deutschland bislang kaum behördlichen Verbraucherschutz.³⁰ Gerade für den digitalen Bereich drängt sich auf, dass das Kartellamt als erfahrene Rechtsanwendungsbehörde in diesem Grenzbereich zum Kartellrecht tätig werden sollte.³¹ Das würde allerdings die Grenzen zwischen Kartellrecht und Verbraucherschutz weiter verwischen. Am Horizont könnte sich dann ein umfassender wettbewerblicher Ordnungsrahmen abzeichnen. Das ist für manche eine Hoffnung, für andere, gerade auch für marktliberale Verfechter eines „reinen“ Kartellrechts, aber eine Drohung.

WERTE UND WETTBEWERB

Die Kartellbehörden führen Leuchtturmverfahren, nicht mehr und nicht weniger. Neue Normen werden dies erleichtern, aber die Grundfrage – „Welche Wirtschaftsordnung wollen wir?“ – werden sie nicht lösen.

Das Kartellrecht bietet zur Klärung dieser Frage großartiges Anschauungsmaterial: In den Verfahren werden Geschäftsmodelle analysiert,

²⁵ Vgl. Heike Schweitzer et al., Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, Baden-Baden 2018; Crémer/de Montjoye/Schweitzer (Anm. 8); Digital Competition Expert Panel, Unlocking Digital Competition, London 2019 („Furman-Report“).

²⁶ Vgl. Rupperecht Podszun/Christian Kersting, Eine Wettbewerbsordnung für das digitale Zeitalter, in: Zeitschrift für Rechtspolitik 2/2019, S. 34–38; dies., Modernisierung des Wettbewerbsrechts und Digitalisierung, in: Neue Juristische Online-Zeitschrift 10/2019, S. 321–325.

²⁷ Siehe Andrea Nahles, Digitaler Fortschritt durch ein Daten-für-Alle-Gesetz, Positionspapier, 12.2.2019, www.spd.de/aktuelles/daten-fuer-alle-gesetz.

²⁸ Vgl. BKartA, Fallbericht zur Entscheidung vom 27.2.2018, B5-1/18-001, XOM Metals.

²⁹ Vgl. Rupperecht Podszun, Muss das Kartellrecht schneller werden?, in: WuW 12/2017, S. 577.

³⁰ Seit der 9. GWB-Novelle hat das BKartA erste Befugnisse im Bereich des wirtschaftlichen Verbraucherschutzes gemäß dem Gesetz gegen unlauteren Wettbewerb. Vgl. §§ 32e Abs. 5 und § 90 Abs. 6 GWB; Rupperecht Podszun/Gregor Schmieder, Verbraucherrechtliche Befugnisse des Bundeskartellamts, in: Christian Kersting/Rupperecht Podszun (Hrsg.), Die 9. GWB-Novelle, München 2017, S. 84–113.

³¹ Vgl. Rupperecht Podszun/Christoph Busch/Frauke Henning-Bodewig, Behördliche Durchsetzung des Verbraucherrechts?, Studie im Auftrag des BMWi, Februar 2018, <https://t1p.de/86cb>; dies., Die Durchsetzung des Verbraucherrechts: Das BKartA als UWG-Behörde?, in: Gewerblicher Rechtsschutz und Urheberrecht 10/2018, S. 1004–1011.

Marktkräfte eingeschätzt, wettbewerbliche Wirkungen aufgezeigt, rechtliche Lösungen durchgeprüft. Damit hat das Kartellrecht oft eine Schrittmacherfunktion: Aus einzelnen Fällen, in denen Missstände durchleuchtet werden, erwachsen Regulierungen, die für ganze Branchen gelten. Die jüngst verabschiedete P2B-Verordnung der Europäischen Kommission³² ist dafür das beste Beispiel: Sie statuiert für Bestpreisklauseln, wie in den Fällen der Hotelbuchungsplattformen, oder für die Bevorzugung eigener Angebote, wie im Fall Google Shopping, branchenübergreifend

32 P2B steht für „Plattform to Business“, die Verordnung zielt also auf das Verhältnis von Plattformen zu Unternehmen. Vgl. Christoph Busch, Towards a „New Approach“ for the Platform Ecosystem: A European Standard for Fairness in Platform-to-Business Relations, in: Journal of European Consumer and Market Law 6/2017, S. 227 f.; Rupprecht Podszun, Digitale Fairness durchsetzen!, Gutachten für die Finanzplatz München Initiative, Dezember 2018, <https://t1p.de/7pb6>.

33 Vgl. Rupprecht Podszun, Wettbewerb, Werte und Recht im Zeitalter der Digitalisierung, in: Roman Herzog Institut (Hrsg.), Werte – und was sie uns wert sind, München 2018, S. 207–223.

Transparenzpflichten. Ohne die kartellrechtlichen Verfahren, die stets parallel von Juristen wie Ökonominen geführt werden, hätte es solche Regelungen nicht gegeben.

Das sind aber nur Mosaiksteine, die es zu einem Gesamtbild zusammenzufügen gilt. Dafür sind die Fragen entscheidend, wie eine Wettbewerbsordnung 4.0 aussehen soll und welche Werte in der Wirtschaft gelten sollen.³³ „Ordoliberalismus reloaded“, das ist in etwa der Auftrag, der sich stellt. Da ist sie wieder, die politische Dimension des Kartellrechts. Sie auszufüllen, ist jedoch Sache der Politikerinnen und Politiker. Das Recht kann letztlich nur in Regelwerke gießen, was die Gesellschaft normativ wünscht.

RUPPRECHT PODSZUN

ist Professor an der Heinrich-Heine-Universität Düsseldorf und dort Direktor des Instituts für Kartellrecht. Er bloggt unter www.d-kart.de. ls.podszun@hhu.de



Der Moment, wenn du merkst,
es ist DEIN Zuhause.

#dankegrundgesetz

bpb: „Die Wohnung ist unverletzlich ...“ — Artikel 13
Das Grundgesetz kostenlos bestellen auf bpb.de/danke-grundgesetz

REGULIERUNGSANSÄTZE IN DER DATENÖKONOMIE

Ingrid Schneider

Gemessen an ihrem Marktwert, stehen die fünf „Internetriesen“ Microsoft, Apple, Alphabet (Google), Amazon und Facebook inzwischen unangefochten an der Spitze der weltweit wertvollsten Unternehmen. Google und Facebook sowie viele andere digitale Plattformen bieten ihre Dienste kostenfrei an; ihre Einnahmen generieren sie überwiegend aus dem Verkauf von Werbeanzeigen, die durch die Analyse der Nutzungsdaten und durch die Erstellung von digitalen Profilen zielgruppengerecht dargeboten werden.⁰¹ Fragen der Sammlung, Aggregation, des Zugangs und des Ausschlusses von Daten sind inzwischen stark mit Machtfragen verknüpft, die über bloße Marktmarkt hinausreichen. Die neuen Machtasymmetrien der Datenökonomie rufen daher auch in der Politik Besorgnis hervor. So sagte etwa Bundeskanzlerin Angela Merkel im Januar 2018 beim Weltwirtschaftsgipfel in Davos: „Daten sind der Rohstoff des 21. Jahrhunderts. Die Antwort auf die Frage ‚Wem gehören diese Daten?‘ wird letztendlich darüber entscheiden, ob Demokratie, Partizipation, Souveränität im Digitalen und wirtschaftlicher Erfolg zusammengehen. (...) Wir brauchen eine Soziale Marktwirtschaft 4.0, nicht nur eine Industrie 4.0.“⁰²

Daten als solche sind, jedenfalls in Europa, nicht eigentumsfähig. Sie können aber als Geschäftsgeheimnisse oder urheberrechtlich geschützt werden. Die Rechtsfigur eines Dateneigentums widerspricht dem traditionellen deutschen Zivilrecht, das (sachenrechtliches) Eigentum nur körperlichen, materiellen Gütern zuerkennt.⁰³ Daten dagegen sind immaterielle Güter, sie gleichen einem öffentlichen Gut, zumindest im Hinblick auf den Aspekt der nicht rivalisierenden Nutzung: Sie können in der Regel nahezu unendlich oft von vielen Akteuren gleichzeitig genutzt werden, ohne dass sie sich aufbrauchen; sie unterliegen weder einer Verknappung noch einer Abnutzung. Deshalb kann eine „Übernutzung“ wie bei klassischen Allmendegütern (etwa einer gemeinschaftlich genutzt-

ten Weide) bei Daten nicht geschehen. Bei der Diskussion um Dateneigentum oder *data ownership* geht es daher vor allem um Zugangs- und Verfügungsrechte über Daten.⁰⁴

Im Folgenden werde ich vier Regulierungsformen untersuchen, die Daten als privates Gut, als öffentliches Gut, als Allmendegut und mittels einer Treuhandenschaft verwaltet und bewirtschaftet sehen wollen. Dabei werde ich jeweils der Frage nachgehen, wie die informationelle Selbstbestimmung der Datengebenden gewahrt und ob ein Brückenschlag zwischen regulierter kommerzieller Nutzung und der Nutzbarmachung für das Gemeinwohl ermöglicht werden kann.

DATEN ALS PRIVATES GUT

Idee und Ansatz

Der Informatiker und Internetpionier Jaron Lanier schlägt eine „humanistische Informationsökonomie“ vor, die darauf beruht, die menschliche Herkunft personenbezogener Daten nicht als weniger wertvoll als ihre algorithmische Analyse und Weiterverwertung zu erachten.⁰⁵ Da jede Art von automatisierter Datenanalyse auf zuvor von Menschen erzeugten Daten angewiesen sei, liege genau darin die eigentliche Wertquelle der digitalen Welt. Online-Übersetzungsdienste beispielsweise basierten auf zuvor von Menschen geleisteten Übersetzungen für das maschinelle Lernen. Diese Arbeit tauche jedoch in keiner Unternehmensbilanz auf und würde auch aus der ökonomischen Gesamtrechnung ausgeschlossen. Diese „Entrechtung“ und Entwertung sei nur zu stoppen, wenn die Menschen nicht länger nur als Konsumenten wahrgenommen, sondern zu Akteuren der Datenökonomie, also zu „Prosumenten“ (Hybridform zwischen Produzenten und Konsumenten) würden, so Lanier. Der Faktor Mensch als Urheber von Daten müsse explizit in die ökonomische Wertschöpfungskette aufgenommen und entlohnt werden. Es dürfe

nicht sein, dass eine riesige Anzahl von Menschen über soziale Netzwerke und Suchmaschinen eine enorme Menge wertvoller Informationen produziere, der Löwenanteil des Wertes aber an die Unternehmen gehe, die die Daten sammeln, aggregieren und weiterverarbeiten.

Lanier plädiert daher für ein Mikrozahlungssystem: Jeder aktiv oder passiv generierte Beitrag in einer digitalen Datenbank oder einem Netzwerk soll in Form eines Kleinstbetrages entlohnt werden. Über die Speicherung der Datenherkunft, die Verknüpfung der Daten mit ihrer Urheberin oder ihrem Urheber, solle jeder Zugriff und jede Nutzung der Daten registriert und ein entsprechender Betrag vom Datennutzenden automatisch auf ein digitales Konto des Datengebenden transferiert werden. Die Entscheidung, welche Daten man zu welchem Preis am Markt anbiete, solle jede und jeder für sich selbst festlegen. Der Markt regle Angebot und Nachfrage. Die Überwachung der Regeleinhaltung und die Sanktionierung etwaiger Verstöße könne der Staat übernehmen. Zugleich fordert Lanier eine Abkehr von der Umsonstmentalität. Die Zeit, in der gefordert wurde, im Internet müsse jegliche Information frei verfügbar sein, sei Geschichte.

Die Etablierung eines Marktes für Daten beziehungsweise einer solchen „Pay-per-View-Wirtschaft“ bedeutet, dass Lanier Daten letztlich als privates Gut konzipiert. Das erklärte Ziel ist dabei die Festschreibung eines Hoheitsrechts jeder Person über ihre persönlichen Daten. Er verspricht sich davon mehr Selbstbestimmung und ein Empowerment der Datengebenden sowie einen Abbau von Machtasymmetrien.

Würdigung und Kritik

Lanier sieht im Markt nach wie vor die zentrale Koordinationsinstanz, fordert innerhalb dieses Systems aber eine Beteiligung der Datenur-

heberinnen und -urheber. Ihren Beitrag möchte er allerdings nicht nur ideell wertgeschätzt, sondern auch materiell in die Wertschöpfungskette aufgenommen sehen. Er konzipiert somit eine Art Angebot- und Nachfragemodell für persönliche Daten und suggeriert, die individuellen Nutzerinnen und Nutzer könnten dadurch Marktmacht erlangen.

Insgesamt bleibt Lanier allerdings im Ungefähren. Sollte es jeweils Einzelentscheidungen zur Datenfreigabe geben, erscheint dies nicht zu Ende gedacht. Eine ständige Fall-zu-Fall-Entscheidung über die Datenfreigabe würde rasch zu Überforderung führen: Beim Aufruf einer einzigen Website werden heute unter anderem durch Cookies 50 bis 100 Verbindungen zu Internetdomains von Dritten hergestellt.⁰⁶ Laniers Prosument müsste mit jedem dieser Datenverwerter in Preisverhandlungen treten. Und selbst wenn man die Aushandlung durch ein Daten-Clearinghouse automatisieren würde, indem man seine Präferenzen angibt, mit wem man zu welchem Preis Daten gegen Geld zu teilen bereit wäre, würden dadurch hohe Transaktionskosten entstehen. Zudem ist zweifelhaft, ob die Nutzerinnen und Nutzer tatsächlich *bargaining power* erhalten würden, denn die Asymmetrie der Marktmacht bleibt bestehen – die Verhandlungsmacht der Plattform wäre noch immer wesentlich größer.⁰⁷

Lanier berücksichtigt zudem zu wenig, dass die Wertschöpfung der Daten im Aggregieren und Auswerten der Daten liegt, nicht aber in einem individuellen, einzelnen Datum. Auch in sozialpolitischer Hinsicht ist sein Modell zweifelhaft: Mikrozahlungen könnten gerade finanzschwache Nutzerinnen und Nutzer dazu verleiten, einer unethischen Datennutzung durch Dritte zuzustimmen oder große Anteile ihres täglichen Lebens tracken zu lassen. Datenschutz sollte aber nicht von finanziellen Möglichkeiten abhängen. Überdies werden viele Datengebende den Wert ihrer Daten möglicherweise überschätzen – und die Konsequenzen, die eine Datenfreigabe für sie hat, eher unterschätzen. Berechnungen zufolge würden nur Bruchteile von Centbeträgen für die Preisgabe einzelner Daten fällig. Selbst wenn

⁰¹ Vgl. Wolfie Christl, *Corporate Surveillance in Everyday Life*, Wien 2017, <http://crackedlabs.org>.

⁰² Angela Merkel, Rede beim Jahrestreffen des World Economic Forum, Davos 24.1.2018.

⁰³ Vgl. Johanna Jöns, *Daten als Handelsware*, Hamburg 2016, S. 66.

⁰⁴ Vgl. Wolfgang Kerber/Louisa Specht, *Datenrechte. Eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland–USA*, 2017, www.abida.de/sites/default/files/ABIDA_Gutachten_Datenrechte.pdf.

⁰⁵ Zum Folgenden vgl. Jaron Lanier, *Wem gehört die Zukunft?*, Hamburg 2014; ders., *Wenn Träume erwachsen werden*, Hamburg 2015.

⁰⁶ Vgl. Justin Brookman et al., *Cross-Device Tracking: Measurement and Disclosures*, in: *Proceedings on Privacy Enhancing Technologies* 2/2017, S. 133–148.

⁰⁷ Vgl. Nicolas Agar, *How to be Human in the Digital Economy*, Cambridge 2019, S. 73–79.

man den (Werbeeinnahmen-)Umsatz der Unternehmen auf alle Nutzerinnen und Nutzer umlegte, ergäben sich etwa bei Facebook nur acht Euro pro Jahr, bei Google etwa 150 Euro – abzüglich der Unterhaltskosten für die Plattform.⁰⁸

Es stellen sich weitere offene Fragen zur Operabilität. Dass mit der Abrechnungsinfrastruktur für die Mikrozahlungen ein gigantisches Überwachungsnetzwerk orwellischen Ausmaßes aufgebaut würde, negiert Lanier. Zuletzt stellt sich die Frage, wie er die Aufsichts-, Kontroll- und Sanktionskompetenz, die er dem Staat zuspricht, umgesetzt sehen wollte. Denn sein Modell ist rein zivilrechtlich zwischen Datenverkäufer und Datenkäufer angelegt. Offensichtlich hat Lanier nur demokratische Staaten im Sinn, nicht aber autoritäre oder korrupte, die aus dem Datenmarkt Renten abschöpfen oder ihn zu Hyperüberwachung und Repression nutzen könnten. Auch wenn positiv hervorzuheben ist, dass Lanier den Beitrag der Datenurheber explizit anerkennt, erweist sich sein Datenmarktmodell insgesamt als unzulänglich, würde es doch eine ganze Reihe nicht intendierter Folgeprobleme aufwerfen.

DATEN ALS ÖFFENTLICHES GUT

Idee und Ansatz

Das Gegenmodell zu dem von Lanier propagierten Datenmarkt bildet der Ansatz des Publizisten Evgeny Morozov, der Daten als öffentliches Gut konzipiert sehen will.⁰⁹ Datengetriebene Technologie berge sowohl Gefahren als auch Potenziale für die Gesellschaft. Menschliches Verhalten in Echtzeit zu erfassen und Profile zu speichern, könne richtig eingesetzt zu effizienterem Ressourceneinsatz, Nachhaltigkeit und entsprechenden Innovationen beitragen. Morozovs Anliegen ist daher keine Technologiekritik, sondern eine politökonomische Kritik des „datenorientierten Kapitalismus“, der auf „Datenextraktivismus“ basiere.

Morozov plädiert daher dafür, die bislang von Unternehmen gesammelten Daten zu vergesellschaften und als Teil der öffentlichen Da-

seinsfürsorge zu verstehen: Die Daten müssten von der marktwirtschaftlichen Dynamik abgekoppelt, die gewerbliche Datensammlung eingedämmt werden. Staatlich reguliert könnten Teile der in den digitalen Profilen gespeicherten Daten in anonymisierter Form von öffentlichen Stellen (Städten, Gemeinden, städtischen Versorgungsunternehmen) genutzt werden, um Dienstleistungsangebote wie etwa die Taktung des öffentlichen Nahverkehrs effektiver an den Bedarf der Bevölkerung anzupassen. Auch andere Dienstleistungen in Verkehr, Bildung, Energieversorgung und Gesundheit könnten auf diese Weise effizienter, innovativer und nützlicher gestaltet werden. Private Unternehmen könnten weiterhin personalisierte Dienstleistungen anbieten, sofern sie für die Datennutzung bezahlten. Die dafür notwendigen Datenbanken könnten auf kommunaler, nationaler oder sogar übernationaler Ebene angesiedelt sein: „All of the nation's data, for example, could accrue to a national data fund, co-owned by all citizens (or, in the case of a pan-European fund, by Europeans). Whoever wants to build new services on top of that data would need to do so in a competitive, heavily regulated environment while paying a corresponding share of their profits for using it.“¹⁰

Der breitere Zugang zu personenbezogenen, aber anonymisierten Daten könne auch das gegenwärtige Problem der Monopolstellung einiger weniger großer Unternehmen lösen, denn innovative Start-ups könnten durch Zugang zu den Daten konkurrenzfähige Alternativen aufbauen. Morozovs Vision ist also eine öffentliche, gemeinwohlorientierte Nutzung von Daten mithilfe staatlicher Regularien zur Koordination des Datenzugriffs und zum Schutz vor Missbrauch. Finanziert werden solle ein solches System zudem durch Steuern beziehungsweise eine Pflichtabgabe aller Bürgerinnen und Bürger. Werbung und die kommerzielle Datensammlung solle jedenfalls nicht länger das indirekte Zahlungsmittel für die Nutzung solcher Dienste sein.

Würdigung und Kritik

Bei Morozovs Modell von Daten als öffentlichem Gut handelt es sich letztlich um eine Verstaatlichung von Daten. Unklar bleibt, ob er diese

⁰⁸ Vgl. Jan Schwenkenbecher, Eine Mail-Adresse bringt 0,75 Cent, in: *Süddeutsche Zeitung*, 2.11.2018, S. 16.

⁰⁹ Zum Folgenden vgl. Evgeny Morozov, Eine humane Gesellschaft durch digitale Technologien?, Essen 2015, S. 29; ders., „Ich habe doch nichts zu verbergen“, in: APuZ 11–12/2015, S. 3–7; ders., Digitale Abhängigkeit. Die Menschen müssen die Daten der Internet-Giganten zurückerobern, in: *Süddeutsche Zeitung*, 19.1.2018.

¹⁰ Evgeny Morozov, To Tackle Google's Power, Regulators Have to Go After Its Ownership of Data, in: *The Guardian*, 2.7.2017.

Vergesellschaftung auf kommunaler, regionaler, nationaler oder gar supranationaler Ebene angesiedelt sehen will – oder eventuell sektoral organisiert, etwa für Energie- oder Verkehrsdaten. Positiv wäre sicherlich, dass kleinen und mittleren Unternehmen dadurch gleiche Zugangschancen eröffnet würden. Eine zentralisierte öffentliche Datenverwaltung kann zudem sozialverträgliche und nachhaltig orientierte Forschung und Innovation erleichtern.

Wie aber wäre mit Mehrfachnutzungen von Daten umzugehen? Denn aus jeder Datenanalytik erwächst gewissermaßen eine neue „Datenschicht“ – soll diese ebenfalls in den staatlichen Datenpool eingebracht oder darf diese privatwirtschaftlich genutzt werden? Morozovs Vorschlag impliziert unausgesprochen ein Zentralisierungsmodell, das real durch eine zentrale Datenbank oder virtuell durch Verknüpfung verschiedener dezentraler Datenbanken ausgestaltet werden kann. In beiden Fällen stellt sich die Frage, ob die Bürgerinnen und Bürger der Datenerfassung überhaupt noch zustimmen dürften. Wie wäre es mit der Freiwilligkeit und der Wahrung informationeller Selbstbestimmung bestellt? Ist jeweils eine Zweckbindung gegeben, oder sollten Bürgerinnen und Bürger breit einwilligen, ohne über die vielfältigen Nutzungszwecke aufgeklärt zu werden? Dies wäre ein erheblicher Rückschritt im Datenschutz. Letztlich wäre damit eine Bringschuld der Bürgerinnen und Bürger sowie eine Sozialpflichtigkeit ihrer Daten festgeschrieben. Gewisse Abhilfe könnte durch eine Pseudonymisierung und Verschlüsselung der Daten geschaffen werden. Doch sollte die staatliche Datensammlung wirklich auf Online-Dienstleistungen ausgeweitet werden?

Zudem besteht die Gefahr des Missbrauchs durch staatliche Überwachung und Repression bis hin zum völligen Verlust der Privatsphäre. Schließlich stellt sich auch hier die Frage der Regulation: Durch welchen Staat oder staatliche Agentur sollte diese erfolgen? Kann der Nationalstaat hier überhaupt noch agieren, wenn es um transnationale Datenflüsse geht? Und wer entscheidet über die Datenfreigabe für wen, nach welchen demokratisch festgelegten und gegebenenfalls gerichtlich anfechtbaren Kriterien? Welche Sanktionsmöglichkeiten sollte es bei Missbrauch geben? Und soll die Verstaatlichung der Daten erst ab einem bestimmten Zeitpunkt erfolgen oder rückwirkend? Wird damit in Eigen-

tumsbestände von Unternehmen eingegriffen, und wie weit ist dies verfassungsrechtlich zulässig? Auf alle diese Fragen gibt Morozov in seinen Schriften keine Auskunft.

DATEN ALS ALLMENDE

Idee und Ansatz

Das dritte hier vorgestellte Modell, wie Daten alternativ bewirtschaftet und genutzt werden könnten, ist an die Allmendekonzeption von Elinor Ostrom angelehnt. Die Politikwissenschaftlerin Ostrom, die für die Erforschung von Gemeingütern 2009 als bisher einzige Frau den Nobelpreis für Wirtschaftswissenschaften erhielt, geht es um eine Perspektive „jenseits von Staat und Markt“.¹¹ Sie untersuchte, wie sich natürliche Ressourcen wie Wälder und Weiden nachhaltig bewirtschaften und im Sinne des Gemeinwohls nutzen lassen. Dabei interessierte sie sich für Handlungsformen, wie sich Gruppen organisieren können, um langfristig gemeinsame Vorteile zu realisieren und negative Folgen individueller Nutzenmaximierung zu verhindern.

Ostrom entdeckte solche Formen von Selbstorganisation, Entscheidungsfindung und Selbstverwaltung in gemeinschaftlich ausgehandelten Zugangs- und Nutzungsregeln, mittels derer sich Interessenkonflikte entschärfen lassen. Sie widersprach damit der gängigen Annahme, dass Allmendeprobleme nur durch eine Privatisierung von Ressourcen oder durch Kontrolle eines Zentralstaats gelöst werden könnten, und wies nach, dass sich gemeinschaftlich genutzte Güter durch von unten organisierte und institutionalisierte lokale Kooperation der Betroffenen in angemessener, fairer und nachhaltiger Form bereitstellen und aneignen lassen. Aus der Betrachtung von gelungenen und gescheiterten Lösungen leitete sie schließlich die folgenden acht „Design-Prinzipien“ für eine erfolgreiche Allmendenführung ab.

Abgrenzbarkeit: Es gibt eindeutige und akzeptierte Grenzen zwischen legitimen Nutzern und nicht Nutzungsberechtigten sowie zwischen einer bestimmten Gemeinressource und ihrer Umwelt.

¹¹ Zum Folgenden vgl. Elinor Ostrom, *Die Verfassung der Allmende. Jenseits von Staat und Markt*, Tübingen 1999; dies./Silke Helfrich, *Was mehr wird, wenn wir teilen*, München 2011; Volker Stollorz, Elinor Ostrom und die Wiederentdeckung der Allmende, in: APuZ 28–30/2011, S. 3–8.

Kongruenz mit lokalen Bedingungen: Die Regeln für die Aneignung und Bereitstellung einer Ressource entsprechen den örtlichen und kulturellen Bedingungen. Die Verteilung der Kosten erfolgt proportional zur Verteilung des Nutzens.

Gemeinschaftliche Entscheidungen: Die an der Allmendenutzung Beteiligten können die Nutzungsregeln mitgestalten.

Monitoring: Es gibt ausreichend Kontrolle über die Nutzung und den Allgemeinzustand der Allmenderessource, um Regelverstößen vorbeugen zu können. Personen, die mit der Überwachung betraut sind, sind rechenschaftspflichtig.

Abgestufte Sanktionen: Verhängte Sanktionen sollen in einem vernünftigen Verhältnis zum verursachten Problem stehen. Die Bestrafung von Regelverletzungen beginnt auf niedrigem Niveau und verschärft sich, wenn Nutzer eine Regel mehrfach verletzen.

Konfliktlösungsmechanismen: Festgelegte lokale Arenen sollen helfen, Konflikte zwischen Nutzern sowie zwischen Nutzern und Behörden möglichst rasch, günstig und direkt beizulegen.

Anerkennung von Rechten: Die Regierung räumt Nutzern ein Mindestmaß an Rechten ein, sich eigene Regeln zu setzen.

Eingebettete und verschachtelte Institutionen: Ist eine Gemeinressource eng mit einem sie umgebenden, großen Ressourcensystem verbunden, werden die Governance-Strukturen auf mehreren, ineinandergreifenden Ebenen miteinander verschachtelt (*polycentric governance*).

Ostrom beschäftigte sich zwar vor allem mit natürlichen, ökologischer Nachhaltigkeit bedürftenden Ressourcen beziehungsweise Allmendegütern. Gleichwohl können aber zumindest einige ihrer Prinzipien auch auf die Verwaltung und Bewirtschaftung von Daten angewandt werden. Als praktische Anschauungsbeispiele bestehender digitaler Allmenden dienen insbesondere Open-Source-Software, Creative-Commons-Lizenzen und digitale Commons wie etwa die Online-Enzyklopädie Wikipedia oder das Online-Kartendienst- und Navigationssystem Open Street Map.

Würdigung und Kritik

Im Gegensatz zum Marktmodell von Lanier und dem Staatsmodell von Morozov verortet das Modell der Allmende Daten als Gemeingut. Zentraler Akteur ist damit die Gemeinschaft. Damit wird ein Modell nahegelegt, wie es etwa durch Kooperativen und Genossenschaften bei mate-

riellen Gütern bereits seit Langem etabliert ist. Positiv an diesem Modell erscheint zunächst die Transparenz über die Datennutzung und die potenzielle Beteiligung aller Datengebenden über die Festlegung von Regeln, mittels derer die Daten – und die Erträge daraus – blieben zumindest anteilig an ihre Erzeuger beziehungsweise deren digitale Identitäten gekoppelt. Die Gemeinschaftsmitglieder könnten Ansprüche gegenüber den Datenverwertern kollektiv geltend machen, was ihnen größere Verhandlungsmacht sichern würde. Auch die Verwerter könnten gegebenenfalls Teil der Gemeinschaft sein – oder aber als externe Dienstleister für die Gemeinschaft auftreten. Da alle Kompetenzen von der Entscheidung über die Datenaufnahme bis zur Festlegung legitimer Verwendungszwecke idealtypischerweise in der Hand der Gemeinschaft liegen, wäre die Kontrolle der Datengebenden und ihre wirkungsvolle Selbst- und Mitbestimmung in der Datenökonomie gesichert.

Fragen stellen sich allerdings dahingehend, inwieweit Ostroms Modell von natürlichen Ressourcen auf immaterielle, nicht rivalisierende Güter wie Daten übertragen werden kann. Schon das erste Designprinzip Ostroms, die Abgrenzbarkeit, ist bei Daten schwer zu realisieren. Wer gehört zur Gemeinschaft, wer darf ihr beitreten und wer nicht? Sind die Datengebenden auch Datennutzende oder gehören sie zu getrennten Kategorien? Wie soll das gemeinschaftliche Handeln zum gemeinwohlverträglichen und nachhaltigen Nutzen der Daten praktisch umgesetzt werden? Und welcher Staat autorisiert die Gemeinschaft? Die bereits bei Lanier und Morozov angesprochenen Probleme von Staatlichkeit und Territorialität bei transnationalen Datenflüssen gelten auch hier. Zudem sind bei großen Gemeinschaften ein Repräsentationsmodell und die Delegation von Entscheidungen nötig. Wie diese demokratisch ausgestaltet werden sollten, bleibt offen.

DATEN-TREUHANDSCHAFT

Idee und Ansatz

Das vierte Modell, das in der Datenökonomie Anwendung finden könnte, ist das einer Treuhand-schaft. Ein Treuhandverhältnis liegt vor, wenn vertraglich oder kraft Gesetzes die Ausübung oder Verwaltung bestimmter Rechte (eines Treugutes) vom Treugeber „zu treuen Händen“ an den

Treunehmer (Treuhänder) übertragen wird. Hier lässt sich an Überlegungen des Wissenschaftsforschers David E. Winickoff anknüpfen, der in Bezug auf genomische Biobanken – bei denen sensible Datenschutzfragen mit der wissenschaftlichen Nutzung der Daten in Einklang zu bringen sind – ein Treuhandmodell entwickelt und hierfür als Rechtsform eine gemeinnützige Einrichtung (*charitable trust*) vorgeschlagen hat.¹²

Winickoff setzte sich intensiv mit der Frage auseinander, wie Verfügungsrechte an gespendeten Biomaterialien (wie Gewebe, Blut, DNA) und an dazugehörigen Daten (aus Patientenakten, Gen- und Analysedaten) geregelt werden sollten. Dabei ging es insbesondere um Zugangsfragen, ethische Aspekte der informierten Zustimmung zu Forschungen sowie um mögliche Gewinne und deren Verteilung. Er kam zu dem Schluss, dass durch den Aufbau einer treuhänderischen Einrichtung eine angemessene Regulierung von Biobanken erreicht werden könne, um den Schutz der Interessen der Daten- und Materialsponder zu garantieren. Spender könnten ihre Verfügungsinteressen über das Biomaterial und die Daten an diese Einrichtung übertragen, die damit wiederum die treuhänderischen Pflichten zur Aufbewahrung und Nutzung übernehme. Gemeinnützigkeit weise dabei als Organisationsform eine Reihe von ethischen, rechtlichen und wissenschaftlichen Vorteilen auf und sichere Vertrauen und langfristige Beteiligung. Durch die beratende Beteiligung der Spendergruppe in Gremien und die Einrichtung einer Ethikkommission solle die Wahrung der Spenderinteressen zusätzlich gesichert werden. Das Treuhandmodell könne Altruismus, gute Governance und öffentlichen Nutzen für das Gemeinwohl miteinander vereinbaren und damit sowohl strikte Regeln zum Datenschutz implementieren wie auch den wissenschaftlichen Wert der Biobank sicherstellen.

Dass das Modell einer Treuhanderschaft auch auf die Verwaltung und Bewirtschaftung von Daten übertragbar ist, zeigen Zertifizierungsprozesse von deutschen Datenschutzbehörden zum Spenderschutz durch Datentreuhänder-

schaft: Demnach müsse der Treuhänder rechtlich und finanziell unabhängig sowie weisungsungebunden sein. Er müsse der Schweigepflicht und dem Forschungsgeheimnis unterliegen und dürfe keinesfalls von der wirtschaftlichen Wertschöpfungskette abhängig sein. Eine Datentreuhand könne nur dann unabhängig agieren, wenn sie ausschließlich gemeinwohlorientiert orientiert sei.¹³ Auch in einem Report des britischen Unterhauses wurde jüngst für die Errichtung von „Data Trusts“ im Rahmen eines „Center for Data Ethics & Innovation“ plädiert. Regierung und Industrie sollten ein Programm zur Entwicklung von Datentreuhändern aufbauen, durch die Dateninhaber und Datennutzer auf „faire, sichere und gerechte Weise“ Daten austauschen könnten. Durch eine derartige Regulierung solle gewährleistet werden, dass die Stimmen der interessierten Parteien vertreten sind, und der Wert, der aus diesen Daten abgeleitet werden kann, gerecht aufgeteilt wird.¹⁴

Würdigung und Kritik

Das Governance-Modell der gemeinnützigen Datentreuhanderschaft basiert auf der Vorstellung einer unabhängigen dritten Instanz, die Hoheitsrechte über Daten ausübt, sowie von delegierter Kontrolle der Datengebenden, die gleichwohl mit Partizipationselementen ausgestattet sind. Positiv an der Übertragung von Vollmachten auf einen unabhängigen Treuhänder ist die Entlastung der Datengebenden, die aber durch ein Widerrufsrecht dennoch gewisse Kontrolle über ihre Daten behalten. In gewissem Umfang wäre somit eine Zweckbindung der Daten gesichert, und durch das Transparenzgebot über die Nutzung durch Dritte verbliebe den Datengebenden ein Entscheidungsspielraum darüber, welche Unternehmen zu welchen Zwecken auf welche persönlichen Daten zugreifen dürfen. Dies würde den Stellenwert des Datenschutzes deutlich erhöhen.

Auch die Repräsentations- und Partizipationsmöglichkeiten der Datengebenden über Beiräte sind positiv zu vermerken. Allerdings bleibt wie bei den anderen Modellen offen, wel-

12 Zum Folgenden vgl. David E. Winickoff/Richard N. Winickoff, *The Charitable Trust as a Model for Genomic Biobanks*, in: *New England Journal of Medicine* 12/2003, S. 1180–1184; David E. Winickoff/Larissa B. Neumann, *Towards a Social Contract for Genomics: Property and the Public in the „Biotrust“ Model*, in: *Genomics, Society and Policy* 3/2005, S. 8–21.

13 Vgl. Wolfgang Zimmermann, *Spenderschutz durch Datentreuhanderschaft*, Beitrag zur Tagung „Die datenschutzgerechte Auditierung von Biobanken“, Kiel 4. 7. 2008, www.datenschutzzentrum.de/projekte/bdc-audit.

14 Vgl. UK House of Commons Science and Technology Committee, *Algorithms in Decision-Making*, HC 351, 23.5.2018, S. 15f.

che staatliche Stelle genau den Treuhänder autorisieren würde. Ebenso wäre zu definieren, auf welcher sektoralen oder verwaltungspolitischen Ebene die Treuhand angesiedelt werden soll. Schließlich bliebe zu klären, wie sich eine Beteiligung und Teilhabe der Datengebenden demokratisch und gegebenenfalls transnational realisieren ließe. Weitere wichtige Fragen münden schließlich in die alte Frage „Quis custodiet ipsos custodes?“ – „Wer aber überwacht die Wächter?“: Wie kann der Treuhänder effektiv kontrolliert und rechenschaftspflichtig werden, sodass dieser keine partikularen Eigeninteressen verfolgt, in Interessenkonflikte gerät und damit seine Vertrauenswürdigkeit gefährdet? Wie kann die Unabhängigkeit des Treuhänders gegenüber staatlichen oder ökonomischen Instanzen langfristig gesichert werden? Und wie kann die Gemeinwohlorientierung der Datennutzung gewährleistet werden?

FAZIT

Die vier vorgestellten politökonomischen Regulierungsmodelle für die Datenökonomie liefern spannende konzeptionelle Ideen, bisher ist aber keines so ausgereift, dass es bereits unmittelbar anwendbare Lösungen bereitstellt. Als Alternativen zu den bisherigen Praktiken und Geschäftsmodellen der Plattformökonomien und deren inhärenten Machtasymmetrien sind sie allerdings durchaus bedenkenswert.

Insgesamt sind die vier Governance-Modelle eher als Idealtypen oder regulative Ideen zu verstehen, nicht als „reine“ Formen. In der Wirklichkeit sind Mischformen denkbar, sowohl als Hybridformen zwischen privaten und öffentlichen Gütern oder etwa zwischen Allmendegut und Treuhanderschaft. Diese bedürfen weiterer Diskussion und Konkretisierung. Es sind klare und nachvollziehbare Regeln für die Sammlung, den Zugriff und die Verwendung von Daten nötig, dies erfordert aber kein Eigentumsrecht an Daten.¹⁵ Wichtig ist ein fairer Interessenausgleich zwischen Datengebenden und Datenverwerten-

den. Hierzu ist insbesondere die Vertretung der schwachen Interessen der individuellen Datengebenden, deren Organisation und Repräsentation schwerlich umzusetzen ist, gegenüber machtkräftigen Verwertungsinteressen vonnöten. Solche Interessen könnten von Verbraucherschutzorganisationen und Datenschutzbehörden wahrgenommen werden, wenn sie mit entsprechenden Ressourcen und Mandaten ausgestattet würden.

Auch die Vertretung der normativen Ansprüche an einen ethischen, fairen und gerechten Umgang mit den Daten und eine Orientierung der Datenverwertung an einer nachhaltigen, sozial- und umweltverträglichen, insgesamt menschenwürdigen Innovation statt ausschließlicher Profitorientierung ist eine wichtige Aufgabe. Diese kann nur mit starker staatlicher Regulation und der Einbindung einer lebendigen und pluralen Zivilgesellschaft erreicht werden und sollte daher nicht allein den Marktkräften und der Selbstregulierung von Unternehmen überlassen werden.

Die Komplexität der Datenaggregation und -analyse wird mit der Ausbreitung des Internets der Dinge, der Weiterentwicklung der künstlichen Intelligenz und weiteren Digitalisierungsschüben noch zunehmen. Sowohl eine Zentralisierung der Datenhaltung (angelegt bei Morozov und Winickoff) als auch eine Dezentralisierung (inhärent bei Ostrom) hätte jeweils Vor- und Nachteile, die von Fall zu Fall abzuwägen sind. Ebenso bedürfen die Finanzierungsaspekte bei den vorgestellten Datenmodellen weiterer Ausarbeitung. Zu erinnern ist zudem an die janusköpfige Rolle des Staates, der ein Garant der Datenverwendung für Gemeinwohl und Gemeinsinn sein kann, sich unter anderen Umständen aber auch in einen „Big Brother“ verwandeln könnte. Der Verlust der Steuerungskapazität des Nationalstaats aufgrund der transnationalen Datenflüsse sollte zur Entwicklung supranationaler Lösungsstrategien auffordern. Die Europäische Union wird hierbei eine wichtige Gestaltungsmacht¹⁶ für eine Regulierung der Datenökonomien bleiben.

¹⁵ Vgl. Max-Planck-Institut für Innovation und Wettbewerb, Argumente gegen ein „Dateneigentum“, 1.8.2017, www.ip.mpg.de/fileadmin/ipmpg/content/forschung/Argumentarium_Dateneigentum_de.pdf.

¹⁶ Vgl. Ingrid Schneider, Bringing the State Back in: Big Data-Based Capitalism, Disruption, and Novel Regulatory Approaches in Europe, in: dies. et al. (Hrsg.), *The Politics of Big Data: Big Data, Big Brother?*, New York 2017, S. 129–175.

INGRID SCHNEIDER

ist Professorin für Politikwissenschaft an der Universität Hamburg, dort ist sie am Fachbereich Informatik im Arbeitsbereich „Ethik in der Informationstechnologie“ tätig.

ingrid.schneider@uni-hamburg.de

MICROTARGETING

Persönliche Daten als politische Währung

Wolfe Christl

Spätestens seit 2016, mit der Wahl Donald Trumps zum US-Präsidenten, dem Brexit-Referendum sowie den Datenskandalen um Facebook und Cambridge Analytica, tobt eine globale Debatte über digitale Kommunikation und Demokratie. Die einst mit dem Internet verbundenen emanzipatorischen Hoffnungen sind in den Hintergrund getreten. Kaum ein Wahlkampf, bei dem nicht über die digitale Verbreitung von Falschmeldungen oder Hetze diskutiert oder gar versteckte Manipulation vermutet wird. Auch kommerzieller Datenmissbrauch und die Macht der Tech-Plattformen sind in den Fokus gerückt.

Parlamente in aller Welt haben Untersuchungen angestoßen. Ironischerweise war es ausgerechnet der Einsatz von Daten in politischen Kampagnen, der die Debatte über unsere digitale Infrastruktur erst ausgelöst hat. Es geht dabei unter anderem um datengetriebenes „Microtargeting“ – also um Praktiken, bei denen kleine Gruppen auf Basis von Datenanalysen mit fein abgestimmter Kommunikation politisch beeinflusst werden sollen.⁰¹ Parteien, politische Kampagnen und andere Lobbys nutzen heute umfassende Daten über die Bevölkerung, insbesondere im Online-Bereich. Wie funktioniert Microtargeting? Welche Rolle spielen Facebook und die datenbasierte Klick-Ökonomie? Und was bedeutet das für Gesellschaft und Demokratie?

CAMBRIDGE ANALYTICA UND DIE TRUMP-WAHLKAMPAGNE

Es ist kein Wunder, dass die Beteiligung der Datenfirma Cambridge Analytica bei den Kampagnen für den Brexit und die Wahl Trumps Besorgnis erregt hat. Das Unternehmen hat umfassende Datenbanken über ganze Bevölkerungen zusammengestellt, mit Tausenden Merkmalen pro Person. Mit Hilfe eines Online-Quiz

wurde auf Profildaten von 87 Millionen Facebook-NutzerInnen zugegriffen und diese mit Informationen aus Wahlregistern und von privaten Datenhandelskonzernen verknüpft.⁰² Dazu war Cambridge Analytica Teil eines undurchsichtigen Firmennetzwerks, das sowohl für Regierungen und militärische Informationsoperationen in Afghanistan als auch für zwielichtige Wahlkampagnen rund um den Globus gearbeitet hat – etwa in den Philippinen, Indien, Pakistan und Kenia.⁰³

Die Trump-Kampagne hat im letzten Monat vor der Präsidentschaftswahl fast eine Million US-Dollar täglich für Online-Werbung ausgegeben, mit einem Fokus auf wenige Bundesstaaten.⁰⁴ Eigenen Angaben zufolge wurden dabei Listen von WählerInnen mit bestimmten Merkmalen an Facebook geschickt. Die Plattform hat die entsprechenden NutzerInnen identifiziert und als adressierbare Zielgruppen zur Verfügung gestellt. Darüber hinaus hat Facebook nach Personen mit ähnlichen Merkmalen gesucht. Damit konnten viele kleine Gruppen mit angepassten Inhalten versorgt werden – zum Teil auch, um sie zu verunsichern und von der Wahl abzuhalten.⁰⁵ Botschaften, Formulierungen und Gestaltung wurden dabei laufend getestet und vermessen, um die effektivsten Kombinationen zu finden. Dazu wurden täglich bis zu 100 000 unterschiedliche Varianten von digitalen Werbeanzeigen eingesetzt.⁰⁶

Welche Rolle die Daten- und Analysekapazitäten von Cambridge Analytica dabei genau gespielt haben, ist nach wie vor nicht geklärt. Die Firma hat sich aggressiv selbst vermarktet, die Effektivität ihrer „psychometrischen“ Datenanalysen wird allerdings infrage gestellt.⁰⁷ Generell sind die Aussagen von Beteiligten wegen ihrer Eigeninteressen mit Vorsicht zu genießen.⁰⁸ Medienberichten zufolge hat Facebook die Trump-Kampagne aber auch in internen Dokumenten als Musterbeispiel für eine „innovative“ Nutzung

der Plattform dargestellt und dabei die permanenten Tests an ahnungslosen NutzerInnen hervorgehoben. Trump hat laut Facebook in den Monaten vor der Wahl 44 Millionen US-Dollar investiert und dabei in Summe 5,9 Millionen Varianten von Inhalten getestet, Clinton hingegen „nur“ 66 000 Varianten.⁰⁹

Ist Microtargeting also für den Wahlsieg von Trump verantwortlich? Allein sicher nicht. Aber hat es eine Rolle gespielt? Welche Wirkung haben derartige Praktiken? Die Antwort ist: Wir wissen es nicht genau. Ein kürzlich veröffentlichter Überblick zum Forschungsstand diagnostiziert „fehlende Transparenz und viele offene Fragen“.¹⁰ Klar ist: Es ist ein riesiges Geschäft. 2018 hat Facebook mit der selektiven Einblendung von Inhalten 55 Milliarden US-Dollar eingenommen, Google gar 113 Milliarden Dollar.¹¹ Mit politischer Werbung hat Facebook in den USA allein seit Mai 2018 über 550 Millionen Dollar erwirtschaftet.¹² In Großbritannien ist der Anteil, den

politische Kampagnen für digitale Werbung ausgeben, von 0,3 Prozent im Jahr 2011 auf 43 Prozent im Jahr 2017 gestiegen.¹³

Auch wenn Parteien in Europa betonen, Datenschutz zu respektieren, machen auch sie sich vielfach eine Infrastruktur zunutze, die letztlich auf permanenter Echtzeit-Überwachung großer Teile der Bevölkerung beruht. Digitales Marketing basiert auf komplexen Mechaniken, die sowohl aus der Makro- wie aus der Mikro-perspektive betrachtet werden müssen. So kann Online-Targeting im Einzelfall ungenau sein und große Streuverluste in Kauf nehmen – aber in Summe trotzdem Verhalten verändern. Meist sind nicht Einzelne das Ziel, sondern Gruppen mit bestimmten Eigenschaften. Basis ist trotzdem die flächendeckende Erfassung und Verknüpfung von Daten auf individueller Ebene. Um zu verstehen, wie Online-Targeting eingesetzt werden kann, ist es notwendig, die Funktionsweise der digitalen Klick-Ökonomie genauer zu betrachten.

BEEINFLUSSUNGSMASCHINE KLICK-ÖKONOMIE

Seit etwas mehr als zehn Jahren werden Daten zur individuellen Adressierung von Online-Werbung eingesetzt.¹⁴ Wenn wir heute eine Website besuchen oder eine App nutzen, wird unser Profil im Hintergrund innerhalb von Millisekunden an den Höchstbietenden versteigert. Wer die Auktion gewinnt, darf eine Botschaft einblenden. Gleichzeitig werden bei jedem Klick Dutzende bis Hunderte Drittfirmen informiert.¹⁵ Diese ergänzen damit ihre digitalen Profile und vermessen, wie wir auf die eingeblendeten Botschaften reagieren. Bezahlt wird meist nicht pro Einblendung, sondern nur, wenn im Anschluss bestimmte Verhaltensweisen zu beobachten sind.¹⁶ Das definierte Ziel kann etwa der Klick auf einen Link sein,

01 Vgl. Frederik J.Z. Borgesius et al., Online Political Microtargeting: Promises and Threats for Democracy, in: Utrecht Law Review 1/2018, S. 82–96.

02 Vgl. Jeff Chester/Kathryn C. Montgomery, The Role of Digital Marketing in Political Campaigns, in: Internet Policy Review 4/2017, <https://policyreview.info/archives/2017/issue-4>.

03 Vgl. House of Commons/Digital, Culture, Media and Sport Committee, Disinformation and „Fake News“: Interim Report, London 2018, S. 17, S. 53 ff., S. 298.

04 Vgl. Donald Trump and Hillary Clinton's Final Campaign Spending Revealed, 9.12.2016, www.theguardian.com/us-news/2016/dec/09/trump-and-clintons-final-campaign-spending-revealed.

05 Vgl. Joshua Green/Sasha Issenberg, Inside the Trump Bunker, With Days to Go, 27.10.2016, www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go.

06 Vgl. Lois Beckett, Trump Digital Director Says Facebook Helped Win the White House, 9.10.2017, www.theguardian.com/technology/2017/oct/08/trump-digital-director-brad-parscale-facebook-advertising.

07 Vgl. Dave Karpf, Will the Real Psychometric Targeters Please Stand Up?, 1.2.2017, <https://civichall.org/civicist/will-the-real-psychometric-targeters-please-stand-up>.

08 Vgl. Andreas Jungherr, Einsatz digitaler Technologie im Wahlkampf, in: Harald Gapski et al. (Hrsg.), Medienkompetenz, Bonn 2017, S. 92–101.

09 Vgl. Ryan Mac/Charlie Warzel, Congratulations, Mr. President: Zuckerberg Secretly Called Trump After The Election, 19.7.2018, www.buzzfeednews.com/article/ryanmac/congratulations-zuckerberg-call-trump-election-2016.

10 Vgl. Landesanstalt für Medien NRW, Forschungsstand: Microtargeting in Deutschland und Europa, Düsseldorf 2019.

11 Vgl. Mozilla, Internet Health Report v.1.0, 2018, S. 66 f., <https://internethealthreport.org/2018>.

12 Vgl. Facebook, Werbebericht, www.facebook.com/ads/archive/report, Zugriff am 28.4.2019.

13 Vgl. UK Electoral Commission, Digital Campaigning. Increasing Transparency for Voters, Juni 2018, S. 4, <https://t1p.de/bqgy>.

14 Vgl. Wolfie Christl/Sarah Spiekermann, Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy, Wien 2016, S. 118.

15 Vgl. Wolfie Christl, Corporate Surveillance in Everyday Life, Juni 2017, S. 44 ff., https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf.

16 Vgl. z.B. Yu (Jeffrey) Hu/Jiwoong Shin/Zhulei Tang, Incentive Problems in Performance-Based Online Advertising Pricing, in: Management Science 7/2016, S. 2022–2038.

das Ansehen eines Videos, eine Registrierung, ein Kauf oder Anderes. Wird dieses Ziel erreicht und die adressierte Person verhält sich wie geplant – klickt also zum Beispiel auf einen Link – spricht man von einer „Konversion“ (also einer „Bekehrung“). Viele Anbieter versuchen darum, mit Daten über unseren Alltag möglichst gut vorherzusagen, wie wir uns künftig verhalten werden, und verkaufen dieses Wissen unzählige Male pro Sekunde. Die Ökonomin Shoshana Zuboff hat für diesen Hochfrequenzhandel mit menschlichem Verhalten den Begriff „Überwachungskapitalismus“ etabliert.¹⁷

Unsere Kommunikationsinfrastruktur ist heute auf vielen Ebenen von dieser Logik geprägt. Nicht nur soziale Beziehungen, sondern auch mediale Inhalte und öffentliche Debatten werden immer mehr von digitalen Umgebungen geformt, die auf die Maximierung von Klicks und Interaktionen sowie auf die Verwertbarkeit von Verhalten hin optimiert sind. Dabei ist die Klick-Ökonomie stark von Betrug geprägt: Stimmen aus der Industrie schätzen, dass ein Viertel der Klicks nicht von realen Menschen stammen und Werbetreibenden dadurch ein Schaden von 20 bis 50 Milliarden US-Dollar pro Jahr entsteht.¹⁸ Außerdem werden NutzerInnen gern mit Anzeigen auf Websites mit qualitativ fragwürdigen Inhalten gelockt, die wiederum Werbeanzeigen enthalten und dabei mehr einbringen als die Anzeigen, mit denen sie dorthin gelockt wurden – eine Art Pyramidenspiel.¹⁹ Auch durch politische Angstmache lässt sich mit Online-Werbung Geld verdienen: Vieles deutet etwa darauf hin, dass obskure Websites im US-Wahlkampf 2016 aus rein ökonomischen Motiven irreführende Informationen verbreitet haben, weil diese einfach viel geklickt werden.²⁰ Natürlich nutzen auch traditionelle

Boulevardmedien diese Dynamiken. Ein österreichischer Chefredakteur hat bezüglich Klick-Maximierung offen über das symbiotische Verhältnis mit einer politischen Partei gesprochen.²¹

Im Unterschied zu früher kann heute aber nicht nur das Zielpublikum einer bestimmten Zeitung oder einer TV-Sendung angesprochen werden. Es können quer durch die Bevölkerung Menschen mit bestimmten Eigenschaften gefunden und adressiert werden – durch die flächendeckende Erfassung und Verknüpfung personenbezogener Daten über viele Firmen hinweg. In einer Studie des US-Forschungsinstituts Data & Society ist von einer „digitalen Beeinflussungsmaschine“ die Rede, die sowohl kommerziell als auch politisch genutzt werden könne.²²

RASTERFAHNDUNG UND VERHALTENSMANAGEMENT MIT FACEBOOK

Facebook spielt mittlerweile eine wichtige Rolle in der Politik. Ausgangspunkt für den Einsatz sind die sogenannten Seiten von Parteien und PolitikerInnen auf der Plattform. Deutsche Parteien betreiben jeweils bis zu 1500 Facebook-Seiten, von Ortsgruppen bis zur Bundesebene.²³ Diejenigen, die einer solchen Seite bereits aktiv auf Facebook folgen, können über diesen Kanal mit Inhalten „bespielt“ werden. Aber nur ein Bruchteil von ihnen bekommt die Postings wirklich zu sehen. Die „organische“ Reichweite – jene, die ohne Zuzahlung erreicht wird – ist im Laufe der Jahre auf ein Minimum gesunken.²⁴ Bezahlung schafft hier Abhilfe: Postings können dadurch an deutlich mehr – oder an ganz bestimmte – NutzerInnen ausgespielt und Interaktionen gezielt verstärkt werden. Die Reichweite erhöht sich auch, wenn viele interagieren – wenn also ein Posting mit einem „Like“ verse-

¹⁷ Vgl. Shoshana Zuboff, *Das Zeitalter des Überwachungskapitalismus*, Frankfurt/M. 2018. Siehe auch den Beitrag von Zuboff in dieser Ausgabe (Anm. d. Red.).

¹⁸ Vgl. Pixelate, *Desktop Click Fraud Has Risen From 20 % to 25 % in 2017*, 31.5.2017, <http://blog.pixelate.com/desktop-ad-click-fraud-rising-stats-data-2017>; Laurie Sullivan, *Brands Lose Up To An Estimated \$ 50 Billion Annually From Ad Fraud*, 5.3.2019, www.mediapost.com/publications/article/332752.

¹⁹ Vgl. Jake Bialer, *Inside The World Of Ad Arbitrage: An Analysis of 272,220 Taboola Ads*, 10.10.2018, <https://medium.com/@jbialer/cc044a54881c>.

²⁰ Vgl. z. B. Dan Tynan, *How Facebook Powers Money Machines for Obscure Political „News“ Sites*, 24.8.2016, www.theguardian.com/technology/2016/aug/24/facebook-clickbait-political-news-sites-us-election-trump.

²¹ Vgl. „Zu weit weg von der Bevölkerung“, Interview von Markus Huber mit Richard Schmitt, in: *Fleisch Magazin* 30/2016.

²² Vgl. Anthony Nadler/Matthew Crain/Joan Donovan, *Weaponizing the Digital Influence Machine. The Political Perils of Online Ad Tech*, 17.10.2018, <https://datasociety.net/output/weaponizing-the-digital-influence-machine>.

²³ Vgl. Jörg Diehl et al., *How the German Right Wing Dominates Social Media*, 29.4.2019, www.spiegel.de/international/germany/a-1264933.html.

²⁴ Vgl. Brandon Lee, *The Death of Social Media Organic Reach and How to Overcome It*, 4.9.2018, www.curatti.com/death-social-media-organic-reach.

hen, kommentiert oder geteilt wird. Gegen Geld können diejenigen, die bereits interagiert haben, zusätzlich als Werbeträger benutzt werden. Im Optimalfall entsteht eine selbstverstärkende Dynamik und die Inhalte verbreiten sich „viral“. Dies alles als „Werbung“ zu bezeichnen, greift eigentlich zu kurz.

Facebook bietet viele Funktionen an, um in diese Dynamiken einzugreifen. Dazu sortiert die Plattform ihre NutzerInnen in Hunderttausende Kategorien entlang demografischer Eigenschaften, Interessen und Verhaltensweisen – darunter viele sensible Attribute, aus denen etwa die politische Einstellung abgeleitet werden kann.²⁵ Parteien können beliebig viele dieser Kategorien kombinieren, um kleine Gruppen anzusprechen. Diese Art der Rasterfahndung kann auch in Kombination mit Postings eingesetzt werden, die nicht allgemein öffentlich sichtbar sind. Diese sogenannten *dark posts* sehen so aus wie andere Inhalte einer Facebook-Seite, können aber gezielt nur bestimmten Gruppen eingeblendet werden. Auch wenn eine Partei nur rudimentäre Targeting-Kategorien wählt, um etwa schlicht möglichst viele NutzerInnen in einem Land zu erreichen, nutzt sie die geballte Datenmacht der Plattform in ihrer ganzen Tiefe. Denn die Facebook-Algorithmen sind daraufhin optimiert, auch in diesem Fall unter allen NutzerInnen im Land diejenigen zu finden, für die die Inhalte „relevant“ sind und die wahrscheinlich reagieren.²⁶

Eine zentrale Komponente der Targeting-Mechanismen auf Facebook sind die sogenannten Audiences.²⁷ Im einfachsten Fall handelt es sich dabei um Listen von NutzerInnen, die sich aus den gewählten Kategorien ergeben – etwa alle Single-Männer über 50 in Leipzig, die sich für Glücksspiel, nicht aber für die SPD interessieren. Alternativ besteht eine Audience aus NutzerInnen, die bereits mit den eigenen Inhalten interagiert haben

– etwa all diejenigen, die ein Posting kommentiert haben, sich für eine bestimmte Wahlkampfveranstaltung „interessieren“ oder sich – als Beispiel – mindestens zehn Sekunden lang ein Video über „Chemtrails“ angesehen haben.

DIGITALE ZWILLINGE UND DATEN ABSEITS VON FACEBOOK

Genau genommen sind Audiences auf Facebook keine statischen Listen, sondern dynamische Bündel aus Regeln. Welche NutzerInnen enthalten sind, wird abhängig von deren Verhalten in Echtzeit aktualisiert. Es können viele unterschiedliche Audiences verwaltet und verknüpft werden. Schließlich kann Facebooks mächtige „Lookalike“-Mechanik dazu genutzt werden, um digitale Zwillinge zu finden – also Personen mit möglichst ähnlichen Verhaltensweisen. Politische Kampagnen können so zum Beispiel mit eigens erstellten – und nur für bestimmte Gruppen sichtbaren – Inhalten eine kleine Zahl von wütenden Menschen in einer Audience „einfangen“. Facebook sucht dann über die Bevölkerung hinweg nach ähnlichen und besonders aktiven Personen, die als Hebel zur Reichweitensteigerung eingesetzt werden können. In Österreich waren im Wahlkampf 2017 zum Beispiel nur 8900 Personen für die Hälfte aller Facebook-Kommentare verantwortlich²⁸ – lohnenswerte Ziele.

Audiences können auch auf Basis von Daten erstellt werden, die außerhalb von Facebook erfasst wurden. Einerseits können politische Kampagnen den sogenannten Facebook-Pixel in ihre Websites und Apps einbauen – ein kleines Programm, das Nutzungsdaten an die Plattform überträgt. Wer die betroffenen Websites oder Apps nutzt, wird von Facebook identifiziert und in Echtzeit Teil einer Audience, die dann dort weiter eingesetzt werden kann. Andererseits können mit sogenannten Custom Audiences Listen mit Namen, Telefonnummern oder E-Mail-Adressen an Facebook geschickt werden.²⁹ Die Trump-Kampagne hat höchstwahrscheinlich Custom Audiences dazu genutzt, um durch Datenanalysen erstellte Listen von WählerInnen

²⁵ Vgl. José González Cabañas et al., *Unveiling and Quantifying Facebook Exploitation of Sensitive Personal Data for Advertising Purposes*, USENIX Security Symposium, Baltimore 15.–17.8.2018, www.usenix.org/conference/usenixsecurity18/presentation/cabañas.

²⁶ Vgl. Muhammad Ali et al., *Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead to Skewed Outcomes*, 3.4.2019, <https://arxiv.org/abs/1904.02095>.

²⁷ Für eine Beschreibung von Audiences/Targeting siehe Facebook, *Zielgruppen*, www.facebook.com/business/help/168922287067163, Zugriff am 25.4.2019.

²⁸ Vgl. Sofia Palzer-Khomenko et al., *Facebook: 8900 User bestimmten Wahlkampf-Diskurs*, 2.1.2018, www.mokant.at/1802-facebook-user-wahlkampf-diskurs.

²⁹ Vgl. Christl (Anm. 15), S. 47.

hochzuladen – und dann diese und ähnliche Personen adressiert.³⁰

Facebook verkauft eine Vielzahl an Funktionen, die es ermöglichen, NutzerInnen zu finden, die sich wahrscheinlich wie gewünscht verhalten – also auf bestimmte Inhalte klicken, sie kommentieren oder teilen – und hilft dabei nach, dass sie sich so verhalten. Denn die Anregung möglichst vieler Interaktionen liegt dem Geschäftsmodell der Plattform zugrunde. Je provokativer die Inhalte, desto günstiger wird es, sie bezahlt zu verstärken. Basis dafür sind die Datenbestände von Facebook. Mit dem Facebook-Pixel und Custom Audiences potenzieren sich die Möglichkeiten, denn damit können politische Kampagnen jegliches Verhalten außerhalb der Plattform zur Grundlage für ihre Aktivitäten auf Facebook machen. Letztlich kann so alles zur Audience werden – egal ob ein Auszug aus einer Wählerdatenbank, die BesucherInnen eines ganz bestimmten Artikels auf einer Website oder Listen von Personen, die von Datenhandelsfirmen oder Analysedienstleistern wie Cambridge Analytica zusammengestellt wurden.³¹

Das manipulative Potenzial vervielfacht sich, sobald mit NutzerInnen so lange experimentiert wird, bis sie sich verhalten wie gewünscht – wenn sie also etwa einen Beitrag aufrufen oder teilen. Facebook bietet diesbezüglich an, automatisiert verschiedene Kombinationen von Texten, Bildern und Videos zu testen.³² Vor Jahren hat die Plattform selbst derartige Experimente gemacht: Dabei wurde bei Millionen von ahnungslosen NutzerInnen die Reihenfolge und Gewichtung der eingeblendeten Inhalte manipuliert, ein anderes Mal wurden Aufforderungen, wählen zu gehen, eingeblendet. In beiden Fällen habe sich – so heißt es in von Facebook publizierten Studien – die Wahlbeteiligung bei den betroffenen Gruppen leicht erhöht.³³

Trump's Team hat auch abseits von Wahlen Tausende Facebook-Werbeanzeigen im Einsatz, nach eigenen Angaben „um zu testen und zu lernen“.³⁴ Bislang gibt es nur eine Studie, in

der systematisch untersucht wurde, welchen Arten von Targeting europäische NutzerInnen auf Facebook ausgesetzt sind. Basis waren 85 Personen, denen zwischen April 2017 und Juli 2018 insgesamt 71 000 bezahlte Postings eingeblendet wurden. Bei 17 Prozent der Anzeigen wurde Lookalike-Targeting eingesetzt, bei acht Prozent Verhaltensdaten von externen Websites oder Apps, und bei zwei Prozent wurden Daten genutzt, die via Custom Audiences hochgeladen wurden.³⁵ Über den konkreten Einsatz durch die Politik gibt es jedoch kaum belastbare Daten. Sowohl Lookalike-Targeting³⁶ als auch der Facebook-Pixel³⁷ dürften auch in der EU oft eingesetzt werden, Custom Audiences zumindest zum Teil.³⁸ In jedem Fall ist der Einsatz von Facebook für politische Kampagnen in vieler Hinsicht datenschutzrechtlich fragwürdig.³⁹

Google bietet ähnliche Funktionen, inklusive der Einbindung von extern erfassten Daten. Abseits der großen Plattformen können derartige Audiences – also regelbasierte Listen über Einzelpersonen und deren Verhalten – nahezu grenzenlos und in Echtzeit zwischen Hunderten Anbietern verschoben werden.⁴⁰

WÄHLERDATEN IN DEN USA UND DER EU

Online-Microtargeting ist im Grunde die konsequente Weiterentwicklung traditioneller Instrumente: Politische Kampagnen setzen schon seit Langem datenbasierte Methoden ein, um UnterstützerInnen zu mobilisieren, Unentschlossene

30 Vgl. Antonio García Martínez, *How Trump Conquered Facebook – Without Russian Ads*, 23.2.2018, www.wired.com/story/how-trump-conquered-facebook-without-russian-ads.

31 Vgl. ebd.

32 Vgl. Florian Litterst, *Facebook Dynamic Creative*, 18.11.2017, www.adventure.de/facebook-dynamic-creative.

33 Vgl. Christl (Anm. 15), S. 77.

34 Gary Coby auf Twitter, 24.5.2018, <https://twitter.com/GaryCoby/status/999764292181340163>.

35 Vgl. Athanasios Andreou et al., *Measuring the Facebook Advertising Ecosystem, Network and Distributed System Security Symposium*, San Diego, 24–27.2.2019, www.eurecom.fr/publication/5779.

36 Vgl. Tom Dobber et al., *Two Crates of Beer and 40 Pizzas: The Adoption of Innovative Political Behavioural Targeting Techniques*, in: *Internet Policy Review* 4/2017, <https://policyreview.info/archives/2017/issue-4>.

37 Vgl. Peter Teffer, *Tory and National Front Websites Hid Facebook Tracking Pixel*, 13.4.2018, <https://euobserver.com/justice/141589>.

38 Vgl. Information Commissioner's Office, *Democracy Disrupted? Personal Information and Political Influence*, 11.7.2018, <https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf>.

39 Vgl. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, *Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit*, 1.4.2019.

40 Vgl. Christl (Anm. 15), S. 49 f.

zu überzeugen, Mitglieder zu rekrutieren, Freiwillige einzubinden oder Spenden zu akquirieren – und umgekehrt um andere Kampagnen zu sabotieren.⁴¹ Zunehmend wird auf der Grundlage von Datenanalysen entschieden, welche Gruppen mit welchen Botschaften auf welchen Kanälen angesprochen werden – von Hausbesuchen und traditioneller Werbung auf Plakaten, in Zeitungen und im Fernsehen über die Ansprache via Post, E-Mail und Telefon bis zu den genannten Methoden auf Facebook und anderen Plattformen. In den USA nutzen Parteien dazu spätestens seit 2004 umfassende Datenbanken mit Informationen über die gesamte Bevölkerung. Neben Daten aus Wahlregistern werden Profile von privaten Firmen zugekauft. Auch die bei Hausbesuchen gesammelten Daten werden eingespeist.⁴²

In Kombination mit Daten aus Wahlergebnissen, Geo- und Soziodemografie, Fokusgruppen und Umfragen werden statistische Modelle erstellt, mit denen die Wahlbevölkerung in größere bis sehr kleine Gruppen unterteilt wird. Darüber hinaus wird für jede Person eine Prognose über das Wahlverhalten berechnet.⁴³ Die Analysen dienen einerseits der Kampagnensteuerung, andererseits werden damit Listen von Personen erstellt, die dann etwa zu Hausbesuchen führen oder als Custom Audience auf Facebook hochgeladen werden. Schließlich wird versucht, jeden Kontakt mit der Kampagne, jeden Besuch einer Wahlveranstaltung und jede Werbeeinblendung zu erfassen. Diese Vermessung ist der eigentliche Ausgangspunkt, denn die Kampagnensteuerung erfolgt anhand von Kennzahlen und Scores – bis auf die individuelle Ebene. Die NGO Tactical Tech hat die politische Nutzung von Daten überall in der Welt untersucht und dabei über 300 private Dienstleister identifiziert, darunter auch Datenfirmen aus Europa.⁴⁴

In Großbritannien verwenden Parteien zentralisierte Wählerdatenbanken ähnlich wie in den USA.⁴⁵ In anderen europäischen Ländern setzt man – soweit bekannt – auf die Segmentierung der Bevölkerung ohne flächendeckende Erfassung von Einzelpersonen. Dabei werden Daten auf der Ebene von mehreren Haushalten oder Straßenzügen zugekauft.⁴⁶ In Österreich ist hingegen kürzlich bekannt geworden, dass die Österreichische Post an mehrere Parteien Daten über Einzelpersonen inklusive politischer Affinitäten verkauft hat.⁴⁷ Wo jedenfalls sehr wohl auch in der EU eine viel weitergehende Verknüpfung personenbezogener Daten stattfindet, ist einerseits im gesamten Online-Bereich und andererseits, wenn es um Personen geht, deren Daten – zumindest formal – mit „Zustimmung“ verarbeitet werden, weil sie in irgendeiner Form Kontakt mit der Kampagne hatten. Dabei werden Kampagnenplattformen und Apps eingesetzt, die selektive Hausbesuche koordinieren und personalisierte Nachrichten verschicken – sowie E-Mail-Adressen und andere Daten sammeln. Parteimitglieder und andere Personen werden mit verhaltenspsychologisch optimierten Belohnungsmechaniken „spielerisch“ in Kampagnen eingebunden. Sie erhalten etwa für jeden Hausbesuch und jeden digital geteilten Beitrag virtuelle Punkte und steigen dadurch in einer Rangliste auf, mit der Aussicht auf ein Treffen mit der Spitzenkandidatin.⁴⁸

Neben Eigenentwicklungen sticht hier Nationbuilder heraus, eine integrierte Kampagnen- und Datenplattform, die weltweit tausendfach eingesetzt wurde – sowohl von Trump und 3000 anderen politischen Kampagnen in den USA als auch von der Wahlkampagne des heutigen französischen Präsidenten Emmanuel Macron.⁴⁹ Nationbuilder bietet tief greifende Funktionen zur

⁴¹ Vgl. Balázs Bodó et al., *Political Micro-Targeting: A Manchurian Candidate or Just a Dark Horse?*, in: *Internet Policy Review* 4/2017, <https://policyreview.info/archives/2017/issue-4>.

⁴² Vgl. Luke Bunting, *The Evolution of American Microtargeting: An Examination of Modern Political Messaging*, in: *Butler Journal of Undergraduate Research* 1/2015, <https://digitalcommons.butler.edu/bjur/vol1/iss1/2>.

⁴³ Vgl. Colin J. Bennett, *Voter Databases, Micro-Targeting, and Data Protection Law: Can Political Parties Campaign in Europe as They Do in North America?*, in: *International Data Privacy Law* 4/2016, S. 261–275.

⁴⁴ Vgl. Tactical Technology Collective, *„Data and Politics project“ overview, 2018–2019*, <https://tacticaltech.org/projects/data-politics>.

⁴⁵ Vgl. Bennett (Anm. 43).

⁴⁶ Vgl. Simon Kruschinski/André Haller, *Restrictions on Data-Driven Political Micro-Targeting in Germany*, in: *Internet Policy Review* 4/2017, <https://policyreview.info/archives/2017/issue-4>.

⁴⁷ Vgl. Addendum, *Wenn die Post Partei ergreift*, 7.1.2019, www.addendum.org/datenhandel/parteiaffinitaet.

⁴⁸ Vgl. Mario Voigt/Rene Seidenglanz, *Trendstudie. Digital Campaigning in der Bundestagswahl 2017*, Dezember 2017, S. 70–74, <https://t1p.de/3of2>; Dobber et al. (Anm. 36).

⁴⁹ Vgl. Chris O'Brien, *How Nationbuilder's Platform Steered Macron's En Marche, Trump, and Brexit Campaigns to Victory*, 14.7.2017, <https://venturebeat.com/2017/07/14/how-nationbuilder-helped-emmanuel-macron-secure-a-landslide-in-frances-legislative-elections>.

Verknüpfung personenbezogener Daten aus vielen Quellen und mit Social-Media-Plattformen, die in der EU bereits Gegenstand behördlicher Untersuchungen waren.⁵⁰ Die Plattform zeichnet alle Kontakte und Aktivitäten auf, berechnet deren ökonomischen Wert und überträgt damit die datenbasierten Wachstumsstrategien der Tech-Konzerne auf politische Kampagnen.⁵¹

CHANCEN, RISIKEN, HANDLUNGSOPTIONEN

Wie wirkt sich datenbasiertes Microtargeting letztlich gesellschaftlich aus? Was die potenziell positiven Wirkungen angeht, gibt es die Hoffnung, dass diese Art der gezielten Ansprache politische Mobilisierung, Interesse und Partizipation stärken und damit gar die Wahlbeteiligung erhöhen könnte. Kampagnen könnten thematisch vielfältiger werden und BürgerInnen angesichts beschränkter Aufmerksamkeit besser informierte Wahlentscheidungen treffen. Zudem könnten sich Vorteile für kleinere politische AkteurInnen ergeben – solange nicht auch finanzstarke Kräfte entsprechend aufgerüstet haben.⁵²

Umgekehrt bedroht exzessive Datenerfassung durch politische Parteien Privatsphäre und Autonomie. Dies kann eine abschreckende Wirkung hinsichtlich freier Meinungsäußerung und politischer Beteiligung haben. An kleine Gruppen angepasste Kommunikation ermöglicht gezielte Irreführung bei minimaler Nachvollziehbarkeit. Selbst wenn keine plumpen Falschinformationen zum Einsatz kommen, können unterschiedliche Schwerpunkte hervorgehoben werden, was zu einer verzerrten Wahrnehmung politischer Prioritäten führen kann. Microtargeting macht es außerdem sehr viel ökonomischer, diejenigen Teile der Bevölkerung, die als nicht mobilisierbar eingestuft werden, auszuschließen. In Summe könnte datenbasiertes Microtargeting gesellschaftliche Debatten fragmentieren sowie das Vertrauen in Politik und demokratische Institutionen weiter unterminieren.⁵³

Können damit tief greifende politische Überzeugungen auf Knopfdruck manipuliert werden? Natürlich nicht. Wenn es Effekte gibt, sind sie sehr viel indirekter. Möglicherweise sind die geschilderten Praktiken nicht einmal sonderlich wirksam, erzeugen aber trotzdem Kollateralschäden für Öffentlichkeit und Demokratie – oder wir sehen erst die Anfänge dessen, was möglich ist.

Was also tun? Unbestritten ist, dass viel mehr Forschung nötig ist und Online-Targeting auf allen Ebenen transparent werden muss – nicht nur Inhalte, Kanäle und Zeiträume, sondern auch Budgets und genutzte Daten müssen nachvollziehbar sein. Datenschutzrecht muss auch bei politischen Parteien durchgesetzt werden, insbesondere im Online-Bereich, bei Kampagnenplattformen sowie bei der Verknüpfung unterschiedlicher Datenbanken. Darüber hinaus müssen EU-weit die Regeln für politische Werbung an das digitale Zeitalter angepasst werden. Wo für Chancengleichheit und Demokratie nötig, haben sich Parteien auch schon früher auf Beschränkungen bei Wahlwerbung geeinigt. Viele Problematiken stellen sich aber sowohl im kommerziellen als auch im politischen Bereich – von personalisierter Manipulation und Experimenten in digitalen Umgebungen bis zur Macht der Tech-Plattformen.

⁵⁰ Vgl. z.B. Judith Duportail, *The 2017 Presidential Election: The Arrival of Targeted Political Speech in French Politics*, Dezember 2018, <https://ourdataourselves.tacticaltech.org/media/ttc-influence-industry-france.pdf>.

⁵¹ Vgl. Fenwick McKelvey/Jill Piebiak, *Porting the Political Campaign: The Nationbuilder Platform and the Global Flows of Political Technology*, in: *New Media & Society* 3/2018, S. 901–918.

⁵² Vgl. Borgesius et al. (Anm. 1), S. 84 ff.

⁵³ Ebd., S. 87 ff.

WOLFIE CHRISTL

forscht und publiziert über Datenökonomie, Algorithmen und Tech-Plattformen und ist Leiter des unabhängigen Forschungsinstituts Cracked Labs in Wien.

cw@crackedlabs.org

SELBSTBESTIMMUNG UND VERBRAUCHERSCHUTZ IN DER DATENÖKONOMIE

Jörn Lamla

Selbstbestimmung wird in der Datenökonomie zu einer Herausforderung, die die Kapazitäten der Einzelnen übersteigt und durch einen verbesserten Verbraucherschutz allein nicht zu meistern ist. Sie betrifft die Demokratie und Gesellschaft insgesamt und wirft grundlegende Gestaltungsfragen auf, die mit historischen Momenten der Verfassungsgebung verglichen werden können – geht es doch ebenso um die Formgebung von Grundrechten und politischen Basisinstitutionen. Eine Behandlung der Zukunftsfragen von Privatsubjekten, so zeigt der kritische Blick auf die Strukturdynamiken der Datenökonomie, kann dieser Aufgabe kaum gerecht werden. Dennoch ist eine solche Sichtweise, die auf Informationskontroll- und Einspruchsrechte sowie entsprechende Pflichten der Nutzerinnen und Nutzer von digitalen Diensten zielt, im Daten- und Verbraucherschutz weiterhin verbreitet.

Angesichts der Asymmetrie von Kontrollpotenzialen und der Dezentrierung, die die Lebensführung unter den neuen soziotechnischen Bedingungen der Datenökonomie erfährt, sollte Selbstbestimmung nicht länger als Sache einzelner Bürgerinnen und Bürger betrachtet werden. Verbraucherpolitik, so möchte ich in diesem Beitrag zeigen, muss sich zur „Verbraucherdemokratie“ erweitern, die die Gestaltung von Regeln und Konventionen der Datenökonomie systematisch an Prozeduren öffentlicher Aushandlung rückbindet.

Im Folgenden werde ich dafür zunächst die Idee der Selbstbestimmung historisieren und soziologisch deuten, um darauf aufbauend neue Perspektiven aufzuzeigen und abschließend einige normative Schlussfolgerungen zu ziehen.

AUTONOMIEFIKTIONEN UND STRUKTURDYNAMIKEN

Der Begriff „Selbstbestimmung“ ist insofern widersprüchlich, als gesellschaftlich bedingt ist, was als Freiheit des Individuums erscheint und diesem sozial oder sogar als Wesenszug zugeschrieben wird. Zwar ist es durchaus möglich, dass sich Individuen an den verantwortungsvollen Gebrauch subjektiver und politischer Freiheitsrechte gewöhnen oder sich den kalkulierenden Umgang mit ökonomischen Privatinteressen antrainieren. Die Idee subjektiver Selbstbestimmung befindet sich dann mit gesellschaftlichen Institutionen und Strukturen des Rechtsstaats oder der Marktgesellschaft in einem Passungsverhältnis; der Widerspruch fällt nicht weiter auf. Gleichwohl handelt es sich aber um historische Konzepte der Selbstbestimmung, die im gesellschaftlichen Wandel an Kraft und Plausibilität verlieren können. Wenn sich die Einstellungen und Gewohnheiten der Menschen oder die institutionellen Rahmenbedingungen der Lebensführung grundlegend verschieben, wie es mit der Entfaltung der Datenökonomie mehr als wahrscheinlich wird, kann diese Freiheitsfähigkeit nicht nur ab-, sondern auch Schaden nehmen.

Um das Argument zu verdeutlichen, sei auf einen Klassiker der Soziologie verwiesen: David Riesman, Nathan Glazer und Reuel Denney beschrieben in ihrem Bestseller „The Lonely Crowd“ („Die einsame Masse“) schon 1950, also noch fernab aller Digitalisierungsdynamiken, eine Entwicklung hin zu einer Gesellschaft von Verbraucherinnen und Verbrauchern, deren Charaktereigenschaften so deutlich von denen innen geleiteter Subjekte abweichen, dass sich das Problem der Autonomiegewinnung auf völlig neue Weise stelle.⁹¹ Der neue, zunehmend dominante Typus des außengeleiteten Charakters sei vor al-

lem ein Informationssammler. Halt und Orientierung gewinne er nicht mehr aus verinnerlichten ethischen Prinzipien, die im turbulenten Leben wie ein in sich stabilisierter Kreiselkompass die Richtung anzeigen, sondern er suche die Umwelt wie mit einer Radaranlage permanent nach Hinweisen auf Hindernisse und Möglichkeiten ab, um seinen Kurs durchs Leben daran immer wieder neu auszurichten.

Die soziologische Qualität der Auseinandersetzung mit dieser Wandlungsdynamik besteht nun darin, dass Riesman und seine Kollegen die Entwicklung nicht nostalgisch verteufelten. Selbstbestimmung sei nicht fest an den Habitus der protestantisch geprägten, innengeleiteten Bürgerinnen und Bürger gebunden. Vielmehr müsse Autonomie immer in der Relation von individuellen Charaktereigenschaften oder Haltungen auf der einen und gesellschaftlichen Strukturbedingungen auf der anderen Seite gedacht werden. So könne das, was dem männlich geprägten bürgerlichen Privatsubjekt in bestimmten Zeiten den Glanz von Autonomie verleihe, etwa die ermöglichenden Normen, Rollenbilder und Routinen geschlechtsspezifischer Arbeitsteilung in der Familie, unter veränderten gesellschaftlichen Bedingungen zur inneren Geißel werden, die es in seiner Fähigkeit zur Veränderung, etwa zur Reduktion von Berufsarbeit, stark einschränke. Was einst als Wesenszug der Selbstbestimmung erschien, wird so zum Element starker bis suchtartiger Abhängigkeit.⁰² Umgekehrt bedeute die Abhängigkeit der Außengeleiteten von wechselnden und unberechenbaren Informationsströmen der Umwelt nicht per se den Verlust von Autonomie.⁰³ Vielmehr gelte es, Selbstbestimmung zeitgemäß zu fassen und die Bedingungen hierfür zu klären.

Vor diesem Hintergrund verlieren Vorstellungen von Selbstbestimmung an Plausibilität, die Verbraucherinnen und Verbraucher überzeitlich als innengeleitete Privatsubjekte mit klaren Präfe-

renzen und verantwortungsethischen Haltungen definieren. Solche Autonomievorstellungen finden sich bis heute keineswegs nur bei ausgewiesenen Anhängern des sogenannten Neoliberalismus, sondern ebenso mit Bezug auf das Recht auf informationelle Selbstbestimmung oder im europäischen Leitbild des mündigen Verbrauchers.

Erst in jüngerer Zeit mehrten sich Versuche, solche Leitbilder zu relativieren und mit empirischen Bedingungen der Selbstbestimmung zu verzahnen.⁰⁴ Die angebotenen Alternativen, die Verbraucherinnen und Verbraucher als verletzte oder vertrauende und nur zum kleinen Teil verantwortungsvoll agierende Subjekte erscheinen lassen, tragen zwar der Komplexität und Unübersichtlichkeit heutiger Märkte sowie der ungleichen Ressourcenausstattung Rechnung. Zugleich verabschieden sie sich aber tendenziell von einer Neubestimmung und -gestaltung von Autonomie, die damit als leere bürgerliche Fiktion zurückbleibt.

Statt Selbstbestimmung durch staatlichen Verbraucherschutz zu ersetzen, käme es jedoch darauf an, Verbraucherschutz und Selbstbestimmung in neuer Weise zusammenzudenken. Das digitale Zeitalter bietet dafür reichlich Anlass: Mit der Entfaltung der Datenökonomie wird die Struktur der Außenlenkung derart auf die Spitze getrieben, dass sich das Problem hier in voller Schärfe stellt.

SELBSTBESTIMMUNG DURCH DATEN?

Ein (scheinbar) extremer Fall ist in diesem Zusammenhang die sogenannte *Quantified-self*-Bewegung. Deren Motto lautet: Selbstbestimmung durch Daten – womit vor allem quantifizierende Informationen über Körperzustände, Leistungsfähigkeiten, statistische Vergleichsmaße, Scores und so weiter gemeint sind. Ein gutes Beispiel ist das Fitnesstracking, das heißt die Nutzung von Apps wie Runtastic. Diese ermöglichen in Verbindung mit „smarter“ Sensortechnologie in Mobiltelefo-

⁰¹ Vgl. David Riesman/Reuel Denney/Nathan Glazer, *Die einsame Masse. Eine Untersuchung der Wandlungen des amerikanischen Charakters*, Hamburg 1958, insb. S. 251 ff.

⁰² Vgl. Anthony Giddens, *Leben in einer posttraditionalen Gesellschaft*, in: ders./Ulrich Beck/Scott Lash, *Reflexive Modernisierung. Eine Kontroverse*, Frankfurt/M. 1996, S. 113–194, insb. S. 129 ff. sowie ders., *Wandel der Intimität. Sexualität, Liebe und Erotik in modernen Gesellschaften*, Frankfurt/M. 1993, insb. S. 86 ff.

⁰³ Vgl. Riesman/Denney/Glazer (Anm. 1), S. 272.

⁰⁴ Vgl. Hans-Werner Micklitz et al., *Der vertrauende, der verletzte oder der verantwortungsvolle Verbraucher? Plädoyer für eine differenzierte Strategie in der Verbraucherpolitik*. Stellungnahme des Wissenschaftlichen Beirats Verbraucher- und Ernährungspolitik beim Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz, Berlin 2010; Christoph Strüneck, *Der mündige Verbraucher. Ein populäres Leitbild auf dem Prüfstand*, in: Christian Bala/Klaus Müller (Hrsg.), *Abschied vom Otto Normalverbraucher. Moderne Verbraucherforschung: Leitbilder, Informationen, Demokratie*, Essen 2015, S. 19–28.

nen oder speziellen Uhren beziehungsweise Fitnessarmbändern durch Auswertung von Körper- und Bewegungsdaten sowie den ständigen Vergleich mit anderen Personen, die eigene Fitness zu überwachen, anderen im sozialen Netzwerk zu demonstrieren und gezielt zu verbessern.⁰⁵

Eine Vielzahl von Tools verspricht heute Unterstützung dabei, *self-tracking* beziehungsweise *lifelogging* als Mittel der Selbsterkenntnis und -beherrschung zu nutzen.⁰⁶ Der Typus des Informationssammlers erscheint dabei nicht länger als außengeleitet, sondern als selbstbestimmt und souverän im Umgang mit Informationen. Daten werden hierfür als Rohstoff gebraucht, und die für die Datenproduktion erforderliche Entäußerung der Person wird – entgegen der verbreiteten Assoziation des Rechts auf informationelle Selbstbestimmung mit Datensparsamkeit – zur Notwendigkeit, wenn nicht gar zur allgemeinen Pflicht erklärt. Die gesteigerte Abhängigkeit von jenen Plattformunternehmen und Datendienstleistern, die diese Daten erheben, aufbereiten, klassifizieren, korrelieren, interpretieren, damit personenbezogene Profile erstellen und das soziale beziehungsweise algorithmisch generierte Feedback organisieren, wird dabei ausgeblendet. Dies wäre sicherlich nicht weiter beachtenswert, wenn es sich tatsächlich um eine Ausnahmeerscheinung handeln würde. In der Datenökonomie jedoch gewinnt dieses Modell der informationsbasierten Lebensführung paradigmatische Qualität.

Die Bestimmung des Selbst mittels digital aufbereiteter Daten und Informationen weist darin viele Facetten auf, die in ihrer Zusammenschau zu erkennen geben, wie sich die Autonomie der Individuen in Fremdbestimmung aufzulösen droht. In der Aufmerksamkeitsökonomie der sozialen Medien herrscht ein gesteigerter sozialer Druck zur Inszenierung des Selbst als singuläre und authentische Person.⁰⁷ Die Angewiesenheit auf Feedback und Anerkennung durch andere macht es dabei erforderlich, ein feines Sensorium für Meinungsumschwünge zu entwickeln, und ein Großteil der Kommunikation dreht sich um aktuelle Trends

und kulturelle Moden. Schon dies ist eine Form medial vermittelter Selbstbestimmung, die durch die datenökonomische Verwertbarkeit von Traffic und Nutzungszeiten, Netzwerkeffekten, Skalierungserfolgen und kulturellen Bedeutungen maßgeblich mitbestimmt ist. Diese vielfältigen Daten werden über die gezielt eingesetzten Bindungskräfte sozialer Netzwerke hinaus erfasst und verknüpft, um Verhalten zu beobachten und vorherzusagen, Nutzerprofile zu erstellen, neue Marktchancen zu erschließen, Erlebnisse zu personalisieren, vielleicht auch Preise zu individualisieren – alles mit dem Ziel, Zugriffschancen auf die Verbraucherinnen und Verbraucher zu erhöhen.

Auch diese, häufig automatisierten Prozesse bestimmen das jeweilige Selbst mit, das sich in passgenauen (Werbe-)Angeboten wiedererkennen kann und soll. Empfehlungsalgorithmen von Musikstreamingdiensten wie Spotify etwa kombinieren Daten zu individuellen Hörgewohnheiten mit einem riesigen Datenpool, der statistische Klassifikationen von Musikstilen erlaubt. Damit unterstützt der Dienst die Verbraucherinnen und Verbraucher bei der Entwicklung ihres ganz eigenen Musikgeschmacks.⁰⁸ Aber dieser Aspekt singulärer Identität ist dann kaum mehr als selbstbestimmt zu bezeichnen.

Die Kontrollpotenziale sind dabei asymmetrisch verteilt, und die Schere zwischen Nutzen und Diensteanbietern öffnet sich weiter.⁰⁹ Innengeleiteten Menschen, die nach eigenen Relevanzkriterien konsumieren und verhindern wollen, dass sich ihre Datenspuren ablösen und als Datenselbst ein Eigenleben entwickeln, bleibt oft nur die Selbstexklusion von Angeboten und Nutzungspraktiken. Jene, die der Ansicht sind, die Strategien kommerzieller Datenkraken taktisch durchkreuzen zu können, indem sie mit konstruierten Identitäten oder Falschinformationen spielen, unterschätzen indes die Möglichkeiten der Anbieter, Daten unterschiedlicher Quellen abzugleichen und in Beziehung zu setzen. Demgegenüber wird die Akzeptanz

05 Vgl. Ramón Reichert, Die Vermessung des Selbst. Self-Tracking in der digitalen Kontrollgesellschaft, in: Michael Friedewald/Jörn Lamla/Alexander Roßnagel (Hrsg.), Informationelle Selbstbestimmung im digitalen Wandel, Wiesbaden 2017, S. 91–107.

06 Vgl. Steffen Mau, Das metrische Wir. Über die Quantifizierung des Sozialen, Berlin 2017, S. 167.

07 Vgl. Andreas Reckwitz, Die Gesellschaft der Singularitäten. Zum Strukturwandel der Moderne, Berlin 2017, insb. S. 225 ff.

08 Vgl. Jonathan Kropf, Recommender Systems in der populären Musik. Kritik und Gestaltungsoptionen, in: ders./Stefan Laser (Hrsg.), Digitale Bewertungspraktiken. Für eine Bewertungssoziologie des Digitalen, Wiesbaden 2018, S. 127–163.

09 Vgl. Jörn Lamla/Carsten Ochs, Selbstbestimmungspraktiken in der Datenökonomie: Gesellschaftlicher Widerspruch oder „privates“ Paradox?, in: Birgit Blättel-Mink/Peter Kenning (Hrsg.), Paradoxien des Verbraucherverhaltens, Wiesbaden 2019, S. 25–39, hier S. 31 ff.

von Außenlenkung vermutlich noch zunehmen, wenn Unterstützungsangebote durch Datenreichtum, größere Rechenleistung und verbessertes *machine learning* immer treffsicherer werden. Es ist allerdings fraglich, ob der Komfort datenökonomischer Navigationshilfen, die bei identitätsrelevanten Problemen der Partneruche oder der politischen Wahl ähnlich agieren wie beim Konsum oder Autofahren, den erlittenen Autonomieverlust ausgleichen kann.

Die derzeit führende Disziplin in der Entwicklung solch datenbasierter Navigationshilfen ist die Verhaltensökonomik, deren Expertise im „Anstupsen“ (*nudging*) von Entscheidungen besteht: Durch Umgebungsreize, die bestimmte Emotionen auslösen sollen (affektives *priming*), oder gezielte Situationsrahmungen werden Bedeutungen und Attraktivitätswerte von Optionen verschoben, um das Verhalten in eine bestimmte Richtung zu lenken.¹⁰ Schon heute beschäftigen Unternehmen professionelle Verhaltensformer, die mit solcher Expertise die Kundenbindung und Zahlungsbereitschaft effektiv zu steigern versprechen.¹¹ Beispielsweise werden über sogenanntes A/B-Testing verschiedene App-Versionen getestet, indem unbemerkt Nutzungsdaten erhoben und ausgewertet werden, um durch Designverbesserungen Nutzungszeiten und Umsätze zu erhöhen. Bei Online-Spielen wird auf diese Weise das Suchtpotenzial gezielt gesteigert.¹² In der Datenökonomie entwickeln sich diese Techniken zum *hypernudging*, das durch umfassendes sensorgestütztes Monitoring, Big-Data-Analysen, verbesserte Vorhersagemodelle und die Möglichkeit zur Echtzeitreaktion, zum Beispiel abhängig von emotionalen Erregungszuständen, immer präzisere Verhaltensimpulse zu setzen vermag.¹³ Nicht nur Privatunternehmen und Krankenkassen, sondern auch Regierungen sind an solchem Beeinflussungswissen äußerst interessiert.

¹⁰ Vgl. Richard H. Thaler/Cass R. Sunstein, *Nudge. Wie man kluge Entscheidungen anstößt*, Berlin 2011.

¹¹ Vgl. Nir Eyal, *Hooked. Wie Sie Produkte erschaffen, die süchtig machen*, München 2014.

¹² Vgl. Katharina Zweig et al., *Kontinuierliches A/B-Testing zur Optimierung von Spielerbindung und Monetarisierung bei „Freemium“-Spielen*, in: Birgit Blättel-Mink/Peter Kenning (Hrsg.), *Paradoxien des Verbraucherverhaltens*, Wiesbaden 2019, S. 43–57.

¹³ Vgl. Karen Yeung, *„Hypernudge“: Big Data as a Mode of Regulation by Design*, in: *Information, Communication & Society* 1/2017, S. 118–136.

WIDERSPRUCH DES LIBERTÄREN PATERNALISMUS

Selbstbestimmung, verstanden als rekursiver Optimierungsprozess der Entäußerung und Freigabe persönlicher Daten, der maschinellen Verarbeitung und Verknüpfung solcher Daten durch Dritte, der Ableitung verborgener personalisierter Verhaltensimpulse und deren evidenzbasierter Erfolgsmessung, ist von Fremdbestimmung nicht mehr zu unterscheiden. Vertreterinnen und Vertreter der Verhaltensökonomik verweisen zur Verteidigung auf den Ansatz des libertären Paternalismus: Anstupser würden das Verhalten keineswegs so starr festlegen wie Vorschriften oder Zwangsmaßnahmen. Das handelnde Subjekt sei immer noch frei, sich anders zu entscheiden. Es könne in der Kantine weiterhin zu den zuckerhaltigen Riegeln greifen, nachdem die Obstschale prominenter platziert wurde; auch könne es die Bereitschaft zur Organspende zurückziehen, sollte das Verfahren auf „Opt-out“ umgestellt werden. Doch für die Reproduktion jener Entscheidungsautonomie, die der libertäre Paternalismus hier unterstellt, wird mit seinen empirisch motivierenden Bindungstechniken nichts mehr getan. Vielmehr setzt er Kompetenzen voraus, die mit seiner erfolgreichen Ausbreitung verdrängt werden. Diese Kompetenzen zu stärken, wird daher zur Aufgabe für den Verbraucherschutz.

In der Verbraucherpolitik manifestiert sich der Widerspruch jedoch ebenso: Auch sie will Verbraucherinnen und Verbrauchern vermehrt mittels *nudging* helfen, ihre wohlverstandenen Interessen einschließlich ihrer informationellen Selbstbestimmungsansprüche zu realisieren. Nicht nur Lebensmittelampeln mit Signalwirkung, sondern auch gesetzlich vorgeschriebene Voreinstellungen im Bereich des Daten- und Privatheitsschutzes (Privacy by Default, Opt-in-Verfahren, erleichterte Verschlüsselung privater Kommunikation) sind hierfür typisch. Damit scheint es über die gesellschaftliche Nützlichkeit der Daten- und Verhaltensökonomie einen breiten Konsens zu geben. Lediglich über die Richtung der Verhaltenssteuerung und die zentralen Werte, die damit wirksam werden sollen, wird noch gestritten.

Dabei geht es nicht selten symbolpolitisch zu: Nicht um Profitanteile oder die Sicherung von politischen Einflusspotenzialen, sondern allein um Gesundheitsförderung oder nachhaltigen Konsum geht es dann – und Cookies dienen selbstverständ-

lich ausschließlich der Serviceverbesserung. Doch nur wer eine unabhängige kritische Öffentlichkeit nicht mehr zu fürchten braucht, kann sich auf solche Muster der nachträglichen Rationalisierung datenökonomischer Praktiken und Geschäftsmodelle zurückziehen. Der Schutz und die politische Stärkung der Verbraucherinnen und Verbraucher könnten hier ansetzen: Diese müssten in die Lage versetzt werden, kritisch prüfen zu können, welche Werte und Präferenzen in die Entscheidungsarchitekturen der Datenökonomie eingeschrieben sind und ob es sich dabei tatsächlich um die ihres wohlverstandenen Interesses handelt. Sie dürften demnach den Verhaltensimpulsen nicht nur empirisch folgen, sondern müssten ihr Einverständnis auch nach kritischer Prüfung noch erteilen können. Doch was meint solche kritische Kompetenz in der Datenökonomie genau, und wie lässt sie sich unter deren Bedingungen entfalten?

An dieser Stelle hilft die Soziologie der Infrastrukturen weiter.¹⁴ Für die Verbraucherinnen und Verbraucher wirkt die verhaltensökonomisch eingerichtete und sich zunehmend automatisiert und in Echtzeit anschmiegende datenökonomische Umwelt – zumindest dort, wo sie erfolgreich eingerichtet ist – wie eine zweite Natur, eben „smart“, aber damit auch undurchdringlich. Infrastrukturen ermöglichen Gewohnheitsbildung und stabilisieren gesellschaftliche Konventionen.

Ganz anders sieht es aus der Perspektive der Designerinnen und Designer dieser gebauten Umwelten aus: Sie erscheinen als Architektinnen und Architekten von Entscheidungsprozessen und legen willkürlich oder gegebenenfalls mit strategischem Kalkül fest, welche Konventionen und normativen Aspekte im Verbraucherverhalten prioritär gelten und verfolgt werden sollen.¹⁵ Das Verhalten läuft in infrastrukturellen Bahnen nicht zuletzt deshalb gerichtet ab, weil die Festlegung der Verhaltensausrichtung durch die Entscheidungsarchitektur irgendwann aus dem Blickfeld verschwindet. Problematisch ist aber, dass diese normativen und verhaltensnormierenden Vorentscheidungen unter den Gestaltungsbedingungen der Datenökonomie nicht länger mühsam politisch ausgehandelt werden müssen, sondern überhaupt nicht mehr in den Blick geraten.

Hier ist die Verbraucherpolitik gefordert: Um das Prinzip und die Möglichkeit der Selbstbestimmung gegen die Eigendynamik der Datenökonomie zu verteidigen, sollte zum einen gesetzlich festgeschrieben werden, dass Prozesse der digitalen Infrastrukturgestaltung nach demokratischen Prinzipien der kollektiven Selbstbestimmung und Aushandlung zu gestalten sind. Diese Prozesse dürfen nicht länger den verborgenen operierenden Entscheidungsarchitektinnen und -architekten überlassen werden, die für die Gestaltungseliten der Digitalwirtschaft arbeiten. Zum anderen sollten die Infrastrukturen der Datenökonomie verpflichtend so gestaltet werden müssen, dass sie die Kompetenz zur kritischen Reflexion von normierenden Designentscheidungen erhalten oder sogar steigern.

BEWERTUNGSKOMPETENZ: VERBRAUCHERSCHUTZ ALS DIGITALE INFRASTRUKTURGESTALTUNG

Genauso wie die Hierarchisierung der Werte in der autogerechten Stadt aus umweltpolitischer Sicht kritikwürdig erscheint, müsste der politische Gehalt infrastruktureller Vorfestlegungen auch im digitalen Zeitalter öffentlich präsent gehalten werden. Man denke nur an die Planungsfantasien für eine umfassende Verhaltenslenkung und Überwachung in „Smart Cities“. Der Verbraucherschutz sollte mithin dabei helfen, die Bedingungen demokratischer Selbstbestimmung langfristig zu sichern, anstatt mit den gleichen Steuerungsmitteln um Anteile an den „Verhaltensterminkontraktmärkten“¹⁶ der Datenökonomie zu kämpfen.

Hierzu müsste die Verbraucherpolitik ein neues, alternatives Gestaltungsparadigma der „Verbraucherdemokratie“ entwickeln und im Bereich datenökonomischer Infrastrukturen zur Anwendung bringen.¹⁷ Dieses könnte und sollte den informationsabhängigen Verbraucherinnen und Verbrauchern die kritische Reflexion und Evaluation infrastruktureller Vorfestlegungen von Wertordnungen und Bewertungsprozessen

¹⁴ Vgl. etwa Susan Leigh Star/Karen Ruhleder, *Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces*, in: *Information System Research* 1/1996, S. 111–134.

¹⁵ Vgl. Thaler/Sunstein (Anm. 10), S. 118ff.

¹⁶ Shoshana Zuboff, *Das Zeitalter des Überwachungskapitalismus*, Frankfurt/M.–New York 2019, S. 25. Siehe auch den Beitrag von Zuboff in dieser Ausgabe (Anm. d. Red.).

¹⁷ Vgl. Jörn Lamla, *Verbraucherdemokratie. Politische Soziologie der Konsumgesellschaft*, Berlin 2013.

duren erleichtern, aber auch abverlangen. Hierfür müsste nicht länger die fragwürdig gewordene Gegebenheit innengeleiteter Subjekte vorausgesetzt oder angestrebt werden. Vielmehr würde die Autonomie an Strukturen und Prozeduren kritischer Evaluation gebunden, die auch kollektive Praktiken und Möglichkeiten professioneller Unterstützung und Stellvertretung einschließen. Sogar *nudging* und *gamification* könnten eine Rolle spielen, wenn diese Techniken statt von moralischer Reflexion zu entlasten, durch Framing, soziales Feedback oder emotionale Gratifikationen umgekehrt Prüfungen ermuntern, inwiefern Algorithmen, Plattformen oder Interfaces diskriminieren, manipulieren oder sich Einsprüchen entziehen.

Eine Schwierigkeit dieses neuen Ansatzes liegt nun darin, dass Praktiken der Bewertung und Evaluation bereits als fester Bestandteil verhaltensökonomischer Entscheidungsarchitekturen in den digitalen Infrastrukturen verbreitet sind. Nahezu überall werden Verbraucherinnen und Verbraucher mit der Vergabe von Sternchen, mit Rankings und Ratings konfrontiert, werden ihnen Testergebnisse und Empfehlungen angeboten und sind sie zugleich aufgefordert, sich selbst durch Kommentare, Likes oder authentische Erfahrungsberichte an solchen Bewertungsprozeduren zu beteiligen.

Insofern – so könnte man meinen – erfüllt die Datenökonomie doch längst das Kriterium, Kritik anzuregen und kritische Kompetenzen der Verbraucherinnen und Verbraucher zu schulen. Eine solche Einschätzung übersieht jedoch, dass diese Bewertungspraktiken die Äußerung von Kritik als Element einer verhaltensökonomisch gestalteten Bewertungslandschaft mit programmierten Verhaltensroutinen ununterscheidbar verschmelzen. Die menschlichen und maschinellen Bewertungen und Empfehlungen dienen maßgeblich der sozialen Einbettung von digitalen Märkten und datenökonomischen Geschäftsmodellen, indem sie Vertrauen, Loyalität und Akzeptanzbereitschaft generieren.¹⁸ Das Resultat aber ist eine hybride Intelligenz, die Kritik nur noch in vorgezeichneten Bahnen zulässt und gegenüber den architektonischen Vorentscheidungen ihre Distanz und unabhängige Urteilskraft verliert.

¹⁸ Vgl. ebd., S. 278 ff.

¹⁹ Vgl. Luc Boltanski/Laurent Thévenot, *Über die Rechtfertigung. Eine Soziologie der kritischen Urteilskraft*, Hamburg 2007.

Soll ein solcher gesellschaftlicher Digitalisierungspfad vermieden werden, muss in die fortschreitende Hybridisierung von menschlicher und künstlicher Intelligenz eine Sollbruchstelle, in das rekursive, datenbasierte Trainieren von Menschen und Maschinen eine Unwucht eingebaut werden. Erforderlich sind Infrastrukturen, die eine kritische Bewertung und Evaluation der Rahmengestaltung von Algorithmen und Bewertungsordnungen initiieren und wachhalten. Transparenzpflichten hinsichtlich der mit Algorithmen- und Interfacegestaltung verbundenen Normierungsabsichten allein reichen dafür nicht aus, da auch die nicht beabsichtigten Folgen und Diskriminierungseffekte Beachtung finden müssen. Vielmehr sollten Prozesse der Informationstechnikgestaltung gezielt und wiederkehrend mit der Pluralität möglicher Konventionen und Bewertungsordnungen konfrontiert werden, um kritische Reflexionen über deren infrastrukturelle Priorisierung anzuregen.¹⁹

Diese Praxis müsste zudem mit den Bewertungs- und Entscheidungsrouinen der Verbraucherinnen und Verbraucher verzahnt werden. Denn es macht einen Unterschied, ob diese in den Bahnen der Schnäppchenjagd oder sozialen Statuskonkurrenz, der Bequemlichkeit oder gesundheitspolitischer Fitnessideale, der ästhetischen Anmutung, kulturellen Diversität oder ökologischen Nachhaltigkeit verlaufen. Die Kontroversen, mit denen die Verbraucherpolitik in Bereichen wie Energie, Wohnen, Verkehr, Tourismus, Ernährung oder Kosmetik laufend konfrontiert ist, können eine solche Pluralität präsent halten. Die Kompetenz zur Selbstbestimmung in der Datenökonomie bildet und erhält sich dann in dem Maße, wie die Verbraucherinnen und Verbraucher ebenso wie die Designerinnen und Designer lernen, die Pluralität und prinzipielle Offenheit von Wert- und Bewertungsordnungen in den Alltagsroutinen und technischen Infrastrukturen nicht länger verdrängen zu müssen.

JÖRN LAMLA

ist Professor für Soziologische Theorie an der Universität Kassel, Mitglied im vom Bundesministerium für Bildung und Forschung geförderten Forum Privatheit sowie Sprecher des Koordinierungsgremiums im bundesweiten Netzwerk Verbraucherforschung.

lamla@uni-kassel.de

Herausgegeben von der
Bundeszentrale für politische Bildung
Adenauerallee 86, 53113 Bonn
Telefon: (0228) 9 95 15-0



Redaktionsschluss dieser Ausgabe: 31. Mai 2019

REDAKTION

Lorenz Abu Ayyash
Anne-Sophie Friedel
Johannes Piepenbrink (verantwortlich für diese Ausgabe)
Frederik Schetter (Volontär)
Anne Seibring
apuz@bpb.de
www.bpb.de/apuz
twitter.com/APuZ_bpb

Newsletter abonnieren: www.bpb.de/apuz-aktuell
Einzelausgaben bestellen: www.bpb.de/shop/apuz

GRAFISCHES KONZEPT

Charlotte Cassel/Meiré und Meiré, Köln

SATZ

le-tex publishing services GmbH, Leipzig

DRUCK

Frankfurter Societäts-Druckerei GmbH, Mörfelden-Walldorf

ABONNEMENT

Aus Politik und Zeitgeschichte wird mit der Wochenzeitung
Das **Parlament** ausgeliefert.

Jahresabonnement 25,80 Euro; ermäßigt 13,80 Euro.

Im Ausland zzgl. Versandkosten.

FAZIT Communication GmbH

c/o InTime Media Services GmbH

fazit-com@intime-media-services.de

Die Veröffentlichungen in „Aus Politik und Zeitgeschichte“ sind keine Meinungsäußerungen der Bundeszentrale für politische Bildung (bpb). Für die inhaltlichen Aussagen tragen die Autorinnen und Autoren die Verantwortung. Beachten Sie bitte auch das weitere Print-, Online- und Veranstaltungsangebot der bpb, das weiterführende, ergänzende und kontroverse Standpunkte zum Thema bereithält.

ISSN 0479-611 X



Die Texte dieser Ausgabe – mit Ausnahme des Textes von Shoshana Zuboff – stehen unter einer Creative Commons Lizenz vom Typ Namensnennung-Nicht Kommerziell-Keine Bearbeitung 3.0 Deutschland.

APuZ
Nächste Ausgabe
27-28/2019, 1. Juli 2019
**BILDUNG UND
DIGITALISIERUNG**



APuZ

AUS POLITIK UND ZEITGESCHICHTE

www.bpb.de/apuz