GLOBALE TRENDS ANALYSEN

Ahmed Maati

COVID-19 und digitaler Autoritarismus: Risiken erkennen, Gegenmaßnahmen ergreifen

02 **2022**

Impressum

Herausgegeben von
Stiftung Entwicklung und Frieden (sef:)
Dechenstr. 2, 53115 Bonn, Deutschland
Bonn 2022

Übersetzung: Angela Großmann
Design und Grafik: DITHO Design, Köln
Satz: Gerhard Süß-Jung (sef:)
Druck: DCM Druck Center Meckenheim GmbH
Papier: Umweltzeichen Blauer Engel
Gedruckt in Deutschland

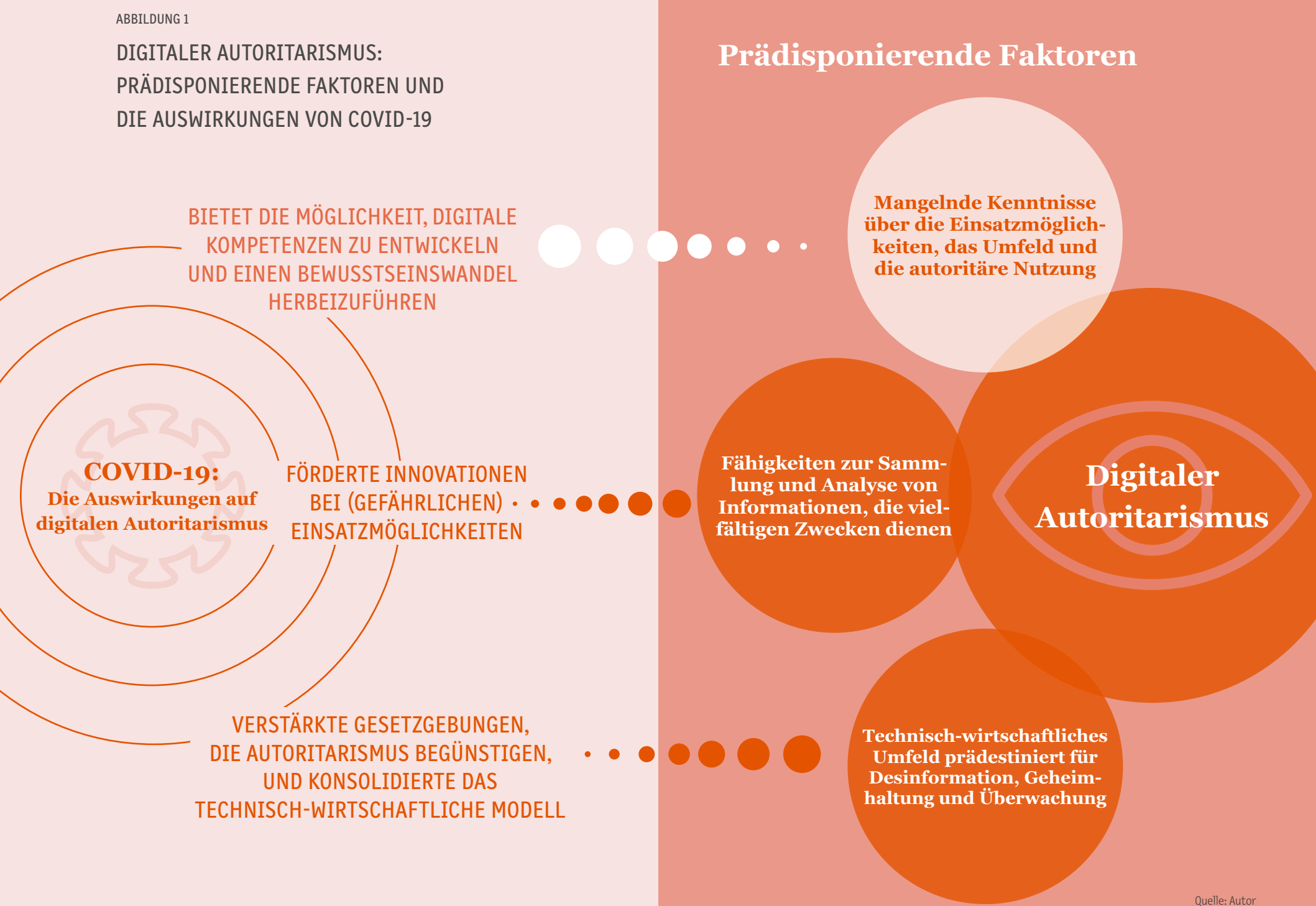
ISSN: 2568-8790

EINLEITUNG

Es besteht kein Zweifel daran, dass sich die Fortschritte im Bereich der digitalen Technologien positiv auf verschiedene Aspekte unseres Lebens ausgewirkt haben. Gleichzeitig haben die letzten Jahre gezeigt, dass solche Technologien weltweit die Privatsphäre und die Freiheit bedrohen können und selbst in etablierten Demokratien Unterdrückung und autoritäre Tendenzen fördern können. Insbesondere vor dem Hintergrund der COVID-19-Pandemie haben verschiedene Wissenschaftlerinnen und Wissenschaftler sowie Bürgerrechtsgruppen vor den zunehmenden Gefahren dieses „digitalen Autoritarismus“ gewarnt. Ich möchte drei Aspekte digitaler Technologien hervorheben, die sie anfällig für Autoritarismus machen: (i) die weitreichenden Möglichkeiten dieser Technologien, vor allem in Bezug auf ihre vielfältigen Verwendungszwecke, (ii) ihre Verankerung in einem bestärkenden Umfeld und (iii) das generell fehlende Wissen über die vielfältigen Möglichkeiten digitaler Technologien, deren technisch-ökonomische und rechtliche Einbettung sowie deren autoritäre Nutzung.
Während die Pandemie Diktatoren die Chance bietet, die autoritäre Nutzung digitaler Technologien zu etablieren und zu normalisieren, können Demokratien sie dazu nutzen, das Bewusstsein dafür zu schärfen, dass diese Technologien Gefahren beinhalten und Autoritarismus begünstigen können. Dies kann wiederum Bürgerinnen und Bürger sowie politische Entscheidungsträgerinnen und -träger dafür sensibilisieren, angemessene Maßnahmen zu ergreifen, um den autoritären Tendenzen dieser Technologien entgegenzuwirken.

ABBILDUNG 1

DIGITALER AUTORITARISMUS:
PRÄDISPONIERENDE FAKTOREN UND
DIE AUSWIRKUNGEN VON COVID-19



Quelle: Autor

1. DIGITALE TECHNOLOGIEN UND AUTORITARISMUS

1.1 DIGITALE TECHNOLOGIEN, AUTORITARISMUS UND AUTORITÄRE PRAKTIKEN

Der Begriff „digitaler Autoritarismus“ ist nicht unproblematisch. Technisch gesehen betrachtet die Politikwissenschaft Autoritarismus als eine bestimmte Form eines politischen Regimes, d. h. als eine Reihe von Vorschriften, die den Zugang zu politischer Macht regeln sowie das Verhältnis zwischen denen, die an der Macht sind, und denen, die nicht an der Macht sind (Fishman 1990, S. 428). Über die genaue Definition von Autoritarismus besteht kein Konsens. Die Fachwelt ist gespalten. Eine Mehrheit betrachtet Autoritarismus als das Nichtvorhandensein von Demokratie, während einige versuchen, eine konkretere Definition zu finden. Bei vielen grundlegenden Merkmalen, wie Macht und Politik in autoritären Regimen funktionieren, besteht mehr Konsens. Um die Risiken und Gegenmaßnahmen identifizieren zu können, konzentriere ich mich auf die für autoritäre Regime charakteristischen Merkmale, untersuche, wie digitale Technologien mit diesen Merkmalen in Verbindung stehen, und bewerte dann die Auswirkungen von COVID-19 auf diese Aspekte.

Der Autoritarismus regelt Vieles auf unzulässige Weise – allem voran den Zugang zur Macht, der hier nicht durch freie und faire Wahlen geregelt ist. Doch freie und faire Wahlen sind noch nicht alles. Sie sind zwar wichtig, machen aber allein noch kein demokratisches Regime aus. Autokraten, die nach politischem Machterhalt streben, müssen die Überzeugungen und das Verhalten ihrer Staatsbürger und Staatsbürgerinnen kennen, beeinflussen und kontrollieren (Schlumberger et al. 2022). Dies führt bei autoritären Regimen automatisch zu einer weitreichenden Verletzung der bürgerlichen und politischen Rechte, unter anderem durch massive Unterdrückung, fehlende Rechenschaftspflicht und exzessive Überwachung.

Zwar sind viele dieser autoritären Tendenzen auch bei einigen Akteuren in Demokratien zu beobachten, unterscheiden sich jedoch dadurch, dass diese Missstände in Demokratien nicht die Logik der politischen Herrschaft verkörpern. Daher ist es sinnvoll, diese Tendenzen in Demokratien als „autoritäre Praktiken“ zu definieren, durch die „die Rechenschaftspflicht gegenüber den Menschen, über die ein politischer Akteur die Kontrolle ausübt, oder ihren Vertreterinnen und Vertretern, durch Geheimhaltung, Desinformation und die Ausschaltung der Mitsprache sabotiert wird“ (Glasius 2018, S. 515; diese und alle weiteren Zitate im Original Englisch). Im Folgenden werden drei Merkmale digitaler Technologien diskutiert, die autoritäre Praktiken oder Autoritarismus begünstigen. Digitaler Autoritarismus und seine oben genannten Missstände werden demnach durch die Digitalisierung bzw. durch digitale Technologien gefördert.

1.2 WIE DIGITALE TECHNOLOGIEN DEN AUTORITARISMUS BEGÜNSTIGEN

(i) Die großartigen Möglichkeiten, mithilfe digitaler Technologien Daten zu sammeln, zu analysieren und Prognosen zu erstellen, machen diese für autoritäre Regime und autoritäre Akteure in Demokratien gleichermaßen sehr attraktiv. Sie bieten (Möchtegern-)Diktatorinnen und Diktatoren die Möglichkeit, in bisher ungekanntem Maße Erkenntnisse über die Bürgerinnen und Bürger zu gewinnen und diese gleichzeitig zu unterdrücken und zu kontrollieren. Viele Technologien ermöglichen es, verdeckt und im Geheimen zu agieren und sich so der Aufsicht und Rechenschaftspflicht zu entziehen. Dies gilt umso mehr, da die meisten Technologien vielseitig eingesetzt werden können. Einige ermöglichen es Diktaturen sogar, gleichzeitig zu überwachen, zu unterdrücken und zu kontrollieren. Es gibt bereits weit verbreitete und kommerziell verfügbare Einsatzmöglichkeiten, während sich andere noch in der Entwicklungs- und Erforschungsphase befinden.

In den letzten Jahren haben digitale Technologien gezeigt, wie mit ihnen umfangreiche Informationen über Personen gesammelt und diese Daten psychometrisch genutzt werden können, um das Verhalten und die Überzeugungen von Individuen zu beeinflussen. Indem sie die Interaktionen von Benutzerinnen und Benutzern mit einer Facebook-Anwendung auswertete, erstellte die Firma Cambridge Analytica einen großen Datensatz über „Dutzende Millionen Benutzerinnen und Benutzer“, der dann zur Beeinflussung ihres Wahlverhaltens genutzt wurde (Confessore 2018). Einige Schadsoftwareprogramme können Smartphones im Verborgenen in Live-Überwachungsgeräte verwandeln und hinterlassen kaum Spuren. Pegasus ist ein weithin bekanntes Beispiel dafür: 2019 enthüllte Facebook, dass eine Sicherheitslücke in der WhatsApp-Anwendung 1.400 Telefone für Pegasus zugänglich machte (Simpson 2019). Pegasus, das als die „unmögliche Spionagesoftware“ bezeichnet wird, ist in mindestens 45 Ländern im

Einsatz und kann nur schwer nachgewiesen werden (Marczak et al. 2018). Wird die Software entdeckt, zerstört sie das infizierte Gerät, ohne Spuren zu hinterlassen (Lookout Security 2017). Pegasus wurde auch eingesetzt, um verschiedene Aktivistinnen und Aktivisten auf der ganzen Welt zu überwachen (Priest et al. 2021). Durch künstliche Intelligenz (KI) wurden diese Möglichkeiten besonders erfolgreich weiterentwickelt. Algorithmen können so trainiert werden, dass sie nicht nur Personen in Echtzeit identifizieren, sondern auch ihr Verhalten vorhersagen können (und manchmal sogar diese Prognosen noch übertreffen). Im Jahr 2017 war eine Google-KI sogar in der Lage, das Verhalten eines Go-Champions vorherzusagen und ihn in diesem komplexen Spiel zu besiegen (BBC 2021).

Es gibt noch weitere beunruhigende Funktionen, wobei das Ausmaß ihres Einsatzes unklar ist. Mehrere Forschungsarbeiten dokumentieren die erfolgreiche Nutzung von WLAN-Wellen in normalen Routern, um die Anzahl der Personen in einem Raum zu identifizieren (Alam Nipu et al. 2018; Cushman et al. 2016). Darüber hinaus waren manche Studien in der Lage, Personen anhand ihres Gehstils zu ermitteln, der eindeutig identifizierbare Störungen in den Wellensignalen erzeugte, und zwar mit einer Genauigkeit von 94,5 % in einem Raum mit zwei Personen und 88,9 % in einem Raum mit sechs Personen (Xin et al. 2016). Andere Forschungsarbeiten nutzten Radiowellen, um die Bewegungen und Handschriften von Personen hinter dicken Wänden zu identifizieren, ohne dass zusätzliche Geräte im überwachten Raum verwendet werden mussten (Ding et al. 2021; Guo et al. 2020). Mit einer ähnlichen Technologie waren wiederum andere Forscher und Forscherinnen in der Lage, Personen hinter Wänden zu „hören“, indem sie die durch Lippenbewegungen verursachten Wellenstörungen analysierten (Wang et al. 2016). Andere identifizierten Tastenanschläge auf Tastaturen mit einer Genauigkeit von mehr als 93 % (Ali et al. 2015). Invasivere Technologien sammeln und analysieren Daten über direkte Gehirn-Computer-Schnittstellen. Im Jahr 2017 bewilligte die Defense Advanced Research Projects Agency (DARPA) Forschungsmittel für die Entwicklung von Gehirnimplantaten, die die Signale von 1 Mio. menschlicher Neuronen gleichzeitig aufzeichnen (DARPA 2017; Miranda et al. 2015; Murphy 2017). Es gibt keine verlässlichen Einschätzungen darüber, wie umfassend diese Einsatzmöglichkeiten genutzt werden; ihre bloße Existenz spricht jedoch für eine bisher beispiellose Bereitschaft, Daten zu sammeln und zu analysieren, um das Verhalten und die Überzeugungen von Personen zu beeinflussen und vorherzusagen.

Die vielseitig nutzbaren digitalen Technologien können sehr unterschiedlich eingesetzt werden, was im Falle einer unrechtmäßigen Nutzung auch die Geheimhaltung und Vermeidung einer Rechenschaftspflicht erleichtert. Überwachungstechnologien können beispielsweise sowohl der Strafverfolgung dienen als auch die Rechte auf Privatsphäre verletzen. Der Algorithmus, der einer medizinischen Diagnosesoftware zugrunde liegt, könnte auch zur Gesichtserkennung genutzt werden. Technologien, die digitale Implantate zur Erfassung, Analyse oder Beeinflussung neuronaler Signale nutzen, um Prothesen für Amputationsopfer besser zu steuern, können auch zur Überwachung und Kontrolle des Verhaltens und der Entscheidungen von Individuen eingesetzt werden.

Regierungsbehörden können daher digitale Technologien für vermeintlich legitime Zwecke erwerben oder entwickeln, während sie gleichzeitig deren unzulässige Nutzung verschleiern. Bekannt wurde hier die digitale Überwachungsfunktion von Pegasus. Sowohl die Entwickler – die NSO-Gruppe – als auch Regierungen behaupten offiziell, dass die Software ausschließlich zu Strafverfolgungszwecken eingesetzt wird (Priest/Dwoskin 2021). In der Praxis wurde Pegasus jedoch sowohl in Demokratien als auch in Autokratien zur Überwachung und Unterdrückung von Aktivistinnen und Aktivisten sowie von Kritikerinnen und Kritikern eingesetzt (Kenyon 2019). Digitaler Autoritarismus entzieht sich jeglicher Rechenschaftspflicht, und zwar nicht nur wegen der Geheimhaltung, sondern auch, weil die jeweilige Verantwortung von Unternehmen und Regierungen unklar geregelt ist. Letztere behaupten, Technologien für legitime Zwecke einzusetzen, während Entwicklerinnen und Entwickler die zugrundeliegende Technologie ursprünglich möglicherweise für medizinische oder andere legitime Zwecke entwickelt haben.

Die oben beschriebene Problematik der weitreichenden und autoritäre Strukturen begünstigende Vielseitigkeit der digitalen Technologien wird verstärkt durch (ii) ein Umfeld, das auf die Verletzung der Privatsphäre und fehlende Transparenz und Kontrolle ausgerichtet ist. Dieses ebenfalls den Autoritarismus fördernde Umfeld besteht aus einer technisch-wirtschaftlichen und einer rechtlichen Ebene. Auf der technisch-wirtschaftlichen Ebene hängt der Profit, den sowohl digitale Dienste als auch die ihnen zugrundeliegenden Technologien erwirtschaften, von der Erfassung und Analyse großer Mengen von Nutzerdaten ab (Saglam 2022). Dies gilt nicht nur für den Überwachungskapitalismus (Zuboff et al. 2019). Wie analoge Dienste profitieren auch digitale Dienste – von sozialen Medien bis zu Musikanwendungen –

von Werbeeinnahmen. Sie sammeln und analysieren Daten, um individuelle Vorlieben und Konsumgewohnheiten zu ermitteln. So werden Nutzerinnen und Nutzer z. B. länger auf Musikplattformen gehalten, indem Musik vorgeschlagen wird, die deren Vorlieben entspricht oder um neue Nutzerinnen und Nutzer zu gewinnen, was wiederum die Werbeeinnahmen erhöht. Sie können die Daten auch an Dritte verkaufen, die sie ebenfalls gewinnbringend verwerten. Analysen von Markttrends hat es zwar schon immer gegeben, durch algorithmische Verfahren werden diese jedoch in nie dagewesener Weise verbessert und automatisiert. Die Algorithmen selbst müssen anhand von großen Datenmengen trainiert werden. Je mehr Daten sie erzeugen und analysieren, desto besser können die Nutzer und Nutzerinnen gezielt angesprochen werden, und desto mehr Gewinn wird erzielt.

Dieses technisch-wirtschaftliche Umfeld ermöglicht nicht nur eine noch nie dagewesene Überwachung und Kontrolle, sondern begünstigt auch Desinformation. Der wirtschaftliche Anreiz, Daten zu generieren, zu sammeln und zu analysieren, gepaart mit mangelnder Transparenz hinsichtlich der zu diesem Zweck verfolgten (algorithmischen) Strategien begünstigt Manipulation und die Verletzung der Privatsphäre, wie der Fall Cambridge Analytica zeigt. Digitalisierte Daten, die aus verschiedenen Quellen und auf verschiedenen Geräten zusammengetragen wurden, können auch übergreifend gelesen und analysiert werden. Durch diese Triangulierung von Informationen entsteht so ein immer genaueres Bild der Ansichten und des Verhaltens einzelner Personen. Um die Nutzung zu maximieren und mehr Nutzerdaten zu gewinnen, verbreiten einige Algorithmen sozialer Medien außerdem absichtlich Falschinformationen, da die Nutzer und Nutzerinnen so noch mehr Zeit auf ihren Plattformen verbringen (Van Cleave 2021).

Auf rechtlicher Ebene operieren digitale Technologien bisher in einem weitgehend unregulierten Umfeld, in dem viele Regierungen die Privatsphäre ihrer Bürger und Bürgerinnen legal verletzen können. Dies betrifft sowohl die Regulierung von Technologien und Diensten wie KI und soziale Medien als auch Vorschriften gegen staatlichen Missbrauch. Mehr als ein Viertel der 169 im Rahmen des Digital Society Project im Jahr 2021 untersuchten Länder ermöglicht es den dortigen Regierungen innerhalb ihres Rechtrahmens zumindest auf „viele“ verschiedene personenbezogene Daten im Internet zuzugreifen (Digital Society Project 2022) [Abbildung 2]. In einer Studie über 38 nationale KI-Strategien heißt es zwar, dass „in fast allen Strategien die Notwendigkeit erkannt wurde, sicherzustellen, dass potenzielle Schäden abgewendet werden“, dass aber „in den Strategien keine konkreten Angaben dazu gemacht wurden, *wie* dies in der Praxis aussehen sollte“ (Bradley et al. 2021, S. 27). Auch die Versuche, Tech-Giganten staatlich zu regulieren, führen in der Regel nicht zu einem besseren Schutz der Nutzergruppen (Shahbaz/Funk 2019, S. 11).

Dies sind nur einige wenige Beispiele für die rechtlichen und wirtschaftlichen Infrastrukturen, in die digitale Kapazitäten eingebettet sind. Die Nutzungsmöglichkeiten digitaler Technologien prädestinieren sie für den Autoritarismus, da sie die Manipulation von und heimliches Wissen und Kontrolle über einzelne Personen ermöglichen. Das Umfeld bietet den rechtlichen und wirtschaftlichen Rahmen dafür.

Und schließlich (iii) hindert ein allgemein fehlendes Bewusstsein für diese Merkmale, die digitale Technologien für Autoritarismus prädestinieren, Bürgerinnen und Bürger sowie die politisch Verantwortlichen daran, rechtzeitig Gegenmaßnahmen zu ergreifen. Die Öffentlichkeit erkennt die meisten autoritären Anwendungen digitaler Technologien erst, nachdem diese bereits Schaden angerichtet haben. So wurden beispielsweise die Überwachungspro-

ABBILDUNG 2
Rechtliche Rahmenbedingungen für den staatlichen Zugang zu Online-Daten
Inhalt der gesetzlichen Bestimmungen zum Schutz der Privatsphäre, 2021, 169 Länder (N = 179; für 10 Länder liegen keine Daten vor)

Quelle: Zusammenstellung des Autors, basierend auf dem Digital Society Project 2022 (http://digitalsocietyproject.org/data/).

gramme der Nationalen Sicherheitsbehörde der USA (National Security Agency, NSA) erst Jahre nach ihrem ersten Einsatz durch die Aussagen von Edward Snowden öffentlich bekannt. Das Debakel rund um Cambridge Analytica entstand erst, nachdem das Unternehmen zwei wichtige Wahlen in den USA und Großbritannien beeinflusst hatte. Die von der NSO entwickelte Spionagesoftware Pegasus geriet erst ins Visier der Öffentlichkeit, nachdem sie zur Unterdrückung von Aktivistinnen und Aktivisten sowie von Journalistinnen und Journalisten beigetragen hatte.

2. COVID-19, DIGITALE TECHNOLOGIEN UND AUTORITARISMUS

Die Pandemie hat insgesamt die Aspekte verstärkt, die digitale Technologien für den Autoritarismus prädestinieren. Sie hat die Entwicklung und den Einsatz gefährlicher digitaler Überwachungs- und Kontrollmöglichkeiten vorangetrieben und Investitionen in digitale Ressourcen und Funktionen begünstigt. Gleichzeitig konnten Regierungen nun rechtfertigen, die Privatsphäre der Bevölkerung legal zu verletzen, es wurden große Mengen digitaler Daten gesammelt, und digitale Desinformation breitete sich weiter aus. Da der „digitale Schatten“ der Pandemie weiterhin existiert (Shahbaz/Funk 2020), könnten wir uns sogar an der Schwelle zu einer gefährlichen Normalisierung des digitalen Autoritarismus befinden (Maati/Švedkauskas 2021). Die negativen Auswirkungen von COVID-19 betreffen sowohl Demokratien als auch Diktaturen. Wie im nächsten Abschnitt gezeigt wird, bietet sich hier Demokratien jedoch auch die einzigartige Gelegenheit, die Öffentlichkeit für autoritäre Methoden zu sensibilisieren und auf die Merkmale hinzuweisen, die digitale Technologien für autoritäre Tendenzen anfällig machen.

COVID-19 hat viele technologische Fortschritte angestoßen, die autoritären Regimen und Praktiken dienen. Die Pandemie war eine Ausnahmesituation, eine Krise, die die Entwicklung und den Einsatz digitaler Überwachungs- und Repressionstechnologien sowohl in demokratischen als auch in autoritären Regimen rechtfertigte (Maati/Švedkauskas 2020). Zwischen April 2020 und 2022 haben 20 Länder KI-Überwachungstechnologien entweder entwickelt oder erworben (Feldstein 2021, S. 227). Im Jahr 2020 gab es den seit 2011 größten Zuwachs an Ländern, die in der Lage waren, mindestens drei Viertel des inländischen Internetzugangs abzuschalten [Abbildung 3a]. Die Daten von Freedom on the Net zeigen auch eine weltweit stärkere Einschränkung der Internetfreiheit in den Jahren der Pandemie im Vergleich zu den Vorjahren [Abbildung 3b]. Im Jahr 2021 schnitten 34 Länder deutlich schlechter ab als 2019, während nur 17 Länder zwischen 2016 und 2018 schlechter abschnitten (Freedom House 2021).

Praktisch alle Länder haben digitale Technologien zur Kontaktnachverfolgung eingesetzt, wobei in vielen Fällen biometrische Daten über Personen erfasst werden (Shahbaz/Funk 2020, S. 14). Zwar sind die Gefahren für die Privatsphäre in einem autoritären Umfeld zweifellos größer als in einer Demokratie, doch auch Demokratien sind gegen diese Tendenzen keineswegs immun. 2020 stufte Amnesty International (2020) die Anwendung zur Kontaktnachverfolgung in Norwegen als eine der „alarmierendsten Massenüberwachungsinstrumente“ ein. In Indien nutzten Smart Cities die Live-Verfolgung von Personen, um Quarantäneanordnungen durchzusetzen. In Israel wurden im Rahmen von Notstandsmaßnahmen GPS-, Kreditkarten- und Handydaten miteinander verknüpft, um Quarantänebestimmungen durchzusetzen und Kontakte zu verfolgen (Halbfinger et al. 2020). Sogar die oft gepriesene Anwendung zur Verfolgung von Kontakten in Deutschland läuft auf Plattformen, die von Apple und Google bereitgestellt werden, was Bedenken hinsichtlich des Zugriffs von großen Technologieunternehmen auf Nutzerdaten hervorruft (Norton Rose Fulbright 2021).

COVID-19 hat die digitale Vernetzung von einer „Annehmlichkeit [zu] einer Notwendigkeit“ (Shahbaz/Funk 2020, S. 1) gemacht und zwingt viele Einzelpersonen, Schulen, Finanzinstitute und Unternehmen, sich auf digitale Technologien zu verlassen (Rodriguez Contreras 2021; Sorgner 2021). Die Pandemie hat auch die Digitalisierung im Lieferkettenbereich um drei bis vier Jahre beschleunigt (Rodriguez Contreras 2021), und einige Untersuchungen zeigen, dass 90 % der Fachleute in diesem Sektor planen, in Digitalisierung zu investieren (Agrawal et al. 2020, S. 3). Die Bedeutung von KI-Technologien für die Kontaktverfolgung, den Datenaustausch und die Entwicklung eines Impfstoffs (Rasheed et al. 2021) hat die Investitionen in die KI-Forschung und -Entwicklung verdoppelt (Stanford AI Index 2022b) [Abbildung 4].

Einige der oben genannten Entwicklungen scheinen unproblematisch zu sein, bergen jedoch inhärente Risiken, da die Pandemie die autoritätsfreundlichen Tendenzen der digitalen Technologien verfestigt. Die Kombination aus rasant steigenden Investitionen in die Entwicklung von KI, der zunehmenden

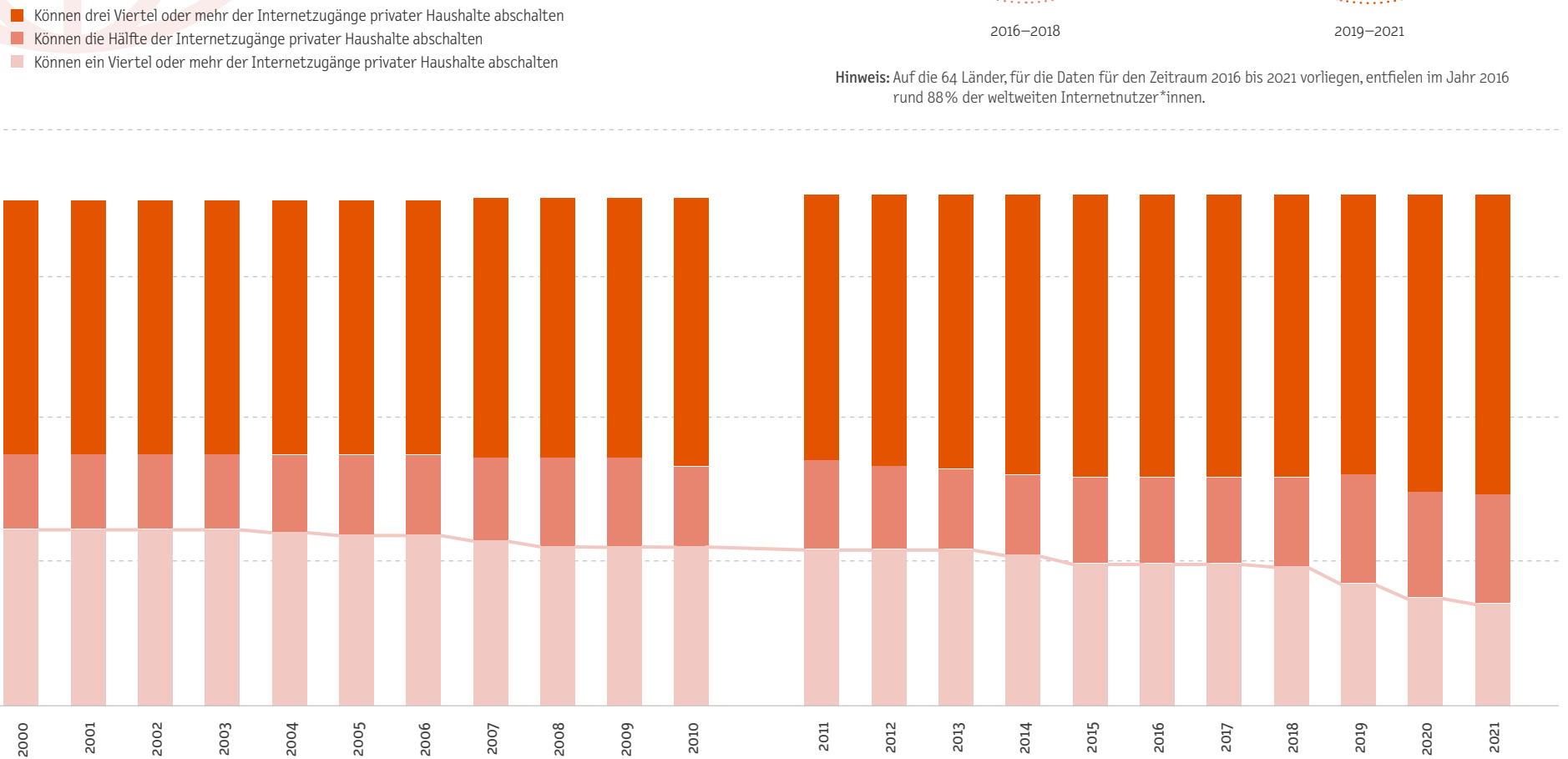
ABBILDUNG 3

DIE COVID-19-PANDEMIE HAT GEFÄHRLICHE TENDENZEN VERSTÄRKT

ABBILDUNG 3a

Regierungen sind zunehmend in der Lage, das Internet abzuschalten

Internet-Abschaltkapazität von Regierungen, 2000–2021, 179 Länder

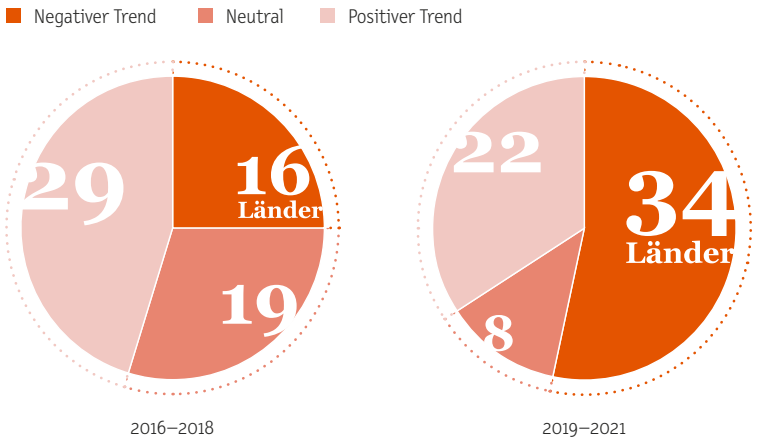


Quelle: Zusammenstellung des Autors, basierend auf dem Digital Society Project 2022 (http://digitalsocietyproject.org/data/).

ABBILDUNG 3b

Die Internetfreiheit ist während der Pandemie massiv eingeschränkt worden

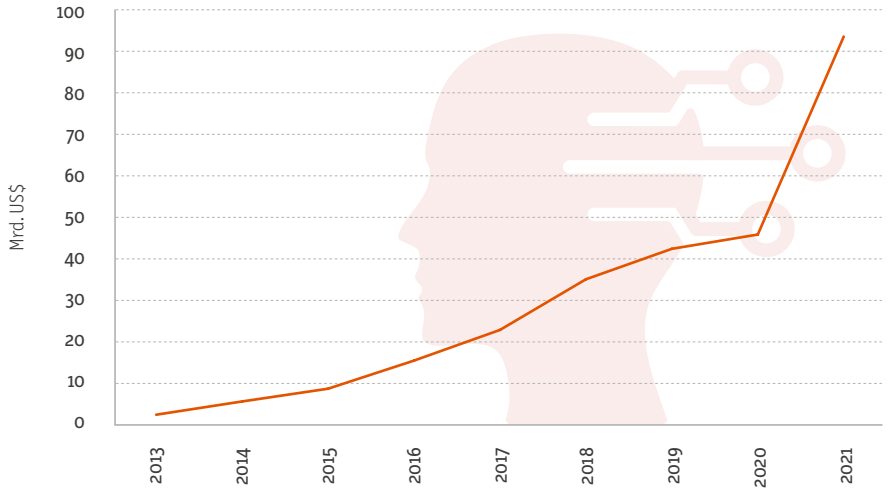
Anzahl der Länder vor (2016–2018) und während (2019–2021) der Pandemie, 64 Länder



Hinweis: Auf die 64 Länder, für die Daten für den Zeitraum 2016 bis 2021 vorliegen, entfielen im Jahr 2016 rund 88 % der weltweiten Internetnutzer*innen.

Quelle: Zusammenstellung des Autors, basierend auf Freedom House 2021.

ABBILDUNG 4
Infolge der Pandemie wurde verstärkt in die Entwicklung und Verbesserung von technologischen Kapazitäten investiert
Gesamtinvestitionen der führenden Länder in KI 2013–2021



Hinweis: Der Stanford AI Index untersucht 29 Länder, die in der KI-Entwicklung weltweit führend sind. Dazu gehören unter anderem China, Deutschland, Indien, Japan, Malaysia, Russland, Singapur, Südkorea, Spanien und die USA.

Quelle: Stanford AI Index 2022a

Abhängigkeit von digitalen Diensten, die wahrscheinlich die Pandemie überdauern werden (OECD 2020a, S. 2), und der Erzeugung großer Mengen digitalisierter Daten erhöht die Anfälligkeit digitaler Technologien für autoritäre Praktiken zur Überwachung, Manipulation und Desinformation. Die zunehmende Abhängigkeit von digitalen Technologien führt dazu, dass „die intimsten Daten der Menschen" (OECD 2020a) gesammelt und analysiert werden. Dadurch werden Algorithmen optimiert, die dann besser in der Lage sind, Personen gezielt zu manipulieren. Das ganze Ausmaß dieser Entwicklung wird sich wahrscheinlich erst in der Zukunft zeigen, da die rasant steigenden Investitionen in digitale Technologien, insbesondere in KI, deren Fähigkeit zur Datenerfassung und -analyse sicherlich noch verbessern werden.

Darüber hinaus verbreiteten die Algorithmen der sozialen Medien während der COVID-19 Krise und deren verstärkter Online-Aktivität kontroverse Informationen, um die Nutzung zu steigern, was zu umfassenden

Fehlinformationen und einer gefährlichen „Infodemie" führte. (WHO 2022). Weiterhin hat COVID-19 auch das ungeregelte und missbrauchsanfällige rechtliche Umfeld verfestigt, in dem digitale Technologien operieren. Regierungen auf der ganzen Welt konnten plötzlich ihre gesetzlichen Befugnisse zur Überwachung und Kontrolle der Bürgerinnen und Bürger erweitern, oft mit Hilfe von Daten, die von großen Technologieunternehmen bereitgestellt wurden (Anisin 2022, S. 263). Der jährlich erscheinende Bericht Freedom on the Net, der den Status der digitalen Freiheit in 65 Ländern untersucht, in denen 87 % der weltweiten Internetnutzer und -nutzerinnen leben (Shahbaz/Funk 2020, S. 5), stellte im Jahr 2020 fest, dass 30 Länder den Datenaustausch mit privaten Unternehmen per Gesetz erleichtert haben (Shahbaz/Funk 2020, S. 19). Außerdem haben mindestens 20 Länder in der Zeit der COVID-Pandemie neue Gesetze oder Verordnungen eingeführt, die die Meinungsäußerung im Internet einschränken (Shahbaz/Funk 2020, S. 10).

2.1 AUTORITARISMUS AUF DEM VORMARSCH, MIT EINEM HOFFNUNGSSCHIMMER FÜR DEMOKRATIE?

Vor diesem Hintergrund hat die Pandemie den schlimmsten Rückschlag für die Freiheit des Internets ausgelöst und gleichzeitig die autoritäre Nutzung digitaler Technologien sowohl in Demokratien als auch in Diktaturen verstärkt. Dennoch eröffnete die Krise sowohl Diktaturen als auch Demokratien unterschiedliche Möglichkeiten, auch wenn beide Systeme teilweise ähnlich reagierten. Diktaturen konnten sich während der Zeit der Pandemie den Wunsch nach stärkerer Überwachung und Kontrolle erfüllen. In Demokratien wurden in dieser Zeit zwar auch autoritäre Praktiken begünstigt, hier bietet sich jedoch auch die Gelegenheit, dem digitalen Autoritarismus entgegenzuwirken. So haben beispielsweise die zunehmende Bedeutung digitaler Technologien und die daraus resultierende Sorge um den Datenschutz dazu geführt, dass beide Arten von Regimen Maßnahmen ergriffen haben, um die Daten(-nutzung) und große Technologieunternehmen unter staatliche Aufsicht zu stellen (Shahbaz/Funk 2021). Während dies für Demokratien eine Chance ist, große Technologieunternehmen einer „demokratischen" Regulierung zu unterwerfen, ist es für Autokraten eine Gelegenheit, ihre autoritäre Kontrolle über Daten zu verstärken und Unternehmen unter Druck zu setzen, damit sie ihren Interessen dienen. Ein Beispiel: Während Deutschland 2021 ein Gesetz verabschiedete, das die Regierung bevollmächtigt, das Verhalten von Unternehmen zu untersuchen, die den Wettbewerb behindern

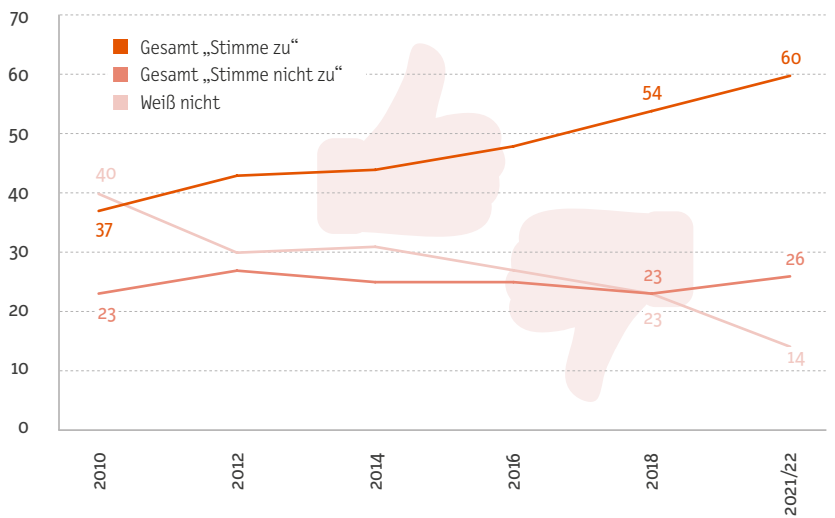
oder den Nutzerinnen und Nutzern die Kontrolle über ihre Daten entziehen, ging Russland mit seinem Antimonopolgesetz gegen Google vor, um YouTube zur Entfernung regimekritischer Inhalte zu zwingen (Shahbaz/Funk 2021, S. 20f.). Sowohl in Demokratien als auch in Diktaturen hat die Pandemie den Einsatz von digitaler Überwachung gefördert. In Diktaturen scheint dies jedoch zu einer schnelleren Normalisierung der digitalen Überwachung zu führen, während es in Demokratien zur Sensibilisierung der Öffentlichkeit und zu Besorgnis führen kann. Eine kürzlich durchgeführte Umfrage zeigt, dass mehr als 60 % der Befragten in China Technologien zur Ermittlung von Kontaktpersonen befürworten, während es in den USA und Deutschland weniger als 20 % sind (Kostka/Habich-Sobiegalla 2020).

Noch wichtiger ist, dass vereinzelte Belege vorsichtig optimistisch stimmen, dass die Pandemie, trotz ihrer negativen Auswirkungen, Demokratien die Möglichkeit gibt, dem digitalen Autoritarismus entgegenzuwirken. COVID-19 könnte nicht nur das Bewusstsein für das autoritäre Potenzial digitaler Technologien schärfen, sondern auch für das Umfeld, in dem diese eingesetzt werden. Die Pandemie hat politische Maßnahmen und wissenschaftliche Diskussionen über digitale Überwachung, Kontrolle, Geheimhaltung und Desinformation in vielen Gesellschaftsschichten ausgelöst. In einigen Demokratien waren die Bürgerinnen und Bürger nicht nur über die digitalen Überwachungsmöglichkeiten besorgt, sondern auch über den Mangel an Transparenz bei Daten und Algorithmen. In Irland ist der am häufigsten genannte Grund, digitale Überwachungs-Apps nicht zu nutzen, die „Befürchtung, dass Technologieunternehmen oder die Regierung die App-Technologie nach der Pandemie für eine stärkere Überwachung nutzen könnten“ (O’Callaghan et al. 2021, S. 863). Im Vereinigten Königreich zeigen qualitative Interviews in verschiedenen Gesellschaftsschichten, dass viele Menschen besorgt waren, „dass ihre Daten von Außenstehenden außerhalb der Regierung und der Gesundheitsbehörden, beispielsweise von ‚Dritten‘ oder ‚Hackern‘, genutzt werden könnten“ (Williams et al. 2021, S. 380). Darüber hinaus hat die Pandemie die Gefahren sowohl der digitalen Kommunikationsmittel zur Verbreitung gefährlicher Desinformationen als auch die Bereitschaft der Social-Media-Plattformen, dies zuzulassen, deutlich gemacht. So waren die Menschen in der französischsprachigen Schweiz am wenigsten bereit, den Informationen in Messaging-Apps und sozialen Medien zu vertrauen (Liu et al. 2020, S. 153). In der EU nahm der prozentuale Anteil der Bürgerinnen und Bürger, die der Meinung sind, dass Informationen in sozialen Medien nicht vertrauenswürdig sind, während der Pandemiejahre weiter zu (European Commission 2022, S. 65) [Abbildung 5]. Ähnliche Bedenken treiben politische Entscheidungsträgerinnen und Entscheidungsträger sowie Wissenschaftlerinnen und Wissenschaftler um. Seit Beginn der Pandemie haben der Europarat (Council of Europe 2020), die WHO (2020) und die OECD verschiedene Dokumente und Richtlinien zum Schutz der Privatsphäre bei der Nutzung digitaler Technologien zur Bekämpfung der weltweiten Pandemie veröffentlicht (OECD 2020b). Auch in wissenschaftlichen Artikeln aus verschiedenen Fachbereichen wurden die Gefahren des digitalen Autoritarismus im Zusammenhang mit der Pandemie diskutiert und mögliche Reaktionen darauf erörtert.

ABBILDUNG 5
Die Pandemie hat die Öffentlichkeit für technologische Gefahren sensibilisiert
Standard Eurobarometer-Umfrage 96, öffentliche Meinung in der EU, Winter 2021–2022

Unabhängig davon, ob Sie soziale Netzwerke im Internet (Internetseiten sozialer Netzwerke, Videoportale und Blogs) nutzen oder nicht, sagen Sie mir bitte, ob Sie folgenden Aussagen voll und ganz zustimmen, eher zustimmen, eher nicht zustimmen oder überhaupt nicht zustimmen:

Die Informationen, die man in sozialen Netzwerken zu politischen Angelegenheiten findet, sind eher nicht vertrauenswürdig (in %)



Quelle: European Commission 2022, S. 66.

3. WAS IST ALSO ZU TUN?

Die zunehmende Relevanz digitaler Gefahren während der Pandemie bietet Akteuren in Demokratien die Gelegenheit, diese zu reduzieren und ihnen entgegenzuwirken. Die vorherigen Abschnitte haben deutlich gemacht, welche Aspekte digitale Technologien für autoritäre Praktiken anfällig machen, die zudem auch für eher technikferne Personen zugänglich sind. Durch die drei oben beschriebenen Merkmale wird der Einfluss von COVID-19 auf den digitalen Autoritarismus verdeutlicht, und zwar auf eine für die Öffentlichkeit und politisch Verantwortliche nachvollziehbare Art und Weise. Dies ermöglicht es den verschiedenen Akteuren in Demokratien, sich über die unmittelbaren Bedenken hinsichtlich Überwachung und Datenschutz hinaus mit den Merkmalen zu befassen, die digitale Technologien anfällig für eine autoritäre Nutzung machen. In den folgenden Abschnitten werden die Verantwortungsbereiche von politischen Entscheidungsträgerinnen und -trägern, der Zivilgesellschaft, der Wissenschaft sowie Bürgerinnen und Bürgern erörtert und anschließend konkrete Empfehlungen formuliert [Tabelle 1].

Zivilgesellschaftliche Akteure und Wissenschaftlerinnen und Wissenschaftler in Demokratien sollten daher die Öffentlichkeit für digitale Potenziale und deren autoritäre Nutzungsweisen sensibilisieren und auf die ihnen zugrundeliegenden Eigenschaften aufmerksam machen, die sie für den Autoritarismus prädestinieren (das Umfeld). COVID-19 bietet eine Gelegenheit, der Öffentlichkeit und den politisch Verantwortlichen in Demokratien diese Themen nahezubringen. In der Zeit vor COVID-19 erschienen die Gefahren digitaler Technologien dem Durchschnittsnutzer oder der politischen Entscheidungsträgerin vielleicht noch in weiter Ferne. Heute gehen die Gefahren digitaler Technologien jedoch nicht mehr nur von Russland oder China aus; vielmehr wird immer deutlicher, dass zumindest einige dieser Gefahren direkt mit der Funktionsweise der Technologien und mit ihren umfangreichen Möglichkeiten zusammenhängen.

Die Wissenschaft hat bei der Erforschung von COVID-19 und den damit verbundenen Gefahren hervorragende Arbeit geleistet; sie sollte der Öffentlichkeit diese Gefahren nun auch auf verständliche Weise vermitteln. Wir neigen dazu, uns in technische Details zu vertiefen und in wissenschaftlichen Jargon zu verfallen. Auch wenn dies für den wissenschaftlichen Fortschritt in gewissem Umfang erforderlich ist, muss die Wissenschaft ihre Arbeit besser

auf ein nicht-wissenschaftliches Publikum ausrichten, ohne dabei die methodische oder analytische Genauigkeit aufzugeben. COVID-19 bietet für diese Aufgabe eine universelle, gemeinsame Grundlage, was die Themen Freiheit und Schutz der Privatsphäre betrifft. Wissenschaftlerinnen und Wissenschaftler sollten sich daher stärker an die Öffentlichkeit wenden und ihre Kommunikation mit einem nicht-akademisches Publikum verbessern.

Politisch Verantwortliche in einigen Demokratien haben Schritte unternommen, um Daten unter staatliche Kontrolle zu bringen (siehe Abschnitt 3.2). Es ist jedoch äußerst wichtig, dass ein solcher Vorstoß in Sachen Datensouveränität mit einer strengen „demokratischen“ Kontrolle gegen staatlichen Datenmissbrauch einhergeht. Die zunehmende öffentliche Sensibilisierung für die Gefahren digitaler Technologien während der Pandemie bietet den politisch Verantwortlichen die Möglichkeit, bei den großen Technologiekonzernen auf mehr Transparenz bei der Erfassung und Verarbeitung von Daten durch ihre Algorithmen zu drängen. Und schließlich sollten demokratische Entscheidungsträgerinnen und -träger eine Debatte darüber führen, wie nicht nur die Nutzung von KI-Technologien reguliert werden kann, sondern auch, wie diese Technologien erforscht werden und anhand welcher Art von Daten sie trainiert werden.

Die Bürgerinnen und Bürger sind der Motor von Demokratien und können zumindest zwei Dinge tun: Erstens können sie gemeinsam Druck auf die politisch Verantwortlichen für eine bessere Regulierung digitaler Technologien ausüben. Dieser Druck sollte sich nicht nur auf die Endprodukte oder deren Einsatz beschränken, sondern auch die zugrunde liegende technisch-wirtschaftliche Infrastruktur einbeziehen. Insbesondere sollten die Bürgerinnen und Bürger gegen alle Rechtsvorschriften vorgehen, die den Regierungen mehr Zugang zu persönlichen Daten gewähren. Sie sollten auch uneingeschränkte Transparenz bei der Erhebung und Nutzung ihrer Daten sowohl durch die Regierung als auch durch große Technologieunternehmen fordern. Dazu gehört auch Transparenz darüber, wie die Algorithmen funktionieren, die den Prozess der Datenerhebung und -analyse automatisieren. Dies hat sich in Demokratien wie z. B. in Deutschland während der Pandemie als wirksam erwiesen, da der öffentliche Druck die Regierung veranlasste, sich auf eine Open-Source-Anwendung zur Ermittlung von Kontaktpersonen zu beschränken. Und schließlich sollten die Bürgerinnen und Bürger mit den politischen Entscheidungsträgerinnen und -trägern darüber diskutieren, wie die in Krisenzeiten im Bereich der öffentlichen Gesundheit gesammelten

TABELLE 1

COVID-19 HAT DIE BEDEUTUNG DER FAKTOREN VERSTÄRKT, DIE DIGITALE TECHNOLOGIEN ANFÄLLIG FÜR AUTORITARISMUS MACHEN

Wie können Demokratien diese Gelegenheit nutzen?

Politisch Verantwortliche

REGULIERUNGEN, UM

Daten unter demokratische staatliche Kontrolle zu bringen (Datensouveränität)

Große Technologieunternehmen zu mehr Transparenz darüber zu verpflichten, wie Algorithmen Daten sammeln und verarbeiten

Schutzmaßnahmen auf der Ebene der Erforschung und Entwicklung (nicht nur der Nutzung) von digitalen Technologien und KI einzuführen

Zivilgesellschaft

DAS WISSEN UM DIE BEDEUTUNG IN KOMPETENZEN ÜBERSETZEN:

Bürgerinnen und Bürger sowie politisch Verantwortliche über die grundlegenden Merkmale (Umfeld), die digitalen Autoritarismus begünstigen, aufklären

Mit konkreten Beispielen beginnen, die während der COVID-19-Pandemie wichtig wurden (Anwendungen zur Kontaktverfolgung, biometrische Datenerfassung usw.)

Schrittweise weniger wichtige Themen einbeziehen (soziale Medien oder Algorithmen für den Online-Einkauf usw.)

Bürgerinnen und Bürger bei Software- und Hardware-Entscheidungen zur Sicherung ihrer Daten unterstützen

Eine ausgewogene und objektive Darstellung gewährleisten: Die Gefahren aufzeigen, ohne die Technologie zu verteufeln oder die Vorteile zu ignorieren
Das Ziel ist, die Vorteile zu nutzen und die Risiken zu minimieren

Bürgerinnen und Bürger

KOLLEKTIVER DRUCK AUF LOKALE VERTRETERINNEN UND VERTRETER UND POLITISCH VERANTWORTLICHE, UM

Den Zugang zu Nutzerdaten strikt zu begrenzen

Vollständige Transparenz darüber zu fordern, wie Unternehmen Daten sammeln und verarbeiten – einschließlich Transparenz darüber, wie Algorithmen funktionieren

Digitale Technologien während ihres gesamten Anwendungszeitraums zu regulieren: Forschung, Entwicklung und Einsatz

DAS INDIVIDUELLE VERHALTEN ANPASSEN, UM RISIKEN ZU MINIMIEREN

Datenschutzrichtlinien und Cookie-Benachrichtigungen sorgfältig lesen. Nur Bedingungen/Cookies akzeptieren, die man für akzeptabel hält

Die Erfolgsbilanz von Unternehmen in Sachen Datenschutz prüfen, bevor man ihre Dienste nutzt oder ihre digitalen Produkte kauft

Cookies und Tracking-Dateien regelmäßig löschen

Sicherheits- und Anti-Tracking-Software auf allen digitalen Geräten verwenden

Wissenschaftlerinnen und Wissenschaftler

DIE ÖFFENTLICHKEIT STÄRKER ANSPRECHEN UND EINE VERSTÄNDLICHE, NICHTTECHNISCHE SPRACHE VERWENDEN, UM

Wissen über die Merkmale und Gefahren des digitalen Autoritarismus' und seine Relevanz für das tägliche Leben in Demokratien zu verbreiten

Die Zivilgesellschaft dabei zu unterstützen, ein ausgewogenes Bewusstsein für die Vorteile und Gefahren der digitalen Technologien zu entwickeln

Regierungen und politisch Verantwortlichen zu helfen, Bedrohungen zu erkennen und Gefahren abzuwehren

Den Bürgerinnen und Bürgern zu helfen, ihr (Online-) Verhalten anzupassen, um die Risiken zu minimieren

Daten davor geschützt werden können, mit anderen bereits vorhandenen digitalen Daten kombiniert und verknüpft zu werden.

Zweitens muss sich das (Online-)Verhalten ändern, um diese Gefahren zu reduzieren. Konkret sollten sich die Bürgerinnen und Bürger die Mühe machen, die 'Cookie'-Benachrichtigungen zum Datenschutz auf Websites zu lesen und so zu handhaben, dass sie die Erfassung und Verarbeitung ihrer Daten kontrollieren können. Es gibt auch eine breite Palette an kostenloser Software, mit der sich Online-Tracking-Daten von digitalen Geräten löschen lassen. Wir sollten außerdem bei der Nutzung von Diensten oder beim Kauf von Geräten „mit Bedacht" auf vertrauenswürdige Quellen zurückgreifen, die das Engagement der Unternehmen für den Schutz von Nutzerdaten bewerten (z. B. https://rankingdigitalrights.org). Und schließlich sollte auf allen digitalen Geräten Sicherheits-, Verschlüsselungs- und Anti-Tracking-Software installiert und verwendet werden (https://netalert.me bietet einfache Erklärungen zu verschiedenen Bedrohungen und Tools zu deren Bekämpfung).

COVID-19 hat zwar den digitalen Autoritarismus weltweit gestärkt, es ist jedoch Aufgabe der Demokratien, in Krisenzeiten neue Wege aufzuzeigen. Die Sensibilisierung ist ein notwendiger erster Schritt, um dem digitalen Autoritarismus zu begegnen.

LITERATUR

AGRAWAL, MAYANK/ELOOT, KAREL/MANCINI, MATTEO/PATEL, ALPESH 2020: Industry 4.0: Reimagining Manufacturing Operations after COVID-19 (McKinsey & Company), o.O. (https://www.mckinsey.com/business-functions/operations/our-insights/industry-40-reimagining-manufacturing-operations-after-covid-19, 26.10.2022).

ALAM NIPU, NAIFUL/TALKUDER, SOUVIK/SOUVIK TALUKDER/ISLAM, SAIFUL/CHAKRABARTY, AMITABHA 2018: Human Identification Using WIFI Signal, in: Joint 7th International Conference on Informatics, Electronics & Vision (ICIEV) and 2nd International Conference on Imaging, Vision & Pattern Recognition (IcIVPR), S. 300-304.

ALI, KAMRAN/LIU, ALEX X./WANG, WEI/SHAHZAD, MUHAMMAD 2015: Keystroke Recognition Using WiFi Signals, in: Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, MobiCom '15, New York: Association for Computing Machinery, S. 90-102.

AMNESTY INTERNATIONAL 2020: Bahrain, Kuwait and Norway Contact Tracing Apps a Danger for Privacy, o.O. (https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/, 24.08.2022).

ANISIN, ALEXEI 2022: Pandemic Surveillance Capitalism: Authoritarian Liberalism or Democratic Backsliding?, in: Journal of Political Power, Jg. 15/2, S. 262-278.

BBC 2021: Google AI Defeats Human Go Champion, London (https://www.bbc.com/news/technology-40042581, 01.09.2022).

BRADLEY, CHARLES/WINGFIELD, RICHARD/METZGER, MEGAN 2021: National Artificial Intelligence Strategies and Human Rights: A Review (Global Partners Digital), o.O. (https://www.gp-digital.org/wp-content/uploads/2021/05/NAS-and-human-rights_2nd_ed.pdf, 12.10.2022).

CONFESSORE, NICHOLAS 2018: Cambridge Analytica and Facebook: The Scandal and the Fallout So Far (The New York Times), New York City (https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html, 01.09.2022).

COUNCIL OF EUROPE 2020: Contact Tracing Apps, Strasbourg (https://www.coe.int/en/web/data-protection/contact-tracing-apps, 30.08.2022).

CUSHMAN, ISAAC/RAWAT, DANDA B./BHIMRAJ, ABHISHEK/FRASER, MALIK 2016: Experimental Approach for Seeing through Walls Using Wi-Fi Enabled Software Defined Radio Technology, in: Digital Communications and Networks, Jg. 2/4, S. 245-255.

DARPA (Defense Advanced Research Projects Agency) 2017: Towards a High-Resolution, Implantable Neural Interface, Arlington (https://www.darpa.mil/news-events/2017-07-10, 03.08.2022).

DIGITAL SOCIETY PROJECT 2022: DSM Data V4, o.O. (http://digitalsocietyproject.org/data/, 12.10.2022).

DING, DIAN/YANG, LANQING/CHEN, YI-CHAO/XUE, GUANGTAO 2021: VibWriter: Handwriting Recognition System Based on Vibration Signal, in: 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), S. 1-9.

EUROPEAN COMMISSION 2022: Media Use in the European Union, Brussels (Standard Eurobarometer 96, Winter 2021-2022) (https://data.europa.eu/doi/10.2775/911712, 08.11.2022).

FELDSTEIN, STEVEN 2021: The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance, Oxford: Oxford University Press.

FISHMAN, ROBERT M. 1990: Rethinking State and Regime: Southern Europe's Transition to Democracy, in: World Politics, Jg. 42/3, S. 422-440.

FREEDOM HOUSE 2021: All Score Data, 2011-2021 (Freedom House), o.O. (https://freedomhouse.org/report/freedom-net, 12.10.2022).

GLASIUS, MARLIES 2018: What Authoritarianism Is... and Is Not: A Practice Perspective, in: International Affairs, Jg. 94/3, S. 515-533.

GUO, ZHENGXIN/XIAO, FU/SHENG, BIYUN/FEI, HUAN/YU, SHU 2020: WiReader: Adaptive Air Handwriting Recognition Based on Commercial WiFi Signal, in: IEEE Internet of Things Journal, Jg. 7/10, S. 10483-10494.

HALBFINGER, DAVID M./KERSHNER, ISABEL/BERGMAN, RONEN 2020: To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data (The New York Times), New York City (https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html, 12.10.2022).

KENYON, MILES 2019: Dubious Denials & Scripted Spin: Spyware Company NSO Group Goes on 60 Minutes (The Citizen Lab), Toronto (https://citizenlab.ca/2019/04/dubious-denials-scripted-spin-spyware-company-nso-group-goes-on-60-minutes, 11.10.2022).

KOSTKA, GENIA/HABICH-SOBIEGALLA, SABRINA 2020: In Times of Crisis: Public Perceptions Towards COVID-19 Contact Tracing Apps in China, Germany and the US, Berlin (https://papers.ssrn.com/abstract=3693783, 26.08.2022).

LIU, ZHAN/SHAN, JIALU/DELALOYE, MATTHIEU/PIGUET, JEAN-GABRIEL/GLASSEY BALET, NICOLE 2020: The Role of Public Trust and Media in Managing the Dissemination of COVID-19-Related News in Switzerland, in: Journalism and Media, Jg. 1/1, S. 145-158.

LOOKOUT SECURITY 2017: Pegasus for Android: Technical Analysis and Findings of Chrysaor (Security report), o.O. (https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-android-technical-analysis.pdf, 11.10.2022).

MAATI, AHMED/ŠVEDKAUSKAS, ŽILVINAS 2020: Framing the Pandemic and the Rise of the Digital Surveillance State, in: Mezinárodní vztahy, Jg. 55/4, S. 48-71.

MAATI, AHMED/ŠVEDKAUSKAS, ŽILVINAS 2021: Long-Term Prescription? Digital Surveillance Is Here to Stay, in: Mezinárodní vztahy, Jg. 56/4, S. 105-118.

MARCZAK, BILL/SCOTT-RAILTON, JOHN/MCKUNE, SARAH/RAZZAK, BAHR A./DEIBERT, RON 2018: Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries (The Citizen Lab), Toronto (https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/, 01.07.2019).

MIRANDA, ROBBIN A. ET AL. 2015: DARPA-Funded Efforts in the Development of Novel Brain-Computer Interface Technologies, in: Journal of Neuroscience Methods, Jg. 244, S. 52-67.

MURPHY, MARGI 2017: The Government Wants to Put 'Telepathy' Chips in Our Brains (New York Post), New York City (https://nypost.com/2017/07/12/the-government-wants-to-put-telepathy-chips-in-our-brains, 03.08.2022).

NORTON ROSE FULBRIGHT 2021: Contact Tracing Apps: A New World for Data Privacy, o.O. (https://www.nortonrosefulbright.com/en-de/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy, 24.08.2022).

O'CALLAGHAN, MICHAEL E. ET AL. 2021: A National Survey of Attitudes to COVID-19 Digital Contact Tracing in the Republic of Ireland, in: Irish Journal of Medical Science, Jg. 190/3, S. 863-887.

OECD (Organisation for Economic Co-operation and Development) 2020a: Digital Transformation in the Age of COVID-19: Building Resilience and Bridging Divides. (Digital Economy Outlook 2020 Supplement), Paris (https://www.oecd.org/digital/digital-economy-outlook-covid.pdf, 12.10.2022).

OECD (Organisation for Economic Co-operation and Development) 2020b: Tracking and Tracing COVID: Protecting Privacy and Data While Using Apps and Biometrics, Paris (https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protect-ing-privacy-and-data-while-using-apps-and-biometrics-8f394636/, 30.08.2022).

PRIEST, DANA/DWOSKIN, ELIZABETH 2021: Chief of WhatsApp, Which Sued NSO over Alleged Hacking of Its Product, Disputes Firm's Denials on Scope of, Involvement in Spyware Operations (The Washington Post), Washington, DC (https://www.washingtonpost.com/investigations/2021/07/24/whatsapp-pegasus-spyware/, 01.09.2022).

PRIEST, DANA/TIMBERG, CRAIG/MEKHENNET, SOUAD 2021: Private Israeli Spyware Used to Hack Cellphones of Journalists, Activists Worldwide (The Washington Post), Washington, DC (https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/, 01.09.2022).

RASHEED, JAWAD ET AL. 2021: COVID-19 in the Age of Artificial Intelligence: A Comprehensive Review, in: Interdisciplinary Sciences: Computational Life Sciences, Jg. 13/2, S. 153-175.

RODRIGUEZ CONTRERAS, RICARDO 2021: COVID-19 and Digitalisation (Eurofound), o.O. (https://www.eurofound.europa.eu/data/digitalisation/research-digests/covid-19-and-digitalisation, 12.08.2022).

SAGLAM, KORAY 2022: The Digital Blender: Conceptualizing the Political Economic Nexus of Digital Technologies and Authoritarian Practices, in: Globalizations, Jg. 19/7, zunächst online veröffentlicht.

SCHLUMBERGER, OLIVER/EDEL, MIRJAM/MAATI, AHMED/SAGLAM, KORAY 2022: How Authoritarianism Transforms: A Framework to Study Digital Dictatorship. Unveröffentlichtes Manuskript (in Überarbeitung).

SHAHBAZ, ADRIAN/FUNK, ALLIE 2019: Freedom on the Net 2019: The Crisis on Social Media. Washington, DC: Freedom House.

SHAHBAZ, ADRIAN/FUNK, ALLIE 2020: Freedom on the Net 2020: The Pandemic's Digital Shadow. Washington, DC: Freedom House.

SHAHBAZ, ADRIAN/FUNK, ALLIE 2021: Freedom on the Net 2021: The Global Drive to Control Big Tech. Washington, DC: Freedom House.

SIMPSON, KAITLYN 2019: Flaw in WhatsApp Exploited to Target Human Rights Lawyer, Finds Citizen Lab (The Varsity), Toronto (https://thevarsity.ca/2019/06/26/flaw-in-whatsapp-exploited-to-target-human-rights-lawyer-finds-citizen-lab/, 25.09.2019).

SORGNER, ALINA 2021: The COVID-19 Crisis and Digital Transformation: What Impacts on Gender Equality?, o.O. (https://www.unido.org/stories/covid-19-crisis-and-digital-transformation-what-impacts-gender-equality, 12.08.2022).

STANFORD AI INDEX 2022a: Global AI Vibrancy Tool (Stanford Institute for Human-Centered Artificial Intelligence), Stanford (https://aiindex.stanford.edu/vibrancy/, 06.09.2022).

STANFORD AI INDEX 2022b: The AI Index Report - Artificial Intelligence Index (Stanford Institute for Human-Centered Artificial Intelligence), Stanford (https://aiindex.stanford.edu/report/, 06.09.2022).

VAN CLEAVE, KRIS 2021: Facebook Whistleblower: Internal Documents Detail How Misinformation Spreads to Users (CBS News), Washington, DC (https://www.cbsnews.com/news/facebook-whistleblower-frances-haugen-documents-misinformation-spread/, 24.08.2022).

WANG, GUANHUA/ZOU, YONGPAN/ZHOU, ZIMU/WU, KAISHUN/NI, LIONEL M. 2016: We Can Hear You with Wi-Fi!, in: IEEE Transactions on Mobile Computing, Jg. 15/11, S. 2907-2920.

WHO (WORLD HEALTH ORGANIZATION) 2020: Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing: Interim Guidance, Genf (https://apps.who.int/iris/bitstream/handle/10665/332200/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1-eng.pdf, 12.10.2022).

WHO (WORLD HEALTH ORGANIZATION) 2022: Infodemic, Genf (https://www.who.int/health-topics/infodemic, 01.09.2022).

WILLIAMS, SIMON N./ARMITAGE, CHRISTOPHER J./TAMPE, TOVA/DIENES, KIMBERLY 2021: Public Attitudes towards COVID-19 Contact Tracing Apps: A UK-Based Focus Group Study, in: Health Expectations: An International Journal of Public Participation in Health Care and Health Policy, Jg. 24/2, S. 377-385.

XIN, TONG/GUO, BIN/WANG, ZHU/LI, MINGYANG/YU, ZHIWEN 2016: FreeSense: Indoor Human Identification with WiFi Signals, Xi'an (http://arxiv.org/abs/1608.03430, 06.09.2022).

ZUBOFF, SHOSHANA/MÖLLERS, NORMA/WOOD, DAVID MURAKAMI/LYON, DAVID 2019: Surveillance Capitalism: An Interview with Shoshana Zuboff, in: Surveillance & Society, Jg. 17/1-2, S.257-266.

DER AUTOR

AHMED MAATI
Postdoktorand am Lehrstuhl für Politikanalyse an der Hochschule für Politik – Technische Universität München

WEITERE AUSGABEN

Alle Ausgaben sind kostenlos abrufbar unter www.sef-bonn.org

GLOBALE TRENDS. ANALYSEN 01|20221

Klimawandel, gewaltsame Konflikte und Environmental Peacebuilding: Die Zusammenhänge verstehen
Tobias Ide
August 2022, 36 Seiten

Der Klimawandel beeinträchtigt in vielen Regionen nicht nur die menschliche Sicherheit, sondern auch die wirtschaftliche und politische Stabilität. Die Konkurrenz um natürliche Ressourcen wird verstärkt, Migration nimmt zu und bewaffneten Gruppen fällt es leichter, neue Mitglieder zu rekrutieren.

Environmental peacebuilding als ein umfassender Ansatz kann klimabezogene Konfliktrisiken angehen, indem er sich mit der Frage auseinandersetzt, wie das gemeinsame Management von natürlichen Ressourcen und Umweltproblemen die Zusammenarbeit zwischen sozialen Gruppen und somit Frieden fördern kann. In GLOBALE TRENDS. ANALYSEN 01|2022 erläutert Tobias Ide die wichtigsten Mechanismen, mit denen *environmental peacebuilding* einen klimaresilienten Frieden unterstützen kann. Hierbei wirft der Autor auch einen Blick auf die Grenzen des Ansatzes. Schließlich gibt das Papier Handlungsempfehlungen an politische Akteure, Geber und zivilgesellschaftliche Organisationen, wie sie *environmental peacebuilding*-Prozesse auf der lokalen Ebene unterstützen könne.

GLOBALE TRENDS.ANALYSEN 03|2021

KI-Regulierung in einen globalen Einklang bringen:
Lehren aus der aktuellen Praxis
Amandeep Singh Gill
Dezember 2021, 32 Seiten

Daten und künstliche Intelligenz (KI) als globale Gemeingüter anzusehen, könnte entscheidend dazu beitragen, dass diese Schlüsseltechnologien des 21. Jahrhunderts der gesamten Menschheit zugutekommen. Bemühungen, die Entwicklung und Regulierung von KI voranzutreiben, sind bisher jedoch stark fragmentiert. Daraus ergeben sich nicht nur Risiken, sondern auch entgangene Chancen. Wie Amandeep Singh Gill in GLOBALE TRENDS. ANALYSEN 3|2021 beschreibt, könnten ein ganzheitlicher Gemeingüter-Ansatz, geteilte Werte, eine gemeinsame Sprache und öffentliche digitale Infrastrukturen dazu beitragen, die Governance von KI global besser abzustimmen und ihre Potenziale zu entfalten.

GLOBALE TRENDS.ANALYSEN 02|2021

Sprechen wir durch das Recht:
Für einen rechtlich verankerten Multilateralismus
Heike Krieger
Dezember 2021, 27 Seiten

Seit einiger Zeit ist der im Völkerrecht verankerte Multilateralismus unter Druck geraten. Im Wechselspiel gegensätzlicher Kräfte eröffnen sich jedoch auch Handlungsspielräume für politische Akteure. In den GLOBALE TRENDS. ANALYSEN 2|2021 fordert Heike Krieger die EU-Mitgliedstaaten dazu auf, sich für Entwicklungen und Trends zu engagieren, die die internationale Ordnung stabilisieren. Zu diesem Zweck sollen sie einen rechtlich institutionalisierten Multilateralismus informellen Netzwerkstrukturen vorziehen. Grundlage ist eine glaubwürdige und konsistente Einhaltung des Völkerrechts sowie die Erarbeitung eines gemeinsamen Verständnisses dieser Rechtsordnung gerade mit Staaten des Globalen Südens.

GLOBALE TRENDS.ANALYSEN 01|2021

Finanzpolitischen Spielraum schaffen:
Ein Gebot der Menschenrechte in Zeiten von COVID-19
Ignacio Saiz
Mai 2021, 29 Seiten

Die Ungleichheit zwischen Staaten hat sich durch die COVID-19-Pandemie verstärkt. Die wirtschaftlichen Folgen der Pandemie sind in Ländern des Globalen Südens besonders verheerend. Die Ressourcen, die sie zur Bewältigung der Krise mobilisieren können, sind völlig unzureichend. Umso wichtiger ist es, dass die wohlhabenderen Länder und die internationalen Finanzinstitutionen die Hindernisse beseitigen, die sich aus ihrer Schulden- und Steuerpolitik für den finanzpolitischen Spielraum von Ländern mit niedrigem und mittlerem Einkommen ergeben. Eine solche Zusammenarbeit ist nicht nur ein Gebot der globalen öffentlichen Gesundheit. Sie ist auch eine bindende menschenrechtliche Verpflichtung, wie Ignacio Saiz erläutert.

Institut für Entwicklung und Frieden (INEF),
Universität Duisburg-Essen, Duisburg

sef: Stiftung Entwicklung und Frieden
Development and Peace Foundation

INEF

GLOBALE TRENDS. ANALYSEN

untersuchen gegenwärtige und künftige Herausforderungen einer globalisierten Welt vor dem Hintergrund langfristiger politischer Trends. Die Reihe widmet sich Fragen von hoher politischer Relevanz für künftige Entwicklungen auf regionaler oder globaler Ebene. GLOBALE TRENDS. ANALYSEN deckt ein breites Themenfeld in den Bereichen Global Governance, Frieden und Sicherheit, nachhaltige Entwicklung, Weltwirtschaft und Weltfinanzsystem, Umwelt und natürliche Ressourcen ab. Die Reihe zeichnet sich durch Perspektiven aus verschiedenen Weltregionen aus.