Deutsche Bank Research

EU-Monitor

Digitale Ökonomie und struktureller Wandel

Digitalpolitik

KI, Big Data und die Zukunft der Demokratie

12. September 2019

Autor
Kevin Körner
+49 69 910-31718
kevin.koerner@db.com

Editor
Barbara Boettcher

Deutsche Bank AG
Deutsche Bank Research
Frankfurt am Main
Deutschland
E-Mail: marketing.dbr@db.com
Fax: +49 69 910-31877

www.dbresearch.de

DB Research Management
Stefan Schneider

Original in engl. Sprache: 22. August 2019

Für Milliarden von Menschen hat die digitale Transformation enorme Vorteile und Annehmlichkeiten gebracht. Allerdings lassen sich die wirtschaftlichen und politischen Implikationen wohl erst im Rückblick vollständig erfassen. Für demokratische Institutionen und Prozesse ergeben sich daraus beträchtliche Herausforderungen für die Beurteilung der Chancen und Risiken neuer Technologien.

Liberale Gesellschaftsmodelle können sich digitale Technologien ebenso zunutze machen wie autoritäre; einerseits können Regierungen besser zur Rechenschaft gezogen werden, andererseits wird gegebenenfalls der Repression der Weg geebnet. Digitale Technologie hat einen beispiellosen Informations-Zugang und Austausch ermöglicht. Sie hat aber auch die Verbreitung von Fehlinformationen und Propaganda sowie das Entstehen von Echokammern verstärkt – und so möglicherweise zu einem wachsenden Populismus und zur Polarisierung demokratischer Gesellschaften beigetragen.

Rund um die Welt profitieren Nutzer von kostenlosen Dienstleistungen in der Datenwirtschaft. Angesichts der zugrundeliegenden Geschäftsmodelle und Konzentration von Einfluss und Vermögen stellen sich jedoch drängende Fragen in Bezug auf den Schutz der Privatsphäre, das Eigentum an Daten und gezielte Manipulation – nicht nur für wirtschaftliche, sondern auch für politische Zwecke.

Autoritäre Staaten haben rasch gelernt, wie sie Überwachungstechnologie, künstliche Intelligenz und Massendaten zu ihrem Vorteil nutzen können, sowohl für staatliche Kontrolle im Inland als auch, um Demokratien im Ausland zu unterminieren. Für Demokratien, deren Zusammenhalt auf Teilhabe und Zustimmung ihrer mündigen Bürger beruht, stellt dies eine ganz neue Herausforderung dar. Wie sie damit umgehen, wird sich entscheidend darauf auswirken, wie sie im intensiver werdenden Wettbewerb der politischen Systeme bestehen. Demokratien müssen zudem einen fundierten Dialog über das Eigentum an Daten und Technologie sowie die Verteilung der Vorteile von KI und Automatisierung führen. Gleichzeitig müssen sie ihre technologische Wettbewerbsfähigkeit und wirtschaftliche Prosperität als Stützpfeiler der demokratischen Ordnung sichern.

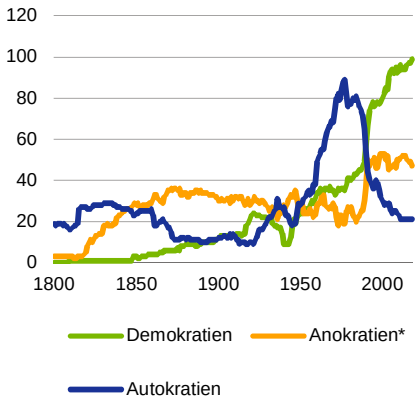
Regierungen müssen regulatorische Vorgaben, Wettbewerbsvorschriften und die staatliche Aufsicht so überarbeiten, dass sie den neuen Anforderungen der globalen, digitalen Wirtschaft gerecht werden. Unternehmen müssen sicherstellen, dass ihre Geschäftsmodelle und Produkte im Einklang mit den verfassungsmäßigen Rechten der Nutzer und mit der Integrität demokratischer Institutionen und Prozesse stehen. Und die Bürger müssen digitale Kompetenzen erwerben, um die Algorithmen und das Design hinter ihren Apps und Geräten sowie die zugrundeliegenden Mechanismen der Datenwirtschaft besser zu verstehen.

Die EU spielt in der Auseinandersetzung mit den Herausforderungen der digitalen Transformation eine Vorreiterrolle. Weltweit setzt sie Maßstäbe bei der Bekämpfung von Desinformation und der Festlegung von rechtlichen und ethischen Standards für den Datenschutz und die KI-Entwicklung.

KI, Big Data und die Zukunft der Demokratie

Siegeszug der Demokratie in den letzten 30 Jahren 1

Zahl der Länder (Bevölkerung > 500 Tsd.)

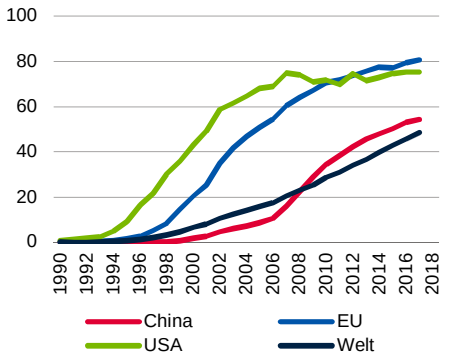


*Zwischenform zwischen Demokratie und Autokratie

Quelle: Center for Systemic Peace Polity iV Project

Anstieg der globalen Konnektivität 2

Internet-Nutzer (% der Bevölkerung)



Quelle: Weltbank aus World Telecommunication/ICT Development Report and database

Die Demokratie muss geschützt werden. Bürger, die in liberalen Demokratien aufgewachsen sind, sehen ihre verfassungsmäßig garantierten Rechte und Freiheiten häufig als selbstverständlich an und glauben, nichts könne diese grundlegende Ordnung erschüttern. Menschen, die in autoritären oder totalitären Strukturen gelebt haben, sind dagegen für dieses Thema stärker sensibilisiert. Sie haben gelernt, dass die Demokratie nie als selbstverständlich anzusehen ist. Tatsächlich sind Demokratien wie diejenigen, die sich in den letzten 30 Jahren durchgesetzt haben, eine absolute Ausnahme in der Menschheitsgeschichte.

Mit Hilfe von Gewaltenteilung, unabhängigen Gerichten und Medienfreiheit schützen sich Demokratien gegen Versuche aus dem autoritären Lager, ihre Fundamente zur untergraben und zu stürzen. In den vergangenen Jahren hat sich jedoch in verschiedenen demokratischen Ländern rund um die Welt, darunter auch Staaten der Europäischen Union, gezeigt, dass diese Mechanismen durchaus fragil sein können.

Dies ist als Warnung zu verstehen: Demokratische Institutionen können für sich allein nicht ordnungsgemäß funktionieren. Dafür brauchen sie gut informierte und engagierte Bürger sowie deren politischen Vertreter. In dieser Hinsicht hat sich die digitale Transformation der beiden vergangenen Jahrzehnte zunehmend als zweischneidiges Schwert erwiesen.

Technologie ist für sich genommen politisch neutral. Digitale Technologien können gleichermaßen in den Dienst liberaler wie autoritärer Gesellschaftsentwürfe gestellt werden; sie können sowohl dazu dienen, Regierungen besser zur Rechenschaft zu ziehen als auch Repression zu intensivieren. Dies soll jedoch nicht heißen, dass die technologische Entwicklung dagegen gefeit sei, einer bestimmten politischen oder wirtschaftlichen Organisationsform Vorteile zu verschaffen. Neue Technologien sind vielmehr eine der treibenden Kräfte in der Menschheitsgeschichte. Wie sie Gesellschaften und politische Systeme formen, hängt jedoch davon ab, wie sie von Unternehmen und Regierungen umgesetzt werden und wie die Bürger damit umgehen.

Milliarden Menschen profitieren. Die Vorteile der digitalen Transformation der vergangenen Jahre für die zwischenmenschliche Kommunikation und Organisation sind kaum zu bestreiten. Der heute selbstverständliche Zugang zu Informationen war noch vor wenigen Jahrzehnten unvorstellbar, gleichzeitig können sich die Menschen weltweit innerhalb von Sekunden austauschen und koordinieren. Für Milliarden von Menschen hat die digitale Transformation – sinnbildlich verkörpert durch das Smartphone – enormen Nutzen und Annehmlichkeiten gebracht. Dies hat den gesellschaftlichen Diskurs um neue Formen der multilateralen Kommunikation bereichert. Bürger, politische Verantwortungsträger und Regierungen nutzen ganz selbstverständlich soziale Medien wie Facebook oder Twitter, um in Kontakt zu treten und Standpunkte, Meinungen oder Vorschläge auszutauschen.

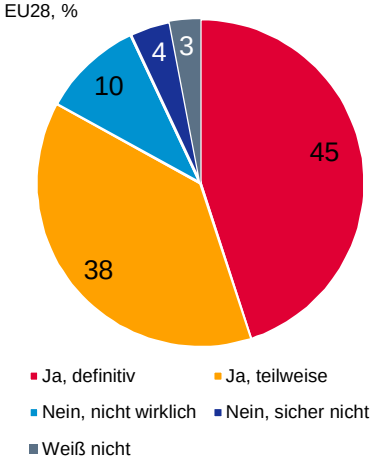
Zunächst hoffte man, dass die neuen Technologien zu einer Demokratisierungswelle führen könnten. In den Neunzigerjahren, d.h. in den Anfangsjahren des World Wide Web, bestanden große Hoffnungen, dass die intensivere globale Vernetzung und rasche technologische Fortschritte zu einer neuen Demokratisierungswelle führen würden. Man glaubte, dass die Bürger mit der zunehmenden Verbreitung der Technologie eine bessere demokratische Kontrolle ausüben könnten und dass die Regierungen intensivere Rechenschaft über ihre Tätigkeit ablegen müssten.[1] Noch während des Arabischen Frühlings zu Beginn

[1] Foreign Affairs (12. Februar 2019). Does technology favor tyranny?

Digitalpolitik: KI, Big Data und die Zukunft der Demokratie

Umfrage: „Fake News“ und Demokratie 3

EU28, %



Umfrage: Ist nach Ihrer Meinung die Existenz von Nachrichten oder Information, welche die Realität ungenau darstellen oder sogar falsch sind, ein Problem für die Demokratie im Allgemeinen? (EU28, %)

Quelle: Flash Eurobarometer 464 (April 2018)

dieses Jahrzehnts sah es so aus, als erfülle sich dieses Versprechen: Staatliche Zensur und Versammlungsverbote wurden in autoritären Staaten über soziale Medien umgangen.

Die dunkle Seite der Technologie. Nach der ersten Euphorie und der umfassenden Einführung von Schlüsseltechnologien dauerte es einige Jahre, bis Individuen, Bürgerrechtsgruppen, Regierungen und die Gesellschaft insgesamt allmählich erkannten, welche Herausforderungen diese Technologien gleichzeitig mit sich bringen. Insbesondere die Skandale um Cambridge Analytica und Facebook im Zusammenhang mit dem Brexit-Referendum sowie den US-Präsidentschaftswahlen im Jahr 2016 haben gezeigt, dass digitale Technologie auch in etablierten Demokratien eingesetzt werden kann, um Wähler bewusst zu manipulieren und den politischen Diskurs zu verzerren.

Die technologischen Entwicklungssprünge des letzten Jahrzehnts haben sich so rasch vollzogen, dass sowohl politische Entscheidungsträger als auch Marktteilnehmer die entsprechenden Implikationen erst im Rückblick vollständig erfassen können. Hierin ist zweifelsohne eine der größten Herausforderungen für Gesetzgebung und Regulierung im Hinblick darauf zu sehen, wie mit den Risiken bestimmter Technologien für demokratische Institutionen und Prozesse umzugehen ist.

Die Anforderungen an jeden Einzelnen, die tägliche Informationsflut zu filtern und kritisch zu hinterfragen, sind deutlich gestiegen. Gleichzeitig haben sich durch die rasche Einbindung von Social Media-Plattformen in alle Lebensbereiche der Nutzer ganz neue Möglichkeiten der gezielten, personalisierten, automatisierten und häufig auch unbemerkten Einflussnahme ergeben. Gleichzeitig haben autoritäre Staaten rasch gelernt, wie sie Überwachungstechnologie, Massendaten und künstliche Intelligenz zu ihrem Vorteil nutzen können – sei es, um die staatliche Kontrolle im Inland zu stärken, oder um demokratische Gesellschaften im Ausland zu unterminieren.

Eine gänzlich neue Herausforderung für die Demokratie. Für Demokratien, deren Zusammenhalt auf Teilhabe und Zustimmung ihrer mündigen Bürger beruht, stellt dies eine ganz neue Herausforderung dar. Wie sie damit umgehen, wird sich entscheidend darauf auswirken, wie sie im intensiver werdenden Wettbewerb der politischen Systeme bestehen.

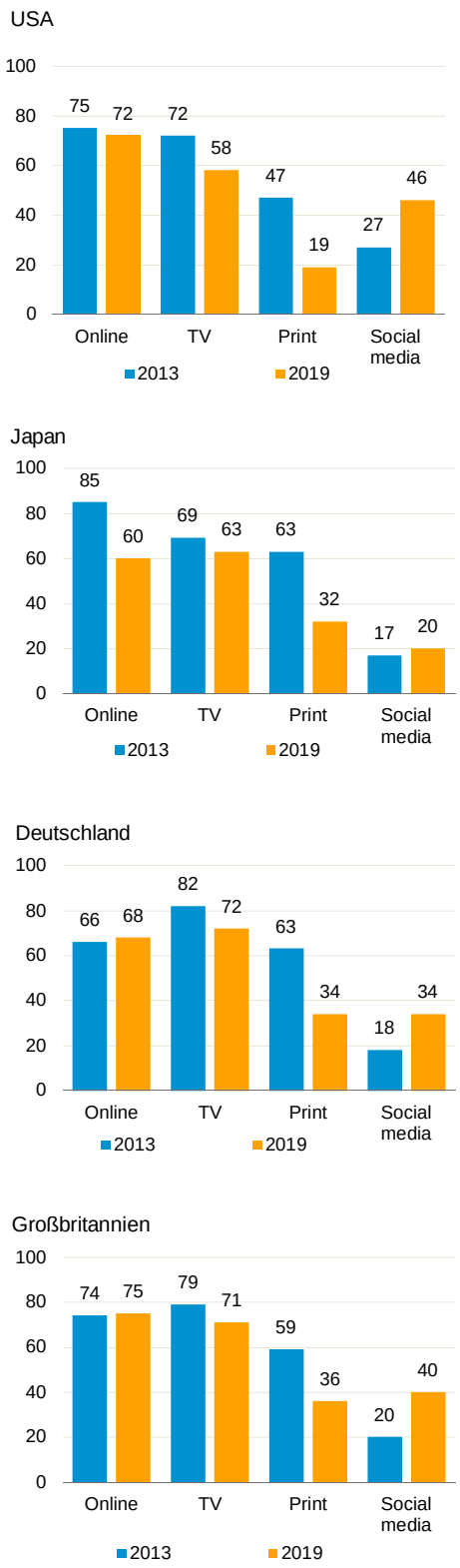
Anhand der Erfahrungen der vergangenen Jahre und der stetig wachsenden Zahl von anekdotischen Belegen lassen sich einige Schlüsselbereiche ermitteln, in denen digitale Technologien die Demokratie potenziell aushöhlen und destabilisieren können:

- Fehlinformationen, Echokammern und gezielte Manipulation
- weitreichende Verschiebungen der finanziellen und politischen Einflusssphären in der Datenwirtschaft
- Verlust der Privatsphäre und sinkende Sensibilität der Nutzer
- persuasive Technologien und Abhängigkeit von sozialen Medien
- Erosion von Bürgerrechten durch algorithmische Voreingenommenheit („algorithmic bias“)
- Massenüberwachung und Stärkung von autoritären Strukturen
- Auswirkungen von KI und Automatisierung auf Wettbewerbsfähigkeit und die Unterstützung der Demokratie durch ihre Bürger

Digitalpolitik: KI, Big Data und die Zukunft der Demokratie

Online dominiert den Nachrichtenkonsum der Nutzer in den meisten Länden 4

Nachrichtenquelle, %



Quelle: Reuters Institute Digital News Report 2019

Fehlinformationen, Echokammern und gezielte Manipulation

Die Auswirkungen der digitalen Transformation der vergangenen beiden Jahrzehnte auf die Politik werden vor allem in der Kommunikation und dem Austausch von Informationen zwischen Einzelnen und der Gesellschaft insgesamt sichtbar. Seit dem Anbeginn der Menschheitsgeschichte sind Propaganda, Desinformation und Manipulation Standardwerkzeuge der Politik. Die allumfassende Vernetzung, immer preiswertere (mobile) Computertechnik und die schiere Verfügbarkeit von Daten haben jedoch in den vergangenen Jahren eine bisher ungekannte, koordinierte Verbreitung von Fehlinformationen und personalisierter Manipulation ermöglicht. In dieser Beziehung wurde eine neue Ebene erreicht.

Inzwischen erfassen die politischen Entscheidungsträger und die Gesellschaften allmählich einige der drängendsten Implikationen:

— Massenhafte, koordinierte Desinformation

— Mikrotargeting von Wählern

— Polarisierung des öffentlichen Dialogs in demokratischen Gesellschaften

— Hybride Kriegsführung und Misstrauen gegenüber demokratischen Institutionen und Regierungen

— striktere staatliche Kontrolle des Informationsflusses und der öffentlichen Meinung in autoritären Gesellschaften

Grundlegende Verschiebungen in der Medienlandschaft und Polarisierung der Gesellschaft. Die Disruption der traditionellen Kommunikationslandschaft, die zuvor von etablierten Medien dominiert wurde, durch digitale und multilaterale Kommunikation und Social Media-Plattformen stellt für demokratische Gesellschaften eine beträchtliche Herausforderung dar. Im Prinzip kann das zusätzliche Angebot an alternativen, multilateralen und weitgehend gratis verfügbaren Informationen und Nachrichten als Bereicherung der politischen Debatte und als Instrument angesehen werden, das Bürgern eine bessere Teilhabe ermöglicht, Korruption aufdeckt und Regierungen verantwortlich hält.

Allerdings werden die auf diesen Plattformen verbreiteten Informationen häufig nicht sorgsam überprüft; dazu kommt die inhärente Tendenz der eingesetzten Algorithmen, die Nutzer in ihren bestehenden Meinungen zu bestärken. Dadurch können Fehlinformationen und Propaganda koordiniert verbreitet werden und es entstehen digitale Filterblasen oder Echokammern, welche wiederum die Gesellschaft polarisieren und den öffentlichen Dialog aushöhlen können.

Vormarsch von „Gratis“-Online-Medien fördert sensationsheischende Darstellung. Da immer mehr Menschen weltweit ihre Informationen größtenteils über Online-Medien, Newsfeeds und Social Media-Plattformen beziehen, spielen diese inzwischen eine wichtige Rolle im politischen Prozess. Diese Veränderung des Nachrichtenkonsumverhaltens hat zu einem verstärkten Maß an Sensationalismus in der Politik geführt. Begünstigt wird dies durch das Geschäftsmodell von Plattformen und Online-Journalismus, das tendenziell eher auf Emotionen als auf faktenbasierte Inhalte setzt.

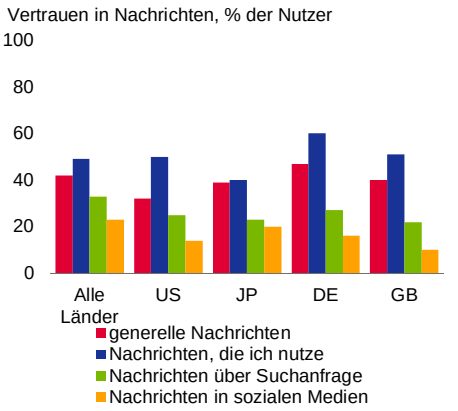
Die zunehmende politische Spaltung und der Aufschwung des Populismus in demokratischen Gesellschaften sowie die Fragmentierung der Parteienlandschaft in den vergangenen Jahren fallen mit dem Aufstieg der sozialen Medien

und dem steigenden Vernetzungsgrad zusammen und können zumindest zum Teil auf diese Entwicklung zurückgeführt werden.[2]

Neue Dimensionen von Cyberkonflikten und autoritärer Kontrolle. Aus geopolitischer Sicht hat die „hybride Kriegsführung" durch neue und immer billigere Technologien an Bedeutung gewonnen. Autoritäre Regierungen, die demokratische Staaten in Misskredit bringen und unterhöhlen sowie ausländische Wähler manipulieren wollen, haben über das offene Internet Zugang zur freien Kommunikation in demokratischen und liberalen Gesellschaften. Gleichzeitig schränken diese Regierungen den Zugang ihrer eigenen Bürger zu Informationen aus dem Ausland ein, indem sie das Internet im eigenen Land abschotten, Zensur ausüben und gleichzeitig die öffentliche Meinung über Online-Medien und Plattformen kontrollieren und steuern.

Nutzer und Bürger im In- und Ausland werden unter anderem durch die Verbreitung unzutreffender oder hochgradig irreführender Informationen durch soziale „Bots" beeinflusst, d.h. Softwareanwendungen, die menschliches Verhalten über automatisch betriebene Social Media-Konten nachahmen, um die öffentliche Meinung zu beeinflussen. Der rasche Fortschritt der KI-Technologie ermöglicht zudem immer ausgefeiltere „Deep Fakes", bei denen Audio- und Videoinhalte manipuliert oder gefälscht werden. So können Fehlinformationen und Propaganda verbreitetet werden, die weit über Chat-Kommentare oder Faked News-Artikel hinausgehen.

Geringes Vertrauen in Nachrichten: Ein globales Phänomen 5



Alle Länder: 24 aus Europa, 7 aus Asien, 6 aus Amerika, 1 aus Afrika
Quelle: Reuters Institute Digital News Report 2019

Vertrauensverlust. Durch die anhaltende Verbreitung von Verschwörungstheorien und anderen unwahren bzw. verzerrten Informationen schwinden die Fähigkeit der Bürger, „objektive" Wahrheiten oder Aussagen, auf die man sich einigen kann, zu erkennen. Dies kann zu einem generellen Misstrauen gegenüber allen Medien, zu Fatalismus und zu mangelndem Engagement in Teilen der Bevölkerung führen, was wiederum den gesellschaftlichen Dialog ernsthaft in Mitleidenschaft zieht und politische Gegensätze verschärft.[3]

Vor allem angesichts neuer Entwicklungen und komplexer Themen wird dies zur Herausforderung, da die Menschen hier nicht auf eigene (kollektive) Erfahrungen zurückgreifen können.[4] Der Vertrauensverlust leistet autoritären Regimen Vorschub, die diejenigen demokratischen Gesellschaften destabilisieren wollen, welche den Anspruch eben dieser Regimes auf uneingeschränkte Macht infrage stellen. Gleichzeitig hilft der Vertrauensverlust diesen Regimen dabei, das liberale demokratische Modell ihrer eigenen Bevölkerung gegenüber als vermeintlich dysfunktional, heuchlerisch und dekadent darzustellen.

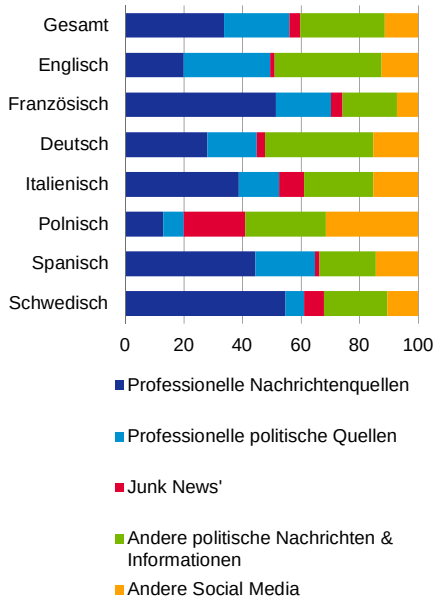
Wie das Ausland über soziale Medien Einfluss nehmen und Wähler manipulieren kann, hat sich bisher insbesondere 2016 bei den Präsidentschaftswahlen in den USA und beim Brexit-Referendum in Großbritannien gezeigt.

Russland und die US-Präsidentschaftswahlen im Jahr 2016. In Russland kam der in diesem Jahr veröffentlichte „Mueller-Report" zu dem Schluss, dass „die russische Regierung umfassend und systematisch in die Präsidentschaftswahlen im Jahr 2016 eingegriffen" habe. Dem Bericht zufolge erreichte die in Russland basierte „Internet Research Agency" Millionen von US-amerikanischen Social Media-Nutzern über Social Media-Konten auf Facebook, Twitter oder Instagram, die angeblich von US-Aktivisten betrieben wurden. Die Social Media-Kampagne habe das Ziel gehabt, „in den USA eine politische Spaltung zu provozieren und zu verstärken", und habe „den Kandidaten Trump [im Wahlkampf] begünstigt". Die zweite große Kampagne war ein Hackerangriff des russischen

[2] Europäisches Parlament (2019). Polarisation and the use of technology in political campaigns and communication.
[3] Deibert, R. (2019). The Road to Digital Unfreedom: Three Painful Truths about Social Medial. Journal of Democracy, Januar 2019.
[4] Schneider, Stefan (2017). Vox populi, vox dei oder etwa nicht? Deutsche Bank Research. Deutschland-Monitor.

Junk-Nachrichten bei den Wahlen zum EU-Parlament 2019 6

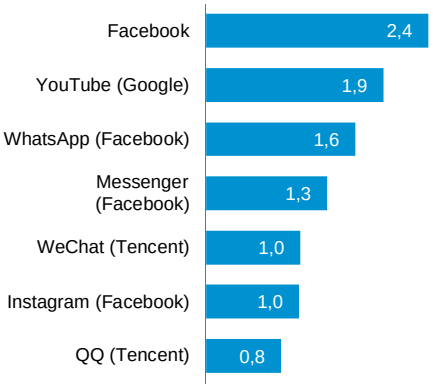
Arten von politischen Nachrichten/Information über Twitter geteilt, %



Quelle: Oxford Internet Institute, Junk News During the EU Parliamentary Elections (2019)

Globale Reichweite von Social Media 7

Monatlich aktive Nutzer in Milliarden, Ende 2018 / Q1 2019



Quellen: Firmenberichte und -webseiten, DataReportal von Hootsuite und We are social, Deutsche Bank Research

Geheimdienstes, um „gehackte Unterlagen zu veröffentlichen, die der Clinton-Wahlkampagne Schaden zufügen konnten".[5] Sonderermittler Mueller warnte mit Blick auf die Wahlen 2020, dass das Risiko einer versuchten Einflussnahme durch Russland weiterhin erhöht sei.[6]

Der Skandal um Facebook und Cambridge Analytica. Im Rahmen eines Vergleichs mit der Federal Trade Commission wurde Facebook im Juli eine Strafzahlung in Rekordhöhe von USD 5 Mrd. für Verstöße gegen die Privatsphäre auferlegt, worunter u.a. der Cambridge Analytica-Skandal im Jahr 2016 fällt. Außerdem musste das Unternehmen neue Datenschutzvorgaben akzeptieren. Nach Auffassung von Kritikern gehen diese Maßnahmen nicht weit genug. Sie bemängeln außerdem, es sei weiterhin unklar, ab wann Facebook gewusst habe, dass Cambridge Analytica die Daten von Millionen Facebook-Nutzern für psychometrisches Profiling und Mikrotargeting im Vorfeld der US-Präsidentschaftswahlen 2016 missbraucht habe.[7] Kürzlich bestätigte ein ehemaliger Mitarbeiter von Cambridge Analytica, dass das Datenanalyseunternehmen außerdem vor dem Brexit-Referendum im Jahr 2016 für Leave.EU und die UKIP-Partei tätig gewesen sei. Beide angeblichen Auftraggeber dementierten dies wiederholt.[8]

Missbrauch von sozialen Medien zu politischen Zwecken ist ein globales Phänomen. Die Skandale des Jahres 2016 sind jedoch kein Einzelfall. Der Einfluss von Social Media auf Wahlen und den politischen Diskurs ist zu einem globalen Phänomen geworden. Als jüngstes Beispiel im Zusammenhang mit den Protesten in Hongkong haben Twitter und Facebook chinesische Konten entfernt, um „das zu blockieren, was sie als staatlich unterstützte chinesische Fehlinformationskampagne beschrieben", so die BCC.[9] Die globale Dimension wurde bereits früher durch den Missbrauch von Facebook und WhatsApp zur Verbreitung von Desinformation, Hassreden und Propaganda in Indien und Brasilien, zwei der größten Demokratien der Welt, sichtbar.[10] Außerdem ist deutlich geworden, dass vor allem die politischen Ränder versuchen, die Wähler und die Öffentlichkeit über Trolle, Bots und gezielte Manipulation zu beeinflussen.[11]

Auch in Europa ist dies zu beobachten. Auch in Europa werden inzwischen regelmäßig „Junk News" und Traffic-Manipulationen eingesetzt, um die Wähler und die öffentliche Meinung zu beeinflussen. Laut einem von der Universität Oxford durchgeführten Forschungsprojekt war dies z.B. bei nationalen Wahlen in Deutschland, Frankreich und Schweden sowie beim Katalonien-Referendum in Spanien und bei den Gelbwestenprotesten in Frankreich der Fall.[12]

Politische Entscheidungsträger reagieren auf die Herausforderung. Vor den Wahlen zum Europaparlament im Mai stellte die EU-Kommission einen Aktionsplan zum Umgang mit Desinformation auf, der u.a. eine Vereinbarung über einen „EU-Verhaltenskodex zur Bekämpfung von Desinformation" mit wichtigen sozialen Netzwerken beinhaltete.[13] Facebook richtete eine „Kommandozentrale" ein, um zu verhindern, dass über seine Plattform Einfluss auf die Europawahlen genommen werde. Zwar kam es bei den Europawahlen anscheinend nicht im selben epidemischen Ausmaß zu Falschinformationen und Propaganda wie in einigen anderen Regionen, aber es gibt immer noch hinreichend Belege dafür,

[5] US Department of Justice (2019). Report on the investigation into Russian interference in the 2016 presidential election.
[6] Financial Times (25. Juli 2019).
[7] The Hill (4. August 2019).
[8] Politico (30. Juli 2019) und The Guardian (30. Juli 2019).
[9] BBC (6. April 2019) und BBC (24. Oktober 2018).
[10] BBC (20. August 2019).
[11] Europäisches Parlament (2019). Polarisation and the use of technology in political campaigns and communication.
[12] Oxford Internet Institute (2019). Junk news during the EU parliamentary elections: Lessons from a seven-language study of Twitter and Facebook.
[13] EU-Kommission (2019). Tackling online disinformation.

dass im Internet bewusst irreführende oder täuschende Informationen, Bots und Fake-Accounts eingesetzt wurden.[14] Einem veröffentlichten Bericht der EU-Kommission zufolge gibt es Belege für „fortgesetzte und aufrechterhaltene Desinformationsaktivitäten russischen Ursprungs, die auf eine Reduzierung der Wahlbeteiligung und Beeinflussung der Wählerpräferenzen abzielten".[15]

Dies zeigt, dass der Kampf gegen Desinformation, Hasskommentare und automatisierte Propaganda in Demokratien nach wie vor eine Herausforderung darstellt. Dabei stellt sich vor allem die Frage, wie eine offene Gesellschaft mit diesem Problem umgehen kann, ohne Meinungsäußerungen zu zensieren oder das Grundrecht auf Redefreiheit zu verletzen.[16]

Weitreichende Verschiebungen der Einflusssphären in der Datenwirtschaft

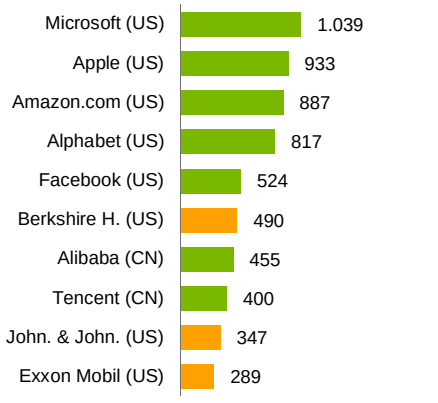
Die oben beschriebene Disruption der traditionellen Kommunikations- und Informationswege ist auf den Aufstieg eines neuen und einflussreichen Geschäftsmodells zurückzuführen, das mit einander zum Teil überschneidenden, wenn auch nicht synonymen Begriffen beschrieben wird, nämlich als

„Plattform"-, „Daten"-, „Aufmerksamkeits"- oder „Überwachungs"-Wirtschaft

Technologieunternehmen, die ihren Nutzern (scheinbar kostenlose) Dienstleistungen wie z.B. Online-Suchen, Kommunikationsanwendungen, Spiele oder sonstige Unterhaltung anbieten, fungieren gleichsam als Torhüter für Werbetreibende. Diesen verschaffen sie nämlich Zugang zur Aufmerksamkeit der Nutzer als auch deren Daten, wodurch Werbeplatzierungen optimiert werden können. Nicht zuletzt der beachtliche Anstieg des Marktwerts von Unternehmen wie Google und Facebook (die zusammen 60% des digitalen Werbemarkts in den USA beherrschen) hat gezeigt, dass der Zugang zu den Nutzern und den Nutzerdaten außerordentlich profitabel vermarktet werden kann.[17]

Die 10 weltweit größten börsennotierten Unternehmen – 7 Tech-Riesen aus den USA und China 8

Marktkapitalisierung, in Mrd. USD



Quelle: Bloomberg Finance LP (Abruf am 19. August 2019)

Dass große Technologieunternehmen exklusiv über riesige Datenmengen verfügen, verschafft ihnen nicht nur in ihren jeweiligen Marktsegmenten enorme Vorteile, sondern auch bei der Entwicklung und beim Trainieren von KI-Systemen. So können sie ihre Marktposition in etablierten Märkten weiter ausbauen und verfügen gleichzeitig über einen Vorsprung bei der Erschließung neuer Märkte.

Das Zeitalter des „Überwachungskapitalismus". Die Harvard-Ökonomin Shoshana Zuboff spricht vom Beginn einer neuen Ära, nämlich des Zeitalters des „Überwachungskapitalismus". Ihr zufolge führen Skalen- und Verbundeffekte in der Plattformwirtschaft zu einer rasch zunehmenden Konzentration von Daten, Wissen, finanzieller Macht und Kontrolle über Kommunikationskanäle in den Händen einer kleinen technologischen Elite.[18] Dadurch entsteht, so Zuboff, eine sich rasch verstärkende gesellschaftliche Asymmetrie beim wirtschaftlichen und politischen Einfluss.[19] Ihre Einschätzung wird vom israelischen Historiker Yuval Noah Harari geteilt. Harari sieht einen engen Zusammenhang zwischen den zunehmenden tribalistischen Tendenzen in der Politik sowie dem Aufschwung autoritärer und populistischer Strömungen in demokratischen Ge-

[14] Politico (23. Mai 2019).
[15] Deutsche Welle (14. Juni 2019).
[16] EU-Kommission (2019). Countering illegal hate speech online – EU Code of Conduct ensures swift response.
[17] Vox (20. Februar 2019).
[18] Zuboff, Shoshana. (2019). The age of surveillance capitalism.
[19] Zuboff, Shoshana. (2016). The secrets of surveillance capitalism. Frankfurter Allgemeine Zeitung. 5. März 2016.

sellschaften und den technologischen Entwicklungen unserer Zeit. Er befürchtet, der Einfluss der Öffentlichkeit auf den politischen Prozess könnte unbemerkt schwinden, sodass vermeintlich freie Entscheidungen und Wahlen irgendwann in der Zukunft nur noch als demokratische Fassade dienen.[20]

Insider aus dem Technologiesektor warnen vor ihren eigenen Schöpfungen. Warnungen vor der Technologie kommen jedoch nicht nur aus der Wissenschaft, von Maschinenstürmern oder Kapitalismuskritikern. Einige der unverblümtesten Kritiker haben selbst entscheidend zu den technologischen Entwicklungen der vergangenen Jahre beigetragen. Laut Tristan Harris, der früher für Design-Ethik bei Google verantwortlich war, werden die Entscheidungen und Auffassungen von Milliarden Menschen zunehmend von einer Handvoll Unternehmen beeinflusst, was weitreichende Folgen für den demokratischen Diskurs hat.[21] James Williams, ein ehemaliger Produktstratege bei Google, stellt die Frage, ob die Demokratie das Zeitalter der Technologie überhaupt überleben kann. Er spricht von einer „Aufmerksamkeitsökonomie“, in der Algorithmen um die Zeit der Nutzer konkurrieren und deshalb sensationsheischende, emotional besetzte Inhalte Vorrang gegenüber rationalen und faktenbasierten Inhalten einräumen. Nach Auffassung von Williams gilt dies auch zunehmend für die Politik.[22]

Forderungen nach einer verstärkten Kontrolle der großen Technologiekonzerne zum Schutz der Demokratie. Einige Kommentatoren sehen den Cambridge Analytica-Skandal als Warnung, dass die Technologie, deren Eigentümer einige der reichsten Mitglieder der Gesellschaft sind, genutzt werden kann, um die Bevölkerung systematisch zu manipulieren und so eine „gelenkte“ Demokratie zu etablieren, die vor allem den eng umrissenen Interessen einer „globalen Plutokratie“ dient.[23] Manche Politiker schlagen bereits eine Zerschlagung der großen Technologiekonzerne vor, um deren Zugewinn an wirtschaftlichen und politischen Einfluss abzumildern. Unter anderem erhebt die US-Senatorin und potenzielle Präsidentschaftskandidatin Elizabeth Warren (Demokraten) diese Forderung.[24] Andere gehen nicht ganz so weit und fordern lediglich eine striktere Regulierung und Beaufsichtigung der Datenwirtschaft. Auch die Regierung Trump hat die Technologieunternehmen genauer in den Blick genommen; so hat das US-Justizministerium eine Untersuchung wegen möglicher wettbewerbsfeindlicher Praktiken eingeleitet.[25] Dass intensiver über den Umgang mit dieser Herausforderung diskutiert wird, zeigt bereits, welchen immensen gesellschaftlichen und politischen Einfluss Digitalunternehmen in den vergangenen Jahren bekommen haben.

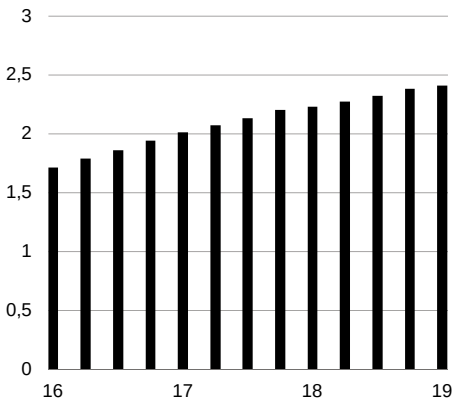
Verlust der Privatsphäre und sinkende Sensibilität der Nutzer

Die Datenwirtschaft hat sich praktisch rund um den Globus verbreitet; aufgrund des preiswerten Zugangs zu Smartphones und freier Inhalte ist das Online-Verhalten der Nutzer weitgehend von ihrem finanziellen, ethnischen, religiösen und politischen Hintergrund abgekoppelt. Gleichzeitig haben sich Nutzer grenzüberschreitend und über politische Systeme hinweg rasch daran gewöhnt, für bequeme Dienste, die Möglichkeit zum Austausch mit anderen und soziale Bestätigung mit ihren eigenen, häufig sehr persönlichen Daten zu bezahlen.

[20] Harari, Yuval Noah (2018). Why Technology Favors Tyranny. The Atlantic. Oktober 2018.
[21] Harris, Tristan (2017). How a handful of tech companies control billions of minds every day. TED2017.
[22] The Guardian (2017). 'Our minds can be hijacked': the tech insiders who fear a smartphone dystopia. 6. Oktober 2017
[23] Cadwalladr, C. (7. Mai 2017). The Great British Brexit robbery: how our democracy was hijacked. The Guardian.
[24] Los Angeles Times (21. März 2019).
[25] Reuters, 23. Juli 2019.

Stetige Zunahme der Facebook-Nutzer 9

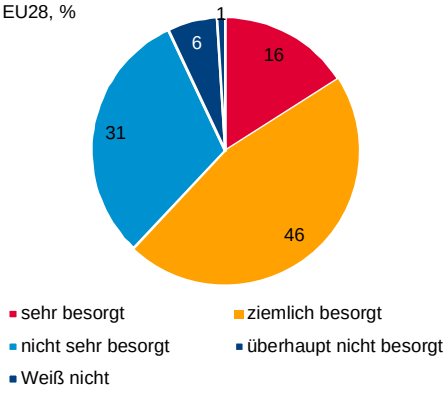
Facebook monatlich aktive Benutzer (MAUs), Mrd.



Quelle: Facebook

Mehr als 60% der Europäer machen sich um ihre Online-Daten Sorgen 10

EU28, %



Umfrage: „Wie besorgt sind Sie darüber, dass Sie nicht die volle Kontrolle über die Informationen haben, die Sie online zur Verfügung stellen?"

Quelle: Special Eurobarometer 487a (Juni 2019)

Die Nutzer haben sich rasch daran gewöhnt, praktisch rund um die Uhr unter Beobachtung zu stehen, **...** wenn auch – zumindest in demokratischen Gesellschaften – nicht durch Orwells „Großen Bruder"; sondern durch unser Allzweckcomputer in der Westentasche, ergänzt durch andere High Tech-Produkte wie smarte Fernsehgeräte, Smartwatches, Fitness Tracker oder virtuelle Assistenten. Cookies, Tracking Tools und Logins in soziale Medien ermöglichen es, Daten zum Nutzerverhalten plattform-, seiten- und geräteübergreifend zu synchronisieren. Diese geben ständig Aufschluss über unseren Aufenthaltsort, unser Verhalten, unsere Einstellungen, unsere Stimmung, unsere Vorlieben und unser Sozialleben. Anhand dieser Daten können Unternehmen aus der Datenwirtschaft akkurate Persönlichkeitsprofile erstellen und das Verhalten der Nutzer vorhersagen – und dadurch gezielt Einfluss ausüben („Mikrotargeting").

Privatsphäre versus Gratis-Dienstleistungen. Zahlreiche Nutzer sind in Bezug auf die Nutzung ihrer persönlichen Daten durchaus besorgt. Einer US-Umfrage zufolge scheint eine Mehrheit jedoch nach wie vor „Gratis"-Leistungen einem besseren Datenschutz vorzuziehen.[26] Dies hat sich auch im Nachgang des Cambridge Analytica-Skandals gezeigt: Die meisten Nutzer haben ihr Verhalten in den sozialen Medien nicht wesentlich bzw. nicht dauerhaft geändert.[27]

Im Prinzip wäre der Austausch von persönlichen Daten gegen „Gratis"-Leistungen als persönliche Entscheidung der Nutzer in einem freien Markt anzusehen, sofern sie über die entsprechenden Bedingungen im Bilde sind. Angesichts einiger Faktoren stellt sich allerdings die Frage, inwieweit die Nutzer wirklich freiwillig ihre Zustimmung erteilen. Zahlreiche Dienste und Geräte schränken die Wahlfreiheit der Nutzer in Bezug auf die Kontrolle ihrer eigenen Daten und den Schutz ihrer Privatsphäre merklich ein. Wenn man nicht digital abstinent leben will, ist es praktisch unmöglich, eine regelmäßige Verfolgung im Internet und eine Sammlung persönlicher Daten zu vermeiden. Rechtliche Hinweise und Nutzungsbedingungen werden häufig absichtlich vage, breit gefächert und ausführlich gefasst, was die Nutzer davon abhält, sie im Detail zu prüfen.[28] Deshalb ist den Nutzern häufig nicht klar, in welchem Umfang sie Dienstanbietern gestatten, auf ihre Daten zuzugreifen, diese zu verarbeiten und weiterzugeben. Auch Nutzer, die Wert auf ihre Privatsphäre legen, sehen zudem häufig keine Alternative zu wichtigen sozialen Netzwerken und Messaging-Diensten, wenn sie mit ihrer Familie, ihren Freunden und Bekannten in Kontakt bleiben wollen, und nehmen daher den entsprechenden Verlust an Privatsphäre widerstrebend in Kauf.

Europa ist beim Schutz der Privatsphäre ein Vorreiter. In Europa wurde im Jahr 2018 die Datenschutz-Grundverordnung (DSGVO) in Kraft gesetzt, um den Nutzern wieder mehr Kontrolle über ihre Daten zu verschaffen. Sie ist auf viele dieser Probleme eingegangen.[29] Aber um dieses Ziel wirklich erreichen zu können, muss die DSGVO noch besser mit anderen EU-Vorschriften zum Schutz der Privatsphäre verknüpft werden. Außerdem kann es nach wie vor mühselig und zeitaufwändig für die Nutzer sein, ihre Rechte durchzusetzen. Die DSGVO ist jedoch kein zahnloser Tiger. Möglicherweise könnten z.B. Facebook aufgrund der Verordnung Strafzahlungen in Milliardenhöhe drohen.[30]

Privatsphäre als öffentliches Gut. In der öffentlichen Diskussion geht es beim Thema Privatsphäre vor allem um Nutzerrechte und den Schutz persönlicher Daten. Unter politischen Gesichtspunkten ist das Thema jedoch viel umfassender. Durch die Konzentration von Nutzerdaten in den Händen einiger großer Unternehmen erhalten diese beispiellosen Zugang zu den Gedanken, Meinungen und Emotionen der Bürger. Auf der Grundlage dieser Daten können die Nutzer

[26] MarketWatch (19. Januar 2019).
[27] Facebook.
[28] Business Insider (15. November 2017)
[29] Körner, Kevin (2018). DSGV – Treiber oder Hemmschuh für Europas Datenwirtschaft? Deutsche Bank Research. Aktueller Kommentar.
[30] Wall Street Journal (12. August 2019).

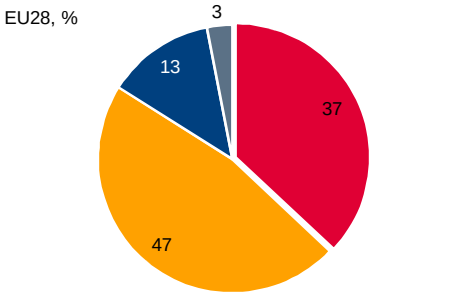
zum Gegenstand genau auf sie zugeschnittener Versuche der Einflussnahme werden, ohne dass ihnen dies bewusst wäre oder dass sie dem zugestimmt hätten. Sowohl in demokratischen als auch in autoritären Gesellschaften können diese Kenntnisse über und der Einfluss auf die Nutzer nicht nur zu wirtschaftlichen, sondern auch zu politischen Zwecken genutzt werden. Damit geht es beim Schutz der Privatsphäre und dem Eigentum an Daten nicht mehr nur um individuelle Rechte und Entscheidungen, sondern auch um ein öffentliches Gut.

Schwindende Sensibilisierung. Außerdem besteht das ernstzunehmende Risiko, dass die Sensibilität der Nutzer in Bezug auf Verstöße gegen den Datenschutz und unerlaubtes Eindringen in die Privatsphäre schwindet oder dass sie (in den Worten von Shoshana Zuboff) „psychisch abgestumpft" werden.[31] Möglicherweise gewöhnen sich die Nutzer an den Eindruck, dass Datenmissbrauch und Verstöße gegen den Datenschutz unvermeidlich sind und dass es zu den Vorrechten der entsprechenden Unternehmen gehört, umfassend Daten zu sammeln. Oder die Nutzer gelangen zu dem Schluss, dass der Schutz der Privatsphäre für sie zu kostspielig ist. Da sie kurzfristig eine Präferenz für „Gratis"-Leistungen hegen, sehen sie möglicherweise die damit einhergehenden langfristigen Kosten nicht. Und wenn sie sich daran gewöhnen, dass private Unternehmen ihre Daten horten und analysieren, verringern sich vielleicht auch ihre Bedenken, wenn Regierungen und Behörden diesem Beispiel folgen.

In autoritären Ländern haben die Nutzer vielleicht keine große Wahl … und möglicherweise trifft dies auch auf Demokratien zu. Insbesondere in demokratischen Staaten mit schwach ausgeprägten Kontrollmechanismen und mangelhafter Gewaltenteilung könnte dies zu einem ernsthaften Problem werden: Sowohl gewählte Regierungen als auch politische Gruppierungen insgesamt könnten in Versuchung geraten, diese Daten zu nutzen, um ihre Macht zu sichern, die Wähler zu manipulieren und Widerspruch und Opposition zu unterdrücken.

Aber nur 13% lesen die komplette Datenschutzerklärung 11

EU28, %



Umfrage: „Wenn Sie über Datenschutzerklärungen im Internet nachdenken, welcher der folgenden Sätze beschreibt am besten, was Sie normalerweise tun?"

Quelle: Special Eurobarometer 487a (June 2019)

Persuasive Technologien und Abhängigkeit von sozialen Medien

Bisher sind wir in dieser Studie davon ausgegangen, dass das Online-Verhalten der Nutzer und die Preisgabe ihrer Daten insgesamt auf freiwilligen Entscheidungen beruhen, auch wenn diese nicht unbedingt auf fundierter Basis getroffen werden. Es gibt jedoch einige Anzeichen dafür, dass zumindest manche Nutzer im Umgang mit ihren Smartphones und den darauf vorhandenen sozialen Medienplattformen ein zwanghaftes und spielsuchtähnliches Verhalten entwickeln.[32] Die Forschung zu diesem Thema steckt noch in den Kinderschuhen, konzentriert sich häufig auf Jugendliche und hat bislang keine eindeutigen Ergebnisse erzielt.

Einer Studie von Ofcom zufolge schauen die Briten tagsüber im Durchschnitt alle 12 Minuten auf ihr Handy. 34% fühlen sich ohne Internetzugang „abgeschnitten", 29% „verloren" und 17% finden eine solche Situation „stressreich".[33] Andere Studien haben erste Zusammenhänge zwischen der „Nutzung von Smartphones und gesteigerter Ängstlichkeit und Depression, Schlafstörungen und einem gestiegenen Risiko von Verletzungen und Todesfällen bei Autounfällen" gezeigt, wie Trevor Haynes von der Neurobiologie-Abteilung der Harvard Medical School schreibt.[34]

Programmierte Abhängigkeit? Falls soziale Medien und Smartphone-Apps tatsächlich Abhängigkeiten auslösen, wäre dieses „Suchtpotenzial" insofern noch brisanter, als es möglicherweise keine unabsichtliche Nebenwirkung ist. Nir Eyal, ehemaliger Lektor in Stanford und Behavioural Design-Spezialist aus dem

[31] Zuboff, Shoshana. (2019). The age of surveillance capitalism.
[32] Forbes (16. August 2019).
[33] Ofcom (2018). Communications market report.
[34] Haynes, Trevor (2018). Dopamine, smartphones & you: A battle for your time.

Silicon Valley, schreibt: „Die Produkte und Dienstleistungen, die wir gewohnheitsmäßig nutzen, verändern unser Alltagsverhalten – genauso wie ihre Schöpfer es beabsichtigt haben“.[35] Unternehmen investieren hohe Summen in Forschung und in Mitarbeiter, um Apps so zu gestalten, dass sie die Aufmerksamkeit der Nutzer maximieren und möglichst häufig verwendet werden. Ähnlich wie bei Spielautomaten wurden kleine Details wie z.B. die Farbe und die Verzögerung des Benachrichtigungssymbols von Facebook akribisch programmiert.[36]

Dopamingetriebene Feedbackschleifen sozialer Validierung. Dabei stützen sich die Unternehmen auf psychologische und neurochemische Erkenntnisse und nutzen gezielt unser angeborenes Bedürfnis nach sozialer Interaktion und Reziprozität. Inzwischen weiß man, dass positive soziale Interaktionen zu einem kräftigen Dopaminausstoß im menschlichen Gehirn führen können.[37] Soziale Netzwerke und andere Apps können dies nutzen, um die Wünsche und das Verhalten der Nutzer so zu modifizieren, dass diese ihre Interaktionshäufigkeit steigern. Laut Sean Parker, dem Gründungspräsident von Facebook, will sich Facebook mit Hilfe einer „Feedbackschleife sozialer Validierung“ die maximale „bewusste Aufmerksamkeit“ der Nutzer sichern. Diese Feedbackschleife wurde so entwickelt, dass sie eine „Schwachstelle der menschlichen Psychologie“ nutzt, indem sie den Nutzern „ab und an einen kleinen Dopaminstoß zukommen“ lässt.[38]

Laut Eyal können Unternehmen, welche „feste Gewohnheiten“ ihrer Nutzer prägen, ihre Produkte mit „internen Auslösern“ verknüpfen. Er bezeichnet dies als „hook“-Modell (im deutschen „Haken“, aber auch „süchtig“). Nach diesem Modell verwenden die Unternehmen die „alltäglichen Routinen und Emotionen“ der Nutzer, um durch „variable Belohnungen“ die Ausschüttung von Dopamin zu erhöhen. Dabei unterdrücken sie denjenigen Teil des Gehirns, in dem „Verstand und Urteilskraft“ angesiedelt sind, zugunsten desjenigen, der für „Wünsche und Begierden“ zuständig ist. Solche „gewohnheitsprägenden Produkte“ binden die Nutzer an die jeweiligen Dienstleistungen, verstärken den Auslöser für die nächste Interaktion und führen so zu beträchtlichen Wettbewerbsvorteilen.[39]

Die Wissenschaft der persuasiven Technologie. Diese Erkenntnisse werden als „Persuasive Technology“ oder „Captology“ an der Stanford University gelehrt, dem wissenschaftlichen Herz der Technologieinfrastruktur des Silicon Valley.[40] Das allgemeine psychologische Rahmenwerk wird von zahlreichen Internetseiten, Netzwerken und Apps angewendet. Ergänzt um die Daten derer Nutzer können diese so auf eine individuell zugeschnittene Weise angesprochen werden.

So werden die Nutzer etwa animiert, Produkte und Dienstleistungen zu kaufen, Inhalte zu teilen oder zu konsumieren oder ihr Verhalten zu ändern (z.B. „Nudging“ durch Gesundheits-Apps). Vor allem aber werden sie dazu veranlasst, mehr Zeit mit der App zu verbringen. Vor dem Hintergrund des Cambridge Analytica-Facebook-Skandals können diese Instrumente aber auch dazu verwendet werden, über menschliche Befürchtungen und Vorurteile die Meinungen und das Wahlverhalten der Nutzer zu beeinflussen.

Inwieweit steht dies mit der Frage nach den Auswirkungen der Technologie auf die Demokratie in Zusammenhang? Wenn die Nutzung von sozialen Medien potenziell abhängig machen kann, diese Abhängigkeiten absichtlich hervorgerufen werden und das Phänomen nicht nur eine marginale Zahl von Nutzern betrifft, könnte dies beträchtliche Folgen für die Demokratie haben. Dies könnte auch

[35] Eyal, Nir (2019). Hooked: How to build habit-forming products.
[36] The Guardian (6. Oktober 2017).
[37] Brent, Lauren J.N. et al. (2014). The neuroethology of friendship.
[38] Axios (2017). Sean Parker unloads on Facebook: “God only knows what it's doing to our children's brains”.
[39] Eyal, Nir (2019). Hooked: How to build habit-forming products.
[40] Fogg, B.J (2008). Mass Interpersonal Persuasion: An Early View of a New Phenomenon.

bedeuten, dass die Nutzer nicht in der Lage sind, ihr Social Media-Verhalten zu ändern, selbst wenn sie ein zunehmendes Bewusstsein und Missmut gegenüber Verletzungen ihrer Privatsphäre oder Manipulationsversuche entwickelt haben. Auf der gesamtgesellschaftlichen Ebene könnten demokratische Prozesse und der öffentliche Dialog dadurch übermäßig dem Einfluss begrenzter privater Interessen ausgeliefert sein. Chamath Palihapitiya, ehemals hochrangiger Manager bei Facebook, sieht gar eine Zerstörung der „Funktionsweisen der Gesellschaft" durch die „von uns geschaffenen kurzfristigen, dopamingetriebenen Feedbackschleifen".[41]

Technologieunternehmen fällt es schwer, darauf zu reagieren. Angesichts der zunehmenden Kritik und des Drucks von besorgten Eltern und Bürgerrechtsgruppen haben die Technologieunternehmen begonnen, sich mit dem Problem der übermäßigen Nutzung von Smartphones zu befassen. Apple z.B. bietet „Screen Time" an. Gleichzeitig schränkt Apple nach Berichten die Verfügbarkeit von externen Apps zur Kontrolle der am Bildschirm verbrachten Zeit bzw. zur Kontrolle durch Eltern in seinem App Store ein.[42]

Dies könnte illustrieren, wie schwer es den Technologieunternehmen fällt, ihr Geschäftsmodell anzupassen. Auch die politischen Entscheidungsträger reagieren inzwischen auf das Thema. In den USA wurde vor kurzem ein „Social Media Addiction Reduction Technology Act" in den Kongress eingebracht, der Social Media-Unternehmen dazu zwingen soll, „Maßnahmen zur Abmilderung des Risikos von Internetabhängigkeit und psychologischer Ausnutzung zu ergreifen". [43]

Erosion von Bürgerrechten durch algorithmische Voreingenommenheit („algorithmic bias")

Wir sind von prädiktiven Algorithmen umgeben, von der Autoplay-Funktion auf YouTube über Filmempfehlungen auf Netflix bis hin zu der Werbung, die bei Google-Suchanfragen gezeigt wird. Prädiktive Algorithmen werden häufig zur Entscheidungsunterstützung bei der Kreditvergabe, über Universitätszulassungen oder bei der Stellenvergabe, aber auch in der Polizeiarbeit, an Flughäfen, bei Grenzkontrollen oder bei juristischen Entscheidungen eingesetzt. Dabei wird davon ausgegangen, dass diese auf statistischer Datenanalyse basierenden Tools effizient arbeiten und frei von menschlichen Vorurteilen sind. Tatsächlich jedoch können Voreingenommenheiten oder diskriminierende Faktoren auf verschiedene Art und Weise in die Modelle der Algorithmen und damit auch die Ergebnisse eingehen.

Prädiktive Analyse können menschliche Voreingenommenheiten replizieren oder sogar verstärken. Wenn sich z.B. auf Algorithmen basierende Einstellungs-Tools auf historische Bewerbungsschreiben stützen, kann dies zur Bevorzugung eines Geschlechts führen; dies musste beispielsweise Amazon feststellen. Ebenso können Algorithmen, die US-Richter zur Einschätzung von Risiken verwenden und anhand derer sie Grenzwerte für Kautionen oder Strafen festlegen, Voreingenommenheiten fortschreiben, soweit sich nämlich in den in diese Algorithmen eingehenden Datensätzen historische Ungleichbehandlungen wie z.B. Rassendiskriminierung widerspiegeln.[44] Auch bei prädiktiver Polizeiarbeit, z.B. der National Data Analytics Solution (NDAS) in Großbritannien, kann der Einsatz von Algorithmen, die auf Polizeidaten über Personenkontrollen und -durchsuchungen beruhen, zur Fortschreibung historischer ethnischer Vorurteile bei

[41] Washington Post (12. Dezember 2017).
[42] New York Times (27. April 2019).
[43] Hawley, J (2019). Social Media Addiction Reduction Technology Act.
[44] Lee, Nicol Turner et al. (2019). Algorithmic bias detection and mitigation. Brookings.

Polizeieinsätzen führen.[45] Und wenn die Datensätze nicht hinreichend diversifiziert sind, werden Minderheiten u.U. diskriminiert, z.B. bei Gesichtserkennungssystemen an US-Flughäfen.[46]

Algorithmen als „Black Box". Darüber hinaus können auf maschinellem Lernen basierende KI-Systeme das „Black Box"-Problem mit sich bringen: Selbst die Entwickler können unter Umständen nicht ohne Weiteres nachvollziehen, wie ein Algorithmus zu seinen Ergebnissen kommt. Daraus entsteht ein weiteres Voreingenommenheitsrisiko, da potenziell diskriminierende Kriterien nicht so einfach zu erkennen sind.

Angesichts der schieren Verfügbarkeit der Daten und der raschen Fortschritte bei KI-Systemen wird eine prädiktive Analyse zunehmend eingesetzt werden – und zwar nicht nur von Unternehmen, Banken und Personalchefs, sondern auch von staatlichen Institutionen und Behörden. Wenn die damit verbundenen Mängel und Risiken nicht angemessen behoben werden, können technologisch begründete Verstärkung von Voreingenommenheiten und Vorurteilen sowie statistische Fehler und Irrtümer dazu führen, dass sich historische Ungleichbehandlungen verfestigen. Dies wiederum könnte den Schutz vor Diskriminierung aushöhlen und gegen den in den Verfassungen moderner Demokratien festgeschriebenen Gleichheitsgrundsatz verstoßen.[47]

Auswirkungen von KI und Automatisierung auf Wettbewerbsfähigkeit und die Unterstützung für die Demokratie

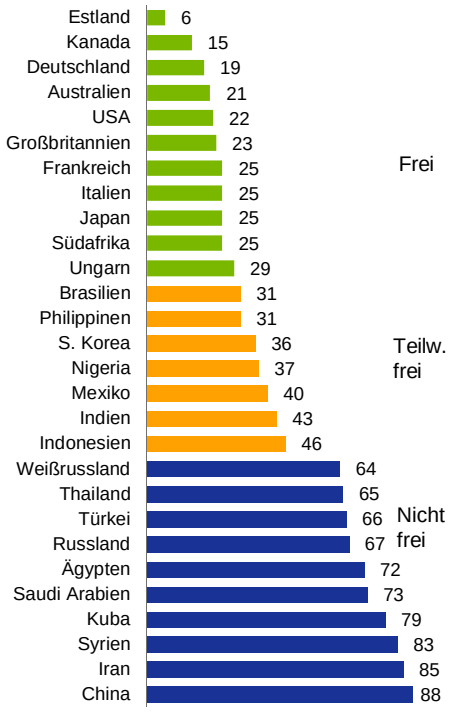
Die Demokratie ist darauf angewiesen, dass eine Mehrheit der Bevölkerung sie unterstützt. Dies gilt für das politische System an sich, beinhaltet aber auch eine informierte Teilhabe der Bürger und Wähler. Die Unterstützung der Demokratie durch ihre Bürger setzt allerdings auch voraus, dass deren wirtschaftlichen Bedürfnisse und Wünsche erfüllt werden. Deshalb sind Chancengleichheit sowie die Erhaltung der Wettbewerbsfähigkeit und des wirtschaftlichen Wohlstands einer demokratischen Gesellschaft von wesentlicher Bedeutung für ihre politische Stabilität und das Funktionieren ihrer Institutionen. Die steigenden Einkommensunterschiede und das Auseinanderdriften von Arbeits- und Kapitaleinkommen haben in zahlreichen westlichen Industrieländern bereits wachsende Unzufriedenheit ausgelöst. Diese Kluft könnte sich in den kommenden Jahren aufgrund der zunehmenden Automatisierung und des Einsatzes von KI noch vertiefen.[48]

Weil nicht klar ist, in welchem Umfang und in welchem Tempo sich die Arbeitsmärkte verändern werden, ist es besonders wichtig, sich auf die potenziellen Folgen der Automatisierung vorzubereiten.[49] Anderenfalls könnte die Stabilität von konsensbasierten demokratischen Systemen ernsthaft in Gefahr geraten. Wenn sich immer größere Teile der Bevölkerung Sorgen um ihre Existenz machen und ein Gefühl der Bedeutungslosigkeit bekommen, bereitet dies einen Nährboden für populistische, antidemokratische und autoritäre Strömungen, die in einer übermäßig komplexen Welt scheinbar einfache Lösungen anbieten.[50]

[45] Guardian (20. April 2019).
[46] CNET (8. Mai 2019).
[47] Europarat (2017). Algorithms and human rights.
[48] Heymann, Eric et al. (2018). Digitale Wirtschaft: Wie künstliche Intelligenz und Robotik unsere Arbeit und unser Leben verändern. Deutsche Bank Research. EU Monitor.
[49] Becker, Sebastian (2019). Digitaler Strukturwandel und der Sozialstaat im 21. Jahrhundert. Deutsche Bank Research. EU Monitor.
[50] Reid, Jim et al. (2019). Politik, Macht und Populismus. Deutsche Bank Research. Konzept.

Freiheit im Netz, globaler Vergleich 12

Freiheit im Netz Index (2018)



Quelle: Freedom House

Verschiebungen bei den globalen Wettbewerbsvorteilen. Die globalen Wettbewerbsbedingungen verändern sich im Zeitalter der Datenwirtschaft rasch. In der Vergangenheit hatten US-Technologiekonzerne auf diesem Gebiet einen beträchtlichen Vorsprung und konnten den globalen Markt rasch unter sich aufteilen. China reagierte darauf mit der Abschottung seiner Digitalwirtschaft und der Förderung eigener Technologiekonzerne; Europa ist bereits weit zurückgefallen. Insofern dürften künftig vor allem die USA und China um die Technologieführerschaft konkurrieren, wenn es Europa nicht gelingt, die Lücke zu schließen.

Autoritäre und zentralistisch organisierte Gesellschaften könnten zunehmend von einer weitreichenden Annahme und Entwicklung neuer Technologien wie z.B. künstliche Intelligenz oder Biotechnologie profitieren, deren Entwicklung in demokratischen Gesellschaften durch ethische und rechtliche Einschränkungen gebremst wird. Außerdem können solche Staaten in einem Umfang auf die Daten ihrer Bürger zugreifen, der mit den Normen demokratischer Gesellschaften nicht vereinbar ist. Dadurch wird einerseits die Entwicklung von KI, andererseits die Kontrolle der Gesellschaft verstärkt. Eine zentralistische Organisation galt vor dem Hintergrund der technologischen Entwicklung des 20. Jahrhunderts noch als ernsthafter Nachteil, könnte sich aber im Zeitalter der Datenwirtschaft als Vorteil erweisen.[51] Wenn KI den wirtschaftlichen Erfolg und die interne staatliche Kontrolle begünstigt, kann sie autoritären Regimen einen Vorteil gegenüber liberalen Demokratien verschaffen und damit die Position der ersteren in einem wieder aufflammenden Wettbewerb der politischen Systeme um die globale Vorherrschaft stärken. Gleichzeitig könnten solche Regimes dadurch die Lehren des Kalten Kriegs widerlegen, denen zufolge wirtschaftlicher Erfolg und eine liberale Demokratie untrennbar miteinander verbunden sind. Dies wiederum würde ein „autoritäres Modell“ für andere Länder attraktiver machen.[52]

China wird durch seinen wirtschaftlichen und technologischen Erfolg gestärkt und stellt sein System der autoritären Führung und des Staatskapitalismus zunehmend als überlegene Alternative zu westlichen Demokratien dar. Wenn die EU-Mitgliedstaaten und andere demokratische Länder auf dem Gebiet der digitalen und wirtschaftlichen Innovation zurückfallen, besteht das Risiko, dass autoritäre Strukturen auch hierzulande zunehmend akzeptiert werden. In einigen EU-Ländern scheint dies bereits der Fall zu sein.[53]

Massenüberwachung und Stärkung von autoritären Strukturen

Autokratische Regime haben rasch verstanden, welche Gefahren ein nicht zensiertes, offenes Internet für ihre politische Kontrolle und Stabilität birgt, aber auch, welche Chancen neue Technologien für staatliche Überwachung und Kontrolle bieten. Denn die Kombination aus Massendaten und fortgeschrittener (KI-)Technologie verschafft den Regierungen gänzlich neue Möglichkeiten, um die Bürger zu überwachen, zu beobachten, zu kontrollieren und zu beeinflussen. Ian Bremmer von der Eurasia Group bezeichnet dies als die „größte geopolitische Überraschung des vergangenen Jahrzehnts“: Gerade diejenige Technologie, die ursprünglich autoritäre Regimes anfälliger gemacht hatte, stützt sie jetzt durch „Big Data, Überwachung und Deep Learning“.[54]

Rasche Fortschritte bei KI-basierter Überwachungstechnologie. In den vergangenen zehn Jahren wurden bei Überwachungstechnologien beträchtliche Fortschritte erzielt. Die komplette elektronische Kommunikation, von E-Mail über Telefonanrufe, SMS, Messenger Apps, Social Media bis hin zum Zahlungsverkehr, kann überwacht werden. Anhand von Suchverläufen, mit Hilfe von Tracking

[51] Europarat (2017). Algorithms and human rights.
[52] Wright, Nicholas (2018). How Artificial Intelligence Will Reshape The Global Order. Foreign Affairs.
[53] Benner, Thorsten et al. (2018). Authoritarian Advance. GPPi and merics.
[54] Foreign Affairs (12. Februar 2019).

Tools und über Logins auf Social Media-Seiten können Nutzer in der virtuellen Welt nachverfolgt und ihre Daten zu individuellen Profilen zusammengefasst werden. Diese Profile können dann psychometrisch analysiert und mithilfe von Algorithmen kategorisiert werden.

Mithilfe von Fortschritten bei der KI-basierten Überwachungstechnologie, z.B. Gesichts-, Stimm- und Bewegungserkennung, und eines Netzes aus Überwachungskameras an öffentlichen Orten können Personen auch in der realen Welt verfolgt werden. Wie bei anderen Technologien können auch Überwachungsinstrumente in Kombination mit einer prädiktiven Analyse einerseits dazu dienen, die Sicherheit zu erhöhen oder den Verkehrsfluss zu verbessern, und es andererseits Regierungen ermöglichen, große Menschenmengen zu kontrollieren und das Aufkommen von Protesten oder Aufständen vorherzusagen.

Gänzlich neue Möglichkeiten für staatliche Kontrolle. Autoritäre Staaten können solche Instrumente nutzen, um abweichende Meinungen bereits in einem frühen Stadium zu erkennen und zu unterbinden und die Bildung von Oppositions- oder Bürgerrechtsgruppen zu verhindern, welche die Konzentration der politischen und wirtschaftlichen Macht in den Händen einer herrschenden Elite infrage stellen könnten. Da sich autoritäre Regierungen Zugang zu allen von privaten Unternehmen gesammelten und gespeicherten Informationen und Daten verschaffen können (die ohnehin häufig nicht klar von der Regierung getrennt sind), können sie so alle Lebensbereiche ihrer Bürger überwachen und kontrollieren. Durch das Internet der Dinge, zu dem auch verschiedenste „smarte Geräte“ gehören, die audiovisuelle und sonstige Sensoren an privaten und öffentlichen Orten einsetzen, kann das Überwachungsnetz noch engmaschiger gestaltet werden. Auch Sozialkredit-Systeme sind mächtige Instrumente, die Selbstzensur und präventiven Gehorsam fördern; gleichzeitig können kritische Bürger aus dem gesellschaftlichen und wirtschaftlichen Leben ausgeschlossen werden. In Kombination mit Zensur sowie einer Abschottung des Internets und der Kontrolle der Informationsströme über Nachrichtenplattformen und soziale Medien ermöglichen diese Tools eine Entwicklung, die zuweilen als „Aufschwung des digitalen Autoritarismus“ bezeichnet wird.[55]

Dass Überwachungstechnologien für verschiedene Zwecke genutzt werden können, erschwert es häufig, zwischen zivilen bzw. polizeilich gebotenen Anwendungen einerseits und politischer Unterdrückung andererseits zu unterscheiden. Eine Überwachungsinfrastruktur, die zur Verkehrslenkung oder Verbrechensbekämpfung dient, kann ebenso als Instrument zur Unterdrückung oder Bekämpfung der Opposition eingesetzt werden.

China ein Vorreiter bei Überwachungstechnologie. Bei der Entwicklung und Einführung von Überwachungstechnologie wie z.B. Gesichtserkennung nimmt China eine weltweite Führungsposition ein. Die beiden bestfinanzierten KI-Unternehmen in China sind im Überwachungsbereich tätig.[56] Im Zuge seiner KI-Strategie für 2030 hat China landesweit laut einem CNBC-Bericht rund 200 Millionen Überwachungskameras installiert.[57] Reuters zufolge werden in der autonomen Region Xinjiang im Nordwesten des Landes die Bewegungen von über zwei Millionen Menschen durch chinesische Überwachungsunternehmen verfolgt.[58] Außerdem wurde berichtet, die chinesische Polizei habe bei Routine-Sicherheitsmaßnahmen, z.B. in der U-Bahn, Datenextraktions-Software auf privaten Smartphones installiert.[59] Nahezu alle 1,4 Milliarden chinesischen Staatsbürger sind in einer Gesichtserkennungs-Datenbank registriert.[60] China plant, bis 2020 ein landesweites Sozialkredit-System einzuführen, das derzeit in mehreren

[55] Freedom House (2018). Freedom on the net 2018.
[56] CBInsights (6. Februar 2019).
[57] CNBC (16. Mai 2019).
[58] Reuters (17. Februar 2019).
[59] Financial Times (4. Juli 2019).
[60] CNBC (16. Mai 2019).

Städten getestet wird. Dies hat weltweit Aufmerksamkeit erregt und Besorgnis hervorgerufen. Das System erteilt anhand des Verhaltens der Bürger in verschiedenen Lebensbereichen Scores und bestraft oder belohnt sie entsprechend. So kann den Menschen z.B. der Zugang zu bestimmten Verkehrsmitteln, Versicherungen oder Anlageprodukten verwehrt werden.[61]

Verbreitung von Überwachungstechnologie. Chinesische Unternehmen sind auch maßgebliche Exporteure für Überwachungstechnologie in andere Länder und an andere Sicherheitsbehörden, etwa im Rahmen von Chinas „Belt and Road"-Initiative, aber auch darüber hinaus. Laut Steven Feldstein von der Boise State University hat China KI-Überwachungstechnologie an über 50 Staaten geliefert, darunter Malaysia, Singapur und Simbabwe oder Serbien. Die Einführung von Überwachungstechnologie ist damit inzwischen ein globales Phänomen.[62] Laut Feldstein „zeigt sich rund um die Welt, wie KI-Systeme potenziell repressive Regimes unterstützen und so die Beziehung zwischen Bürgern und Staat grundlegend verändern können, wodurch der Autoritarismus weltweit wieder an Boden gewinnt". Nach Auffassung der Studie ist der Export von KI-Technologie an autoritäre Regimes als zentrales Element der chinesischen Geopolitik anzusehen. Laut Feldstein ermöglichen es Technologien wie Gesichtserkennung auf der Grundlage von umfangreichen Datenbanken und fortgeschrittenem Maschinellen Lernen „autoritären Bestrebungen auf ganz andere Weise, den Diskurs zu bestimmen und Opposition zu unterdrücken".

Im Gegensatz zu autoritären Ländern wird die extensive Nutzung von Überwachungstechnologien in demokratischen Staaten häufig durch Gesetze und öffentlichen Widerstand eingeschränkt. Auch in Demokratien besteht für die Regierungen jedoch ein Anreiz, solche Technologien zur Terrorismus- und Kriminalitätsbekämpfung einzusetzen. Durch Terroranschläge und Verbrechen kann sich öffentliche Meinung zugunsten solcher Anwendungen ändern.[63] Die USA haben im Rahmen eines Pilotprojekts an Grenzübergängen zu Mexiko Gesichtserkennungstechnologie eingesetzt und zur Bestätigung der „biometrischen Ausreise" an Flughäfen ein Gesichtserkennungssystem für die Passagiere eingeführt.[64] Auch in anderen Ländern wie z.B. Deutschland, Großbritannien oder Japan wird Gesichtserkennungstechnologie an öffentlichen Orten eingesetzt oder getestet.[65]

Ausgleich zwischen Sicherheit und Schutz der persönlichen Rechte. In Ländern mit starken demokratischen Institutionen muss bei der Einrichtung einer umfassenden Überwachungsinfrastruktur ein Ausgleich zwischen öffentlicher Sicherheit einerseits und dem Schutz der persönlichen Rechte und Freiheiten andererseits gefunden werden. Parlamentarische und richterliche Kontrolle ist eine Voraussetzung dafür, dass das Risiko eines Missbrauchs durch Politiker und Behörden präventiv verhindert wird. Außerdem ist zu prüfen, welche Rolle private Unternehmen bei der Sammlung und Analyse von Daten spielen – und zwar im Hinblick auf ihre Zusammenarbeit sowohl mit staatlichen Stellen als auch mit in- und ausländischen Dritten.

Überwachungstechnologien können in anfälligen demokratischen Gesellschaften, die sich bereits auf dem Weg hin zu stärker autoritär geprägten Strukturen befinden, ein Risiko für die Demokratie darstellen. Dies zeigt sich in Schwellenländern in Asien, Afrika und Lateinamerika ebenso wie in einigen EU-Ländern.

[61] The Guardian (1. März 2019).
[62] Feldstein, Steven (2019). China is exporting AI surveillance technology to countries around the world. Newsweek (23. April 2019) und Reuters (2. August 2019).
[63] In Deutschland sprachen sich in einer Umfrage im Jahr 2018 87% der Befragten für eine Videoüberwachung von öffentlichen Orten aus. Nur 10% sehen dies als übermäßigen Eingriff in die Privatsphäre an (Forsa, 2018).
[64] The Verge (18. April 2019).
[65] Politico (24. Juni 2019) , Der Spiegel (12. Oktober 2018) und Reuters (13. August 2019).

Dort könnten die Regierungen zunehmend Überwachungstechnologien einsetzen, um die „Aktivitäten politischer Gegner und der Zivilgesellschaft zu beobachten und präventiv gegen mögliche Herausforderungen für ihre Autorität vorzugehen“.[66]

Überwachungsverbote und Grenzen der Überwachung. Zum Schutz der Bürgerrechte wurden in einigen Ländern bzw. Regionen bereits politische Maßnahmen ergriffen, um das Missbrauchsrisiko zu verringern. So wurde z.B. der Einsatz von Gesichtserkennungssoftware durch die Polizei und andere staatliche Stellen in den US-Städten San Francisco, Somerville und Oakland verboten.[67] Ein US-Gericht hat vor Kurzem entschieden, dass Nutzer gerichtlich gegen Facebook vorgehen können, wenn der Konzern ihre Gesichtsdaten ohne ausdrückliches Einverständnis für seine Gesichtserkennungssoftware nutzt.[68] Europa, das bei der KI-Entwicklung hinter China und den USA zurückliegt, nimmt beim Datenschutz sowie bei der Festlegung von ethischen Standards und Vorgaben in Bezug auf Überwachungstechnologie eine Vorreiterrolle ein. Die Expertengruppe der EU-Kommission erklärte in ihren „Leitlinien für eine vertrauenswürdige KI“ in Europa, dass „Einzelne nicht in ungerechtfertigter Weise mithilfe KI-gestützter biometrischer Erkennungsmethoden persönlich, physisch oder mental nachverfolgt oder identifiziert, ihr Profil erstellt oder sie Objekt von Nudging-Bemühungen (...) werden dürfen“. Der „Einsatz solcher Technologien in Ausnahmefällen, z.B. zu Zwecken der nationalen Sicherheit, muss evidenzbasiert, erforderlich und verhältnismäßig sein und Grundrechte respektieren“.[69]

Dringend erforderlich: Eine Gesellschaft mit digitaler Grundbildung

Die digitale Transformation wirkt sich auf alle Aspekte des privaten und öffentlichen Lebens aus, und zwar sowohl in Demokratien als auch in eingeschränkten Demokratien oder autoritären Staaten. Angesichts des Tempos des digitalen Wandels, des Mangels an vergleichbaren Entwicklungen, der Komplexität und häufig auch der subtilen Natur der Veränderungen ergeben sich beträchtliche Herausforderungen für Regierungen und Bürger.

Die Technologie ist an sich neutral, ihre Anwendung ist es nicht. Die globale Vernetzung und der rasche technologische Fortschritt bieten zweifelsohne Chancen und Vorteile. Gleichzeitig müssen wir jedoch besser verstehen, in welchem Umfang sich dies auf den politischen Dialog und die Interaktion zwischen Staaten und Wählern auswirken kann. Die Technologie selbst ist in Bezug auf ihren möglichen Gebrauch bzw. Missbrauch neutral, die politischen Verantwortungsträger und die Unternehmen, die besagte Technologie kontrollieren, sind es jedoch nicht.

Technologie und Demokratie sind weiterhin kompatibel. In dieser Studie haben wir uns mit den Risiken und Chancen befasst, die die digitale Transformation des vergangenen Jahrzehnts mit Blick auf die Demokratie mit sich bringt. Die Vorteile der Datenwirtschaft und des technologischen Fortschritts in Schlüsselbereichen wie KI und Automatisierung sind unseres Erachtens vollumfänglich mit einer stabilen, dynamischen und wohlhabenden demokratischen Gesellschaft vereinbar, die auf liberalen Werten und dem Schutz der Rechte und Freiheiten des Einzelnen beruht. Wie im vergangenen Jahrhundert können Technologie und Kommunikation weiterhin eine wichtige Rolle spielen, um den Bürgern

[66] Feldstein, Steven (2019). The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression. Journal of Democracy, Januar 2019.
[67] New York Times (14. Mai 2019) und Vox (18. Juli 2019).
[68] Reuters (8. August 2019).
[69] EU-Kommission (26. Juni 2019). EU policies – delivering for citizens: Digital transformation.

mehr Einfluss zu verschaffen, den gesellschaftlichen Diskurs zu bereichern und demokratische Institutionen zu stärken.

Dafür müssen demokratische Gesellschaften auf die Nebenwirkungen und Risiken der Technologie für ihre Institutionen sowie für Bürgerrechte reagieren, sei es nun im In- oder im Ausland. Die Regierungen müssen die regulatorischen Vorgaben, Wettbewerbsvorschriften und die staatliche Aufsicht so überarbeiten, dass sie den neuen Anforderungen der Datenwirtschaft gerecht werden. Die Unternehmen ihrerseits müssen sicherstellen, dass ihre Geschäftsmodelle und Produkte im Einklang mit den in der Verfassung garantierten Rechten und mit der Integrität demokratischer Institutionen und Prozesse stehen.

Und die Nutzer und Bürger müssen die Algorithmen und das Design hinter ihren Apps und Geräten sowie die zugrundeliegenden Mechanismen der Datenwirtschaft besser verstehen. Die demokratischen Gesellschaften müssen einen fundierten Dialog über das Eigentum an Daten und Technologie führen und darüber, wie die Errungenschaften des technischen Fortschritts verteilt werden sollen und wie verhindert werden kann, dass eine zunehmend ungleiche Verteilung von Vermögen und Einfluss zur Destabilisierung ihrer eigenen Grundlagen führt.

EU spielt bei der Regulierung von KI und Datenwirtschaft eine Führungsrolle. Der EU und ihren Mitgliedstaaten mangelt es an großen Technologiekonzernen und sie haben Mühe, im globalen Wettlauf um die Führungsposition im KI-Bereich Schritt zu halten. Dieser Wettbewerb wird anscheinend vor allem zwischen den USA und China ausgetragen. Gleichzeitig scheint sich Europa den Herausforderungen, welche die neuen Technologien an demokratische Gesellschaften richten, besser zu stellen als andere Staaten.

In den vergangenen Jahren hat sich die EU als Vorreiter in Bezug auf entsprechende Regulierungen und Initiativen positioniert. Beispiele sind der Schutz der Privatsphäre und der Nutzerrechte (DSGVO), der Plan zur Bekämpfung von Desinformation oder die KI-Allianz – ein Multi-Stakeholder-Forum, das nicht nur KI-Investitionen und -Forschung fördern, sondern auch drängende ethische und rechtliche Fragen ansprechen soll. Es handelt sich dabei jedoch um einen Lernprozess: Immer wieder wird man Schwachstellen in den Vorgaben ausbessern und Schlupflöcher stopfen müssen. Regeln und Vorschriften müssen nach Bedarf so angepasst werden, dass ein guter Ausgleich zwischen wirtschaftlichen, gesellschaftlichen und politischen Aspekten gewährleistet ist. Aber die Grundbotschaft der EU ist klar: Technischer Fortschritt und die Datenwirtschaft gehören allen Bürgern.[70]

Kevin Körner (+49 69 910-31718, kevin.koerner@db.com)

[70] Europäisches Parlament (2019). Politische Maßnahmen der EU im Interesse der Bürger: Der digitale Wandel.

Deutsche Bank
Research

EU-Monitor

Unsere Publikationen finden Sie unentgeltlich auf unserer Internetseite www.dbresearch.de Dort können Sie sich auch als regelmäßiger Empfänger unserer Publikationen per E-Mail eintragen.

Für die Print-Version wenden Sie sich bitte an:
Deutsche Bank Research
Marketing
60262 Frankfurt am Main
Fax: +49 69 910-31877
E-Mail: marketing.dbr@db.com

Schneller via E-Mail:
marketing.dbr@db.com

Druck: HST Offsetdruck Schadt & Tetzlaff GbR, Dieburg

ISSN (Print): 1612-0256; ISSN (Online): 1612-0264