2022

# Atlas der Zivil-gesell-schaft

## Freiheitsrechte unter Druck

## Schwerpunkt Digitalisierung

Zahlen. Analysen. Interviews. Weltweit.

oekom

CIVICUS

Brot für die Welt

# Vorwort

Zivilgesellschaftliche Organisationen leiden immer stärker unter Einschränkungen, Verboten und Repressionen: Wieder verloren weltweit viele Partnerorganisationen von Brot für die Welt ihre Registrierung oder konnten sie nicht mehr verlängern. Wieder mussten viele ihrer Mitarbeitenden das Land verlassen, um nicht verhaftet zu werden. Noch nie mussten so viele Organisationen in ihrem Ursprungsland geschlossen werden und ihre Arbeit aus dem Ausland fortsetzen. Dabei sind Menschenrechte und zivilgesellschaftliche Initiativen essenziell für Demokratie, Entwicklung und Frieden.

Vor diesem Hintergrund veröffentlichen wir nun zum fünften Mal den Atlas der Zivilgesellschaft gemeinsam mit CIVICUS, dem weltweiten Netzwerk für Bürgerbeteiligung. Die Daten des CIVICUS-Monitor spiegeln unsere eigenen Beobachtungen des weltweiten Trends wider: Der Handlungsraum zivilgesellschaftlicher Organisationen und Akteur:innen schrumpfte im vergangenen Jahr erneut. Die Zahl der Menschen, die in offenen Gesellschaften leben, sinkt weiter – und die der Menschen, die in Staaten leben, deren Regierungen die Zivilgesellschaft unterdrücken und schließen, wächst. 70 Prozent der Weltbevölkerung leben inzwischen in diesen Ländern, die der Atlas orange und rot darstellt.

14 Länder haben sich in ihrer Einstufung verschlechtert, darunter auch Polen, das nun neben Ungarn als zweites EU-Mitglied in der Kategorie „beschränkt“ eingestuft wird. Das zeigt, dass längst auch im Globalen Norden und der Europäischen Union die zivilgesellschaftlichen Handlungsräume zunehmend schrumpfen. Die Zahl der im Atlas der Zivilgesellschaft grün eingefärbten – also offenen – Länder in der EU hat mit zwölf einen neuen Tiefstand erreicht.

Deutschland gehört weiterhin zu den offenen Staaten. Doch auch hier ist die Situation für die Zivilgesellschaft nicht perfekt. Reporter ohne Grenzen hat Deutschland 2021 in der Rangliste der Pressefreiheit eine Kategorie abgewertet, weil Journalist:innen stärker als je zuvor von Protestierenden angegriffen wurden. Des Weiteren ist zu beobachten, dass zivilgesellschaftliche Organisationen und Freiwillige, die sich etwa in der Flüchtlingsarbeit oder für Klima- und Umweltschutz engagieren, immer häufiger attackiert und bedroht werden. Nicht nur über die Sozialen Medien, sondern auch physisch.

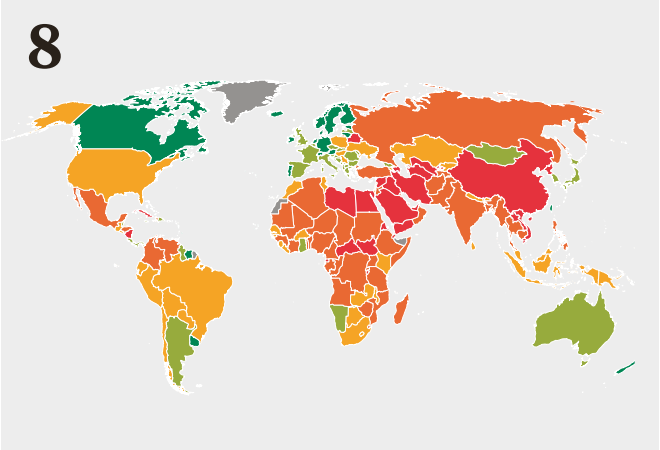
Hinzu kommt, dass weltweit die Digitalisierung an Bedeutung gewonnen hat und in immer mehr Bereiche hineinwirkt. Diesem Thema widmet sich daher der Schwerpunkt unserer Publikation. Denn Digitalisierung ist für die Aktivist:innen Chance und Problem zugleich: Mithilfe moderner Kommunikationskanäle können sie einerseits direkter und erfolgreicher informieren, mobilisieren, sich vernetzen. Andererseits können Autokrat:innen mittels Digitalisierung viel leichter Meinungsäußerungen zensieren und Menschen überwachen. Und doch kommen wir zu dem Fazit, das auch die 2021 erschienene Denkschrift der EKD „Freiheit digital. Die Zehn Gebote in Zeiten des digitalen Wandels“ teilt: Digitalisierung ist auch ein wichtiger Baustein für nachhaltige Entwicklung. Vorausgesetzt, dass Barrieren des Zugangs abgebaut und Menschenrechte respektiert werden.

Bei allen Herausforderungen der Digitalisierung, die unser Schwerpunktteil beleuchtet, wird eines klar: Menschenrechtsorganisationen und NGOs, die sich mit Fragen der Digitalisierung beschäftigen, und viele andere setzen sich unermüdlich dafür ein, dass digitale Tools unser Leben bereichern und Schäden minimiert werden. Ob Nicht-Diskriminierung bei automatisierten Entscheidungen und künstlicher Intelligenz, bessere Regulierung der Exporte von Überwachungstechnologien, der biometrischen Erkennung oder der großen Tech-Konzerne, Vermeidung von Hasskriminalität, Bewahrung von Datenschutz oder Meinungsfreiheit online: Zivilgesellschaftliche Initiativen erfüllen auch hier ihre wichtige Watch-Dog-Funktion und wachen darüber, dass Menschen weltweit so viel wie möglich von technologischen Entwicklungen profitieren – und dabei Menschenrechte eingehalten werden.

**Dr. Dagmar Pruin**
Präsidentin von Brot für die Welt

# Inhalt








## 1

## CIVICUS-Monitor: Verschärfte Bedingungen für die Zivilgesellschaft



## Die Weltregionen


# 2

## Schwerpunkt Digitalisierung: Gefahren und Chancen für die Zivilgesellschaft im Netz



# 3

## Zivilgesellschaft im Fokus




## Unsere Forderungen



Teil 2

# **Schwerpunkt Digitalisierung:** Gefahren und Chancen für die Zivilgesellschaft im Netz

Weltweit nutzen Staaten und Regierungen das Netz, um unliebsame Stimmen zum Schweigen zu bringen. Oft geschieht das unter dem Vorwand, Hass und Hetze einzudämmen. Gleichzeitig nimmt tatsächlicher Hass auf eine Weise zu, die Regeln für den digitalen Diskurs notwendig macht. Daraus resultieren jedoch noch mehr Möglichkeiten für Überwachung und Zensur. Die Zivilgesellschaft aber findet weiter Wege, digitale Instrumente erfolgreich zu nutzen.

# Internet und Zivilgesellschaft: Der digitale Raum wird enger

Die Idee vom Internet als Freiheitsmedium hat gelitten. Autoritäre Regime setzen digitale Technologien als Kontrollinstrument ein.
Doch das Netz hat noch immer ein großes emanzipatorisches Potenzial.

Es gibt eine alte Erzählung, die sagt: Das Internet ist unzensierbar. Die dezentrale Organisation der Infrastruktur mache sie immun gegen Kontrolle, glaubten viele. Die globale Vielfalt der Stimmen werde fast von allein für Demokratie sorgen, die Körperlosigkeit der Begegnungen für ein Ende von Diskriminierung. „Wir erschaffen eine Welt, in der jede:r Einzelne an jedem Ort die eigenen Überzeugungen zum Ausdruck bringen kann, ohne Angst, zum Schweigen oder zur Konformität gezwungen zu werden", schrieb der US-Bürgerrechtler John Perry Barlow 1996 in seiner „Unabhängigkeitserklärung des Cyberspace".[8]

Als 15 Jahre später der Arabische Frühling anbrach, schien es, als werde diese Utopie wahr. Durch die Straßen Nordafrikas und der Arabischen Halbinsel zogen damals nicht nur Zehntausende Demonstrant:innen und der Geruch von Tränengas, sondern auch die Idee dezentraler und vernetzter Massenproteste. Immer mehr Menschen taten im Netz ihren Unmut über repressive Politik und die katastrophale wirtschaftliche Lage kund, verabredeten sich zu Demonstrationen und teilten Bilder davon, die die staatlichen Medien zurückhielten. Für einen Moment sah es so aus, als würde die arabische Welt mit Hilfe digitaler Medien alle autokratischen Herrscher abschütteln.

## Immer weniger Internetfreiheit

Aus heutiger Sicht weiß man: Die Hoffnung, dass die Aufstände die politische Struktur der Region nachhaltig demokratisieren könnten, hat sich kaum erfüllt. Aktivist:innen aus der Region wurde zudem schnell deutlich, wie eurozentrisch die westliche Rede von „Facebook- und Twitter-Revolutionen" war. Soziale Medien mögen als Verstärker des Protests gewirkt haben, doch das Rückgrat der Aufstände waren lokale Strukturen und oftmals ganz analoge Netzwerke des Widerstands.

Vor allem aber wirkten die Aufstände als Weckruf für die Diktatoren dieser Welt, ihre Regime digital aufzurüsten: Sie installierten Netzsperren und bemächtigten sich der digitalen Infrastruktur, erließen Zensurgesetze und kauften im Westen Überwachungstechnologie. Wo dies schon vorher geschehen war, wurden digitale Protestposts schnell zu Beweismitteln: Unzählige Blogger:innen und Online-Aktivist:innen landeten im letzten Jahrzehnt im Gefängnis. Zum zwölften Mal in Folge konstatierte die NGO Freedomhouse 2021, dass die Internetfreiheit gegenüber dem Vorjahr kleiner geworden ist.[9]

## Internet: Sowohl Hilfe als auch Gefahr

Heute wissen wir, dass Internet beides zugleich ist: Ein Medium der Freiheit und ein Medium der Kontrolle – je nachdem, wie es technisch, sozial und politisch gestaltet wird. In vielen demokratischen Staaten etwa hat das Internet zu einer weiteren Demokratisierung der Öffentlichkeit beigetragen. So viele Menschen wie noch nie haben heute einfachen Zugang zu Wissen, Kultur und Diskursen. Damit haben sich auch die Spielräume zivilgesellschaftlicher Akteur:innen für Organisation und Mobilisierung erweitert, konnten marginalisierte Gruppen sich Gehör verschaffen. Durch das Hashtag-Prinzip von Social-Media-Plattformen wie Twitter konnten beispielsweise die vielen Einzelstimmen Schwarzer US-Amerikaner:innen zu einer politischen Bewegung werden. Vernetzt durch das Schlagwort #BlackLivesMatter waren sie ein mächtiger Chor, der Alltagsrassismus und Polizeigewalt anklagt. Ein anderes Beispiel für kollektive Kraft der Hashtags sind feministische Initiativen wie #Aufschrei in Deutschland, #ShutItAllDown in Namibia[10] oder #MeToo weltweit. Auch wenn sich dadurch allein noch nicht Verhältnisse ändern: Nie zuvor konnten Menschen ihren alltäglichen Erfahrungen mit sexualisierter Gewalt und Diskriminierung so erfolgreich Gehör verschaffen wie heute.

Doch auch rechtspopulistische und rechtsextreme Akteur:innen wissen die neuen Möglichkeiten zu nutzen – oft mit dem Ziel, jene Marginalisierten zum Schweigen zu bringen, die sich gerade erst ermächtigt sahen. Studien zeigen, dass im Netz insbesondere Frauen, queere Menschen und solche mit Migrationshintergrund angefeindet werden und sich immer öfter aus der digitalen Öffentlichkeit zurückziehen.[11] Derweil hat wohl kein Politiker so sehr von den Sozialen Medien profitiert wie Ex-Präsident Donald Trump. Die Targeting-Werkzeuge der Plattformen halfen seinem Wahlkampf 2016, gezielt Schwarze US-Bürger:innen zu demobilisieren,[12] Facebooks

Algorithmen belohnten seine polarisierende Rhetorik und blanke Desinformation mit unglaublicher Reichweite.
Dass im Ringen um die demokratische Öffentlichkeit am Ende nicht diejenigen Akteur:innen die Oberhand behalten, die die Demokratisierung am liebsten rückgängig machen würden, ist keineswegs ausgemacht. Die Situation wird dadurch erschwert, dass mit den Sozialen Medien die wichtigsten Arenen der Netzöffentlichkeit von wenigen hyperkapitalistischen Konzernen betrieben werden. Sie haben Diskurse lange Zeit nur nach eigenem Gutdünken moderiert, geleitet von Profitstreben. Seit Jahren ringt die Politik deshalb darum, wie Plattformkonzerne und mit ihnen die digitale Öffentlichkeit zu regulieren sind.
Nicht selten schießen sie dabei mit hehren Absichten über das Ziel hinaus. Deutschland etwa erhöht über das Netzwerkdurchsetzungsgesetz seit 2017 den Druck auf Facebook und Co., rechtswidrige Inhalte schnell zu löschen. Doch welche Äußerungen verboten sind und welche nicht, ist oft diffizil. Das abzuwägen, bleiben den Klickarbeiter:innen der Plattformen oft nur wenige Sekunden, im Zweifelsfall löschen sie lieber zu viel.[13] Erst 2021 verpflichtete eine Reform des Gesetzes die Unternehmen, ihren Nutzer:innen geordnete Widerspruchsverfahren zu ermöglichen und zu Unrecht gelöschte Inhalte wiederherzustellen. Unterdessen werden Innenminister:innen auch in Demokratien nicht müde, die staatliche Überwachung digitaler Räume auszubauen. Sie wollen Zugang zu verschlüsselten E-Mails und Messengern, verpflichten Telefon- und Internetanbieter zur anlasslosen Vorratsdatenspeicherung von Nutzungsdaten und versuchen, mit Gesichtserkennung & Co. auch die analoge Welt besser im Blick zu haben.

## Digitaler Aufruf, analoger Protest

Diesem wachsenden Kontrolldruck zum Trotz überwiegt in vielen liberalen Demokratien die emanzipatorische Wirkung des Internets. Bürger:innen dokumentieren mit Smartphones Polizeigewalt und rassistische Übergriffe, Aktivist:innen zwingen den Staat zu Transparenz und Blogger:innen schaffen zivilgesellschaftliche Gegenöffentlichkeiten.
Auch die Erfolge von globalen Umweltbewegungen wie Fridays for Future oder Extinction Rebellion wären ohne digitale Hilfsmittel kaum denkbar. Für die Planung von Aktionen, die Organisation von Ortsgruppen und die Koordination von Forderungen sind Messenger und kollaborative Online-Tools unersetzlich. Zudem verstehen die jungen Klimaaktivist:innen wie kaum jemand vor ihnen, analogen Protest und Aktionen des zivilen Ungehorsams mit digitalen Medien zu verbinden.
Auch in Ländern wie Uganda und Indien streiken junge Menschen für das Klima, auch dort bedienen sie sich geschickt der Sozialen Medien. Doch während die Aktivist:innen mit Fakten überzeugen wollen, sind die Sozialen Medien in vielen

## „Wir benutzen Tools, die leicht zugänglich sind“

**Frau Ramolefo, Ihre Organisation Amandla.mobi unterstützt vor allem Frauen mit geringem Einkommen in Südafrika. Sie mobilisieren zu Themen wie geschlechtsspezifische Gewalt, wirtschaftliche Gerechtigkeit, Polizeibrutalität, Ernährungssicherheit, Korruption und Klimawandel. Welche digitalen Tools nutzen Sie für Ihre Kampagnen?**
**Palesa Ramolefo:** Wir benutzen vor allem Tools, die leicht zugänglich sind. Wir wollen, dass sich möglichst viele Menschen an unseren Kampagnen beteiligen können. Und deshalb sind unsere wichtigsten digitalen Hilfsmittel die ganz einfachen Kommunikationsmittel wie SMS, WhatsApp und Social-Media-Kanäle.

**Wie helfen die Ihnen?**
**Palesa Ramolefo:** Ein Beispiel: Es gibt öffentliche Anhörungen des Parlaments, bevor ein neuer Haushalt aufgestellt wird. Eine alte Frau vom Land hat vielleicht nicht die Möglichkeit, zum Parlament nach Kapstadt zu fahren. Sie hat auch kein Smartphone oder ausreichend Datenvolumen, um an Zoom-Meetings zur Anhörung teilzunehmen, möchte sich aber beteiligen. Da helfen wir und geben ihr die Möglichkeit, etwa per SMS oder WhatsApp ihren Beitrag zur Anhörung zu übermitteln, so dass auch ihre Stimme gehört wird – und nicht nur die Stimmen derer, die genug Geld haben und ohne unsere Unterstützung auskommen.

**Mit Erfolg?**
**Palesa Ramolefo:** Aber ja, wir können für unsere Kampagnen durch die Beteiligung vieler sehr viel mehr Druck aufbauen und erzielen spürbare Veränderungen. Wir haben so beispielsweise erreicht, dass die Mehrwertsteuer auf Hygieneartikel wie Tampons und Binden abgeschafft wurde, ein großer Erfolg für viele Frauen mit geringem Einkommen. Und unsere erfolgreiche Data-Must-Fall-Kampagne hat dazu geführt, dass 30 Millionen Menschen leichter Zugang zum Internet bekommen haben. Die großen Mobilfunkanbieter wurden verpflichtet, die Kosten für ihre Produkte zu senken. Vorher waren die Kosten für Menschen mit geringem Einkommen zu hoch.

**Interview mit Palesa Ramolefo** Aktivistin beim Brot für die Welt-Partner amandla.mobi (https://amandla.mobi)

Ländern des Globalen Südens zur Brutstätte von Desinformation, Hass und Gewalt geworden. Denn dort gehen die Plattformen noch weniger effektiv dagegen vor als in den USA und in Europa.

Die Facebook Papers zeigten 2021, wie der Konzern in Indien oder Äthiopien versagt, irreführende Posts und Aufrufe zu Gewalt zu unterbinden. Das Unternehmen gibt schlicht nicht genug Geld für Faktenprüfer:innen, Moderator:innen und algorithmische Erkennungssysteme mit den richtigen Sprachkenntnissen aus. Weil ihre sortierenden Algorithmen Inhalte belohnen, die besonders emotional und polarisierend sind, wirken sie oft wie ein Brandbeschleuniger.

Nichtsdestotrotz finden Menschen in repressiveren Staaten immer wieder Wege, die Sozialen Medien auch für ihren Widerstand zu nutzen. Im Iran etwa, wo Frauen auf Instagram Fotos und Videos von sich beim Tanzen und ohne Kopftuch posteten, um gegen die sexistische Moralpolitik des Mullah-Regimes zu protestieren.[14] Oder in Nigeria, wo sich 2020 vor allem junge Menschen unter dem Hashtag #EndSARS auf Twitter zusammenschlossen, um auf Gewalt durch die Polizeieinheit Special Anti-Robbery Squad (SARS) aufmerksam zu machen und Proteste zu organisieren.[15]

Die Reaktion der Regierenden auf solche Aktionen ist häufig gleich: Sie nutzen ihre Macht über die Telekommunikationsinfrastruktur und lassen den Zugang zu den Diensten sperren. Im Iran sind Facebook und Twitter seit langem nicht zu erreichen, auch Instagram war zwischendurch blockiert. In Nigeria ließ Präsident Muhammadu Buhari als Reaktion auf den Protest Twitter für einige Zeit sperren, in der Türkei war Wikipedia über Jahre unzugänglich. Einigen Menschen gelingt es, die Sperren mit Verschlüsselungs- und Anonymisierungswerkzeugen zu umgehen, doch gegen digitalen Massenprotest sind die Netzsperren oft ein wirksames Mittel.

## Lukrative Märkte, lasche Kontrolle

Immer wieder greifen Regierungen zu noch drastischeren Maßnahmen und lassen das Internet im Land oder einigen Regionen gleich ganz abschalten. 155 Shutdowns dieser Art zählte die NGO Access Now allein in 2020, von Belarus über Myanmar bis nach Indien, das die Liste mit 109 Internetabschaltungen anführt. Insgesamt summierten sich die Shutdowns in dem Jahr auf mehr als 3.000 Tage – insbesondere vor Wahlen oder während Protesten (siehe Seite 41).[16]

Kaum maßvoller sind die in vielen Staaten erlassenen Zensurgesetze für Soziale Medien und andere digitale Räume. Diese werden zwar häufig als Maßnahmen gegen Terrorpropaganda, Cyberkriminalität oder Fake News getarnt. Doch sie zielen mit schwammig formulierten Vorgaben und drastischen Sanktionsmöglichkeiten fast immer darauf ab, den Diskurs im Netz zu kontrollieren, ohne die Dienste gleich ganz sperren zu müssen. Nicht selten berufen sich Machthaber wie der russische Präsident Vladimir Putin oder der türkische Regierungschef Recep Tayyip Erdoğan dabei explizit auf Deutschland und das Netzwerkdurchsetzungsgesetz als Vorbild.[17] Allzu häufig fügen sich die US-Plattformkonzerne, weil sie nicht den Zugang zu lukrativen Märkten verlieren wollen.

## Technisches Katz-und-Maus-Spiel

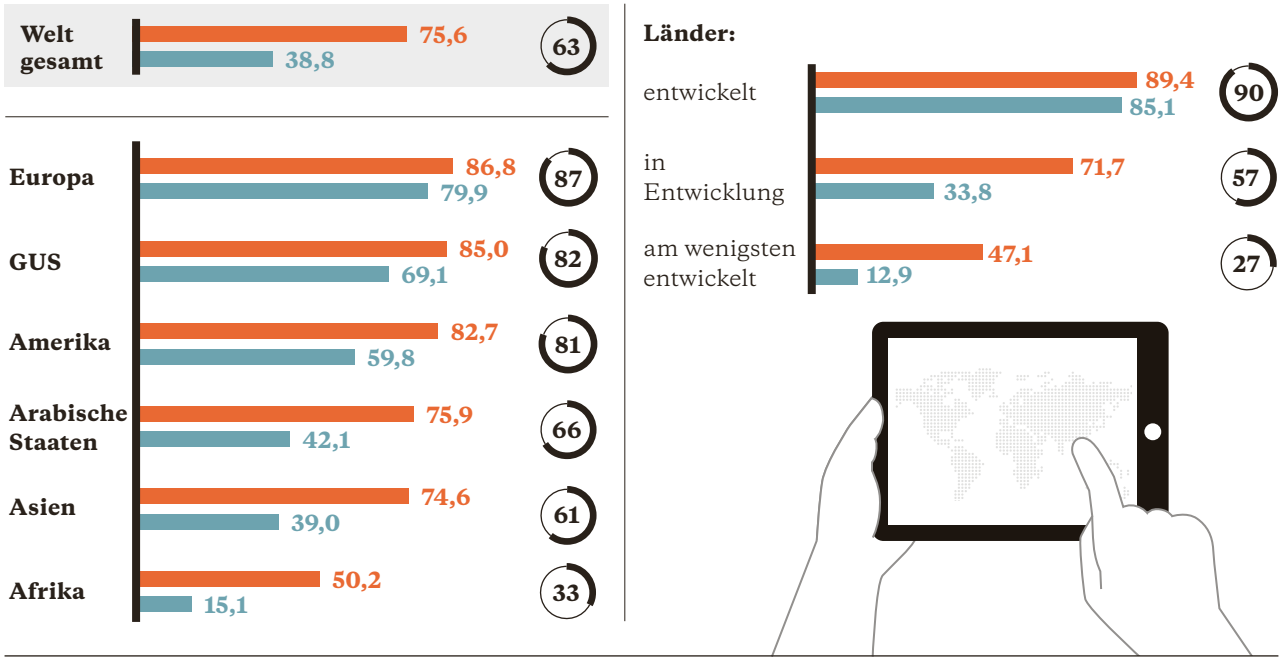
Vervollständigt wird der Instrumentenkoffer der staatlichen Kontrolle digitaler Räume schließlich durch Überwachung. Etwa in Hongkong, wo die Demokratiebewegung ihre Proteste über verschlüsselte Messenger und Bluetooth-Kommunikation organisierte und die Geräte verhafteter Oppositioneller zur Analyse nach China geschickt wurden. Oder in Mexiko (siehe Seite 58), wo mit dem Pegasus-Trojaner Oppositionelle, Journalist:innen und Geistliche überwacht wurden. Nicht erst seit diesem Skandal ist klar: Oft sind es Firmen aus dem Westen, auch aus Deutschland, die den Überwachungsstaat im Globalen Süden mit hochrüsten (siehe Seite 50).

Ein gutes Jahrzehnt nach dem Arabischen Frühling ist klar: Derlei vernetzte Massenproteste sind heute vielerorts kaum noch möglich. Zu fest haben die Autokraten das Internet im Griff, zu gut lassen sich digitale Technologien zur Kontrolle nutzen. Und doch blitzt das emanzipatorische Potenzial als Freiheitsmedium immer wieder auf. Viele Aktivist:innen liefern sich heute ein technisches Katz-und-Maus-Spiel mit den Behörden, umgehen Zensur mit Anonymisierungsdiensten und setzen auf verschlüsselte Messenger.

Dass emanzipatorische Möglichkeiten ausgebaut werden, ist auch eine Aufgabe westlicher Staaten. Zu selten haben sie im Blick, dass sich die eigenen Regulierungsentscheidungen auf die digitalen Räume in weniger demokratischen Staaten auswirken. Wenn etwa deutsche Behörden das Wissen über Schwachstellen in weit verbreiteten IT-Systemen horten, statt diese Sicherheitslücken zu schließen, weil sie sie für digitale Waffen benötigen, dann macht das auch Geräte von Oppositionellen in autoritären Systemen angreifbar. Wenn die Forderung europäischer Innenminister:innen nach Hintertüren zu verschlüsselten Messengern und E-Mails umgesetzt wird, dann gefährdet das auch die Kommunikationsfreiheit von Journalist:innen in repressiven Staaten. Und wenn die EU Plattformen verpflichtet, automatische Upload-Filter gegen Urheberrechtsverletzungen einzurichten, dann freuen sich illiberale Machthaber über die Etablierung einer Infrastruktur, die sich leicht für Zensur missbrauchen lässt. Regierungen und Unternehmen in Europa und den USA tragen eine Mitverantwortung für die digitalen Infrastrukturen weltweit.

## Internet-Nutzung weltweit

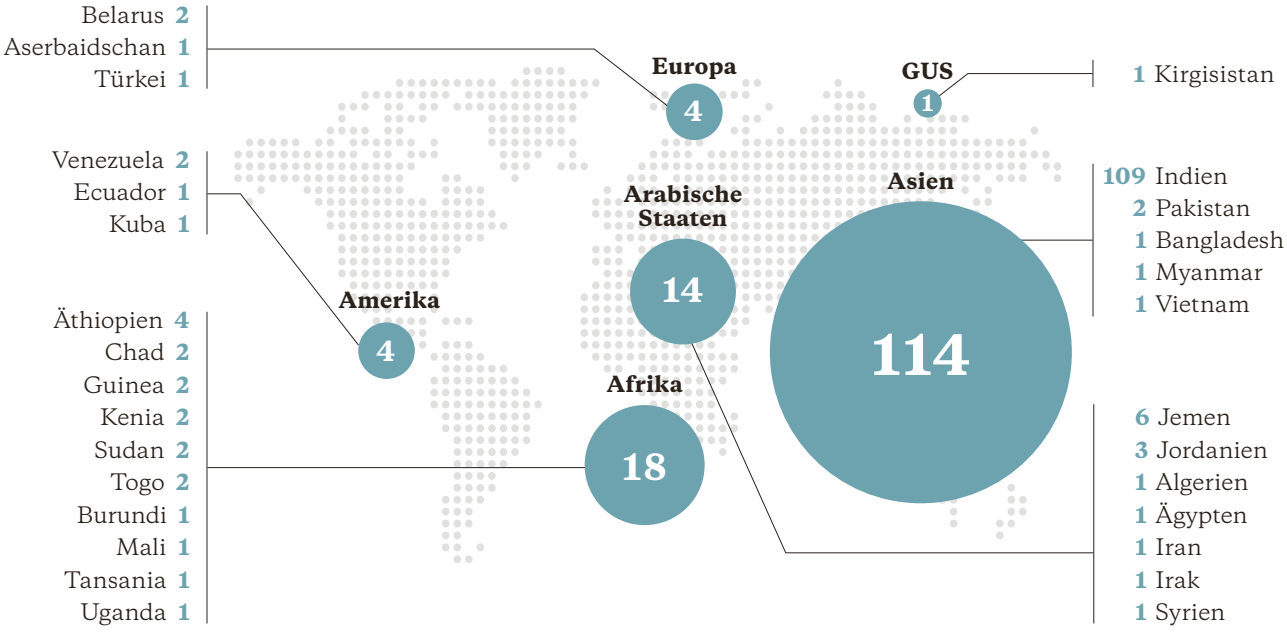
Anteil der Personen, die das Internet nutzen, in Prozent — Stadt — Land (2020) — xx insgesamt (2021)




*Quelle: Internationale Fernmeldeunion (UN ITU) (2021): Measuring digital development, Facts and Figures*

## Internet-Shutdowns weltweit

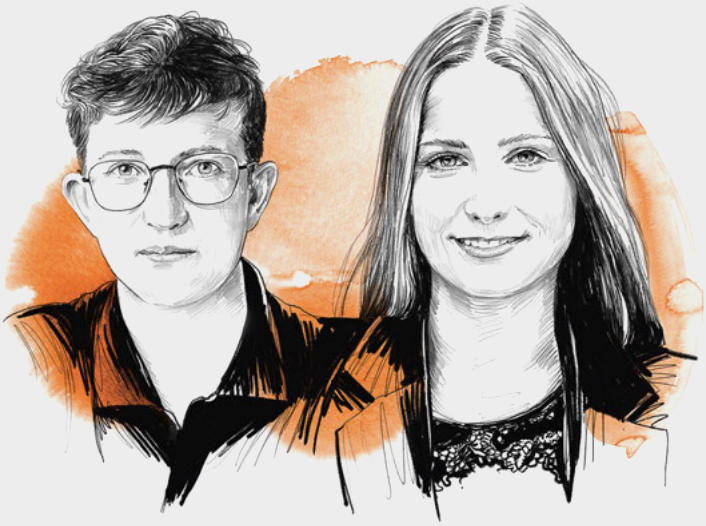
Laut der NGO Access Now haben Regierungen im Jahr 2020 den Zugang zum Internet in insgesamt 29 Ländern 155 Mal blockiert.




*Quelle: Access Now (2021): Shattered Dreams and Lost Opportunities. A year in the fight to #KeepItOn*

# Ist der Rechtsstaat im Netz gefangen?

Vor Provokateur:innen, die jeden Widerspruch aus dem Netz verdrängen wollen, müssen vor allem Angehörige marginalisierter Gruppen geschützt werden. Doch ab wann beschneidet dieser Schutz Grundrechte wie Meinungs- oder Berufsfreiheit?



**Interview mit Josephine Ballon**, Rechtsanwältin und Head of Legal bei HateAid, und **Felix Reda**, Projektleiter bei der Gesellschaft für Freiheitsrechte

**Frau Ballon, Ihre Organisation betreut Betroffene von Hasskommentaren im Netz. Mit Ihrer Unterstützung erstritt die Grünen-Politikerin Renate Künast Anfang Februar 2022 einen Erfolg beim Bundesverfassungsgericht. Es kam zum Schluss, dass die Entscheidungen des Land- und Kammergerichts Berlin gravierende handwerkliche Fehler aufwiesen: Die beiden Gerichte hatten die größtenteils anonymen sexistischen Beleidigungen, die Künast auf ein nicht von ihr erstelltes Meme mit einem Falschzitat erhielt, als von der Meinungsfreiheit gedeckt angesehen. Glauben Sie, dass das Urteil der obersten Richter:innen Menschen in Zukunft abschreckt, wüste Beschimpfungen zu posten?**

**Josephine Ballon:** Das hoffe ich! Nach dem Urteil des Bundesverfassungsgerichts wird den zehn Verfasser:innen der am Ende zehn beanstandeten Kommentare hoffentlich das Herz in die Hose gerutscht sein. Jetzt muss das Kammergericht die Kommentare erneut überprüfen. Aber wir erhoffen uns natürlich, dass davon ein Empowerment für die Betroffenen ausgeht. Und alle Täterinnen und Täter sehen, dass Konsequenzen auf sie zukommen können. Sie merken jetzt: Es gibt keine absolute Anonymität im Internet.

**Herr Reda, Sie beschäftigen sich in Ihrer Arbeit bei der Gesellschaft für Freiheitsrechte mit dem Spannungsfeld zwischen Meinungsfreiheit und Rechtsverstößen im Netz. Wie bewerten Sie das Urteil?**

**Felix Reda:** Ich bin mit dem Ausgang des Verfahrens ebenfalls zufrieden. Es ist gut, dass nicht Facebook allein entschieden hat, ob die persönlichen Daten weitergegeben werden oder nicht. Dennoch war die Kritik an der ersten Entscheidung des Landgerichts berechtigt. Auch wenn man besorgt ist darüber, wie willkürlich teilweise Online-Plattformen Meinungen sperren, ist es trotzdem sinnvoll und im Interesse aller, dass die Gerichte bei einer solchen Grundrechtsabwägung die Gesamtsituation miteinbeziehen und im Zweifelsfall sagen, dass eine bestimmte Aussage nicht in Ordnung war. Andernfalls wäre es für Personen, die sich politisch engagieren oder zu gesellschaftlich umkämpften Themen Stellung nehmen, kaum noch möglich, am öffentlichen Diskurs teilzunehmen.

**In einem anderen Fall hat der Chat-Dienst Telegram auf Druck der deutschen Bundesregierung 64 Kanäle gesperrt. Sie haben einmal gewarnt, solche Vorschläge und Aktionen kenne man sonst nur von autokratischen Regimen wie Russland. Der Ruf nach technischen Lösungen für ein gesellschaftliches Problem drohe zur Gefahr für die Grundrechte zu werden. Warum ist in diesem Fall eine Sperrung gerechtfertigt?**

**Felix Reda:** Mein Kommentar bezog sich auf einen anderen Sachverhalt. Da ging es um die Forderung eines Landesinnenministers, Telegram in Deutschland ganz zu sperren. Das ist etwas völlig anderes als das, was Telegram jetzt gemacht hat: nämlich einzelne Kanäle zu sperren, in denen immer wieder rechtswidrige Äußerungen gefallen waren. Das wäre sonst, als nehme man einen Fernsehsender offline, weil eine bestimmte Sendung rechtswidrig war. Etwas anderes

ist es, politisch auf eine Plattform wie Telegram Einfluss zu nehmen, damit sie sich an europäisches Recht hält. Man muss sich auch der Geschichte einer solchen Plattform bewusst sein. Telegram wurde gegründet, um eine Gegenstimme zum russischen Regime zu sein. International ist es schwer zu sagen: Wenn sich alle an Recht und Gesetz halten, ist für die Meinungsfreiheit gesorgt. Es gibt viele Staaten auf der Welt, in denen eine Gegenöffentlichkeit nötig ist.

**Nach welchen Kriterien werden solche Sperrungen entschieden?**

**Felix Reda:** Das ist nach wie vor eine große Baustelle. Nicht nur bei Telegram, sondern bei so ziemlich allen Plattformen – also auch bei Facebook, Instagram, TikTok oder YouTube. Bei allen können die Betroffenen oft nicht nachvollziehen, was der Grund für eine Sperrung war. Sie mag im Einzelfall gerechtfertigt sein. Aber man hat dennoch ein Anrecht darauf zu erfahren, auf welcher Grundlage eine Entscheidung getroffen wurde, und sie anzufechten. Was immer deutlicher wird, ist, dass Online-Plattformen keine normalen privatwirtschaftlichen Unternehmen sind, sondern wichtige Diskursräume, die für bestimmte Gruppen entweder Grundlage für die Ausübung ihrer Meinungsfreiheit oder ihrer Berufsfreiheit sind.

**Können Sie uns ein Beispiel nennen?**

**Felix Reda:** Wir hatten es zu tun mit einer Gruppe türkischer Exiljournalist:innen, die von Deutschland aus einen YouTube-Kanal betreiben für das Publikum in der Türkei. In diesem setzen sie sich kritisch mit der Politik der Regierung Erdoğan auseinander. Wegen angeblicher Urheberrechtsverletzungen wurden die Videos von YouTube immer wieder gesperrt. Es war für die Journalist:innen extrem schwierig, einen echten Menschen bei YouTube zu kontaktieren. Mit unserer Hilfe haben sie dann jemanden erreicht, der sich diesen Fall angesehen und festgestellt hat, dass die Sperrvorlagen unberechtigt waren. Sie waren offensichtlich politisch motiviert, um kritische Berichterstattung zu unterbinden. Je größer eine Plattform wird, umso mehr Verantwortung trägt sie dafür, dass auf ihr die Grundrechte ausgeübt werden können.

**Frau Ballon, wie gehen Sie mit dem Spannungsfeld um zwischen Hassbotschaften, die strafrechtlich verfolgt werden müssen, und dem Grundrecht darauf, die eigene Meinung äußern zu dürfen?**

**Josephine Ballon:** Wir wissen, dass unsere Arbeit in diesem Spannungsfeld stattfindet. Aber Meinungsfreiheit ist keine Einbahnstraße. Sie gilt auch nach dem Grundgesetz nicht schrankenlos. Sie hat ihre Grenzen dort, wo die Rechte anderer schützenswerter sind. Wir sehen, dass die Meinungsfreiheit vor allem in den Sozialen Medien missbraucht wird von strategisch arbeitenden Gruppierungen. Vieles davon kommt aus dem rechten und rechtsextremen Spektrum. Im Jahr 2020 waren das laut Bundeskriminalamt 62 Prozent der erfassten politisch motivierten Hasskommentare. In diesen Kreisen kursieren auch Leitfäden, dass man sich zum Beispiel vor allem auf junge Studentinnen stürzen solle, weil sie besonders leicht mundtot zu machen seien. Wir sehen europaweit in Studien, dass sich nicht nur die angegriffenen Personen selbst danach überlegen, ob sie sich zu einem bestimmten Thema noch äußern wollen, sondern auch die Mitlesenden, die erleben, wie schutzlos andere digitaler

## Netzwerkdurchsetzungsgesetz und Digital Services Act: Wie die EU und Deutschland das Netz regulieren

**Netzwerkdurchsetzungsgesetz (NetzDG):** Das „Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken“ verpflichtet Social-Media-Plattformen seit 2017, gegen rechtswidrige Posts vorzugehen. Unter anderem müssen sie innerhalb von 24 Stunden „offensichtlich rechtswidrige Inhalte“ löschen, die von Nutzer:innen gemeldet wurden. Sonst drohen Bußgelder in Millionenhöhe. Das NetzDG gilt für Plattformen mit mehr als zwei Millionen Nutzer:innen in Deutschland. Eine abschließende Liste führt die Bundesregierung nicht. Doch mindestens Facebook, Twitter, YouTube, Instagram, Reddit, TikTok, Change.org und SoundCloud haben die vorgeschriebenen Transparenzberichte veröffentlicht. Seit 2021 müssen die Unternehmen ihren Nutzer:innen ein Widerspruchsverfahren anbieten, seit 2022 potenziell strafrechtlich relevante Inhalte mit IP-Adresse an das Bundeskriminalamt melden.

**Digital Services Act (DSA):** Das „Gesetz über Digitale Dienste“ soll den Anbieter:innen von Online-Diensten in der Europäischen Union umfassende Regeln vorgeben. Der Ende 2020 von der EU-Kommission vorgelegte Verordnungsvorschlag betrifft auch den Bereich des NetzDG, geht aber darüber hinaus. Der DSA soll nicht nur vereinheitlichen, wie mit rechtswidrigen Inhalten umzugehen ist, sondern enthält auch weitergehende Vorgaben zur Haftung der Unternehmen für Inhalte ihrer Nutzer:innen, zu Online-Werbung, zum Betrieb von Online-Marktplätzen und zur staatlichen Aufsicht über die Dienste. Der Gesetzgebungsprozess war bei Redaktionsschluss noch nicht abgeschlossen.

Gewalt ausgesetzt sind. 2019 gab es eine Erhebung, dass sich schon die Hälfte der Internetnutzenden in Deutschland nicht mehr traut, ihre politische Meinung im Netz zu äußern. Deshalb müssen wir Rahmenbedingungen schaffen, die es allen Seiten des politischen Spektrums erlaubt, sich in den Sozialen Medien sicher zu bewegen. Diese sind ja inzwischen die wichtigsten Plattformen für den öffentlichen Austausch. Sonst ziehen sich vor allem marginalisierte Gruppen und Menschen zurück, die sich für gesellschaftliche Werte stark machen: Aktivist:innen, Journalist:innen und Politiker:innen, vor allem auf kommunaler Ebene. Wir wissen, dass schon 19 Prozent der Kommunalpolitiker:innen in Deutschland aufgrund von digitaler Gewalt nicht erneut kandidieren oder gar ihr Amt niederlegen wollen.

**Herr Reda, ein solcher Rahmen soll mit dem sogenannten Netzwerkdurchsetzungsgesetz, kurz: NetzDG geschaffen werden. Es ist aber stark umstritten, weil es offensichtlich zu Overblocking führt, also zum übermäßigen Sperren legaler Inhalte. Was sagen Sie?**

**Felix Reda:** Das NetzDG hat Licht und Schatten. Auf der einen Seite wurden einige grundsätzliche Dinge richtig gemacht. So werden beispielsweise Plattformen nicht für jeden einzelnen Inhalt direkt haftbar. Das würde sonst dazu führen, dass die Plattformen auf Anfrage einfach alles sperren würden, weil das Haftungsrisiko sonst zu groß wäre. Die Plattformen müssen bestimmte Sorgfaltspflichten erfüllen, so dass bei offensichtlichen Rechtsverstößen auch eine unverzügliche Steuerungspflicht eintritt – aber nicht bei Fällen, über die sich Gerichte jahrelang streiten würden.

**Und der Schatten?**

**Felix Reda:** Zum Beispiel bei der Pflicht der Plattformen, Informationen ans Bundeskriminalamt weiterzugeben. Das ist aus meiner Sicht grundrechtswidrig. Denn damit werden private Daten weitergegeben von Menschen, bei denen noch gar nicht klar ist, ob sie illegale Aussagen gemacht haben. Starre Löschfristen schaffen zudem einen Anreiz, dass Plattformen im Zweifel lieber zu viel sperren als zu wenig. Und ein dritter Punkt: Deutschland ist mit dem Gesetz vorgeprescht und hat damit anderen Ländern in gewisser Weise eine Blaupause gegeben: Die Türkei etwa hat mit Verweis auf das NetzDG ihr eigenes Plattform-Gesetz verteidigt – dabei schränkt dieses Gesetz die Meinungsfreiheit massiv ein.

**Frau Ballon, wie sehen Sie das?**

**Josephine Ballon:** Das NetzDG ist ein guter Anfang mit einigen Geburtsfehlern, die jetzt zum Teil nachgebessert und zum Teil verschlimmbessert wurden. Dass Deutschland vorgeprescht ist, finde ich gar nicht so negativ. Wenn das nicht passiert wäre und nicht einige andere Länder nachgezogen hätten, wäre der europäische Wille zu einer Regulierung im Rahmen des Digital Services Act nicht aufgekommen.

**Und wo sehen Sie die Schwachstellen?**

**Josephine Ballon:** Ich bedaure, dass es auf europäischer Ebene kaum Bereitschaft gibt, sich mit den Lehren aus dem NetzDG auseinanderzusetzen. Man muss leider sagen: Wo immer man den Plattformen Interpretationsspielraum lässt, werden sie ihn bis zum Maximum zu ihren Gunsten ausreizen. Ich habe auch mit den Plattformen relativ wenig Mitleid, wenn es immer heißt: Ach, die armen Plattformen sind doch keine Richter – wie sollen die entscheiden können, was illegal ist und was nicht? Dafür muss man sich eben den entsprechenden Sachverstand ins Haus holen, wenn das notwendig ist, um den gesellschaftlichen Gefahren zu begegnen.

**Was vermissen Sie?**

**Josephine Ballon:** Klare Vorgaben zu Löschpflichten, am besten mit Deadlines. Leider sieht der Digital Services Act diese nicht vor, da es hierfür auf europäischer Ebene keinen politischen Willen gibt. Es heißt, das ginge nicht, weil dann massenhaftes Overblocking entstehe. Dafür gibt es aber keine Belege.

**Herr Reda, sehen Sie diese Schwachstelle ebenfalls?**

**Felix Reda:** Nein. Der Grund, weshalb es im Digital Services Act keine Löschfristen gibt, ist ganz einfach: Das NetzDG ist ein Spezialgesetz, das sich an ganz bestimmte große kommerzielle Plattformen richtet und ihnen Verhaltenspflichten auferlegt, um bestimmte Straftatbestände zu bekämpfen. Der Digital Services Act auf der anderen Seite ist eben nicht die europäische Reaktion auf das NetzDG. Er ist ein umfassendes horizontales Regulierungsinstrument, das alle Onlinedienste betrifft: vom Internetzugangsanbieter über Webseitenbetreiber bis hin zu großen Social-Media-Plattformen oder Diensten wie Amazon. Für so unterschiedliche Plattformen und Inhalte starre Löschfristen vorzugeben, würde tatsächlich zu Overblocking führen. Auch beim NetzDG können wir durchaus Missbrauch beobachten: In dem Moment, in dem privatwirtschaftliche Unternehmen angehalten sind, automatisch auf bestimmte Eingaben von außen zu reagieren, kann beispielsweise das massenhafte Reporting von Accounts marginalisierter Gruppen durch Provokateur:innen zur Sperrung von Accounts führen, weil keine richtige inhaltliche Prüfung stattfindet.

## Das ist bei der Regulierung von Tech-Konzernen zu beachten

Vorschläge und Warnungen der NGO Freedom House


*Quelle: Freedom on the Net (2021):The Global Drive to Control Big Tech*

**Und geht der Digital Services Act die Regulierung von Online-Diensten richtig an?**

**Felix Reda:** Ein positiver Aspekt ist, dass Plattformen sich selbst Regeln geben können in Form von Allgemeinen Geschäftsbedingungen. Es wäre falsch, es so zu handhaben, wie das zum Beispiel die polnische Regierung vorgeschlagen hat: Danach müssten Plattformen einfach alles online lassen, was nicht gegen Gesetze verstößt. Das ist zu einfach gedacht.

**Warum?**

**Felix Reda:** Es würde ja bedeuten, dass etwa die Wikipedia nichts löschen darf, was nicht gegen Gesetze verstößt. Für eine Enzyklopädie sind aber ganz andere Kriterien wichtig als nur die Legalität einer Aussage – beispielsweise ob sie belegt ist oder ob sie zum Thema des Eintrags passt. Der Digital Services Act sagt: Die Plattformen dürfen sich eigene Regeln geben, aber müssen bei der Durchsetzung dieser Regeln transparent vorgehen. Sie dürfen nicht willkürlich handeln und müssen die Grundrechte wahren.

**Kann der Digital Services Act Strahlkraft über die EU hinaus entfalten?**

**Felix Reda:** Gerade Länder im Globalen Süden werden weiterhin das Problem haben, dass sie einfach wirtschaftlich nicht wichtig genug sind für diese Unternehmen, um im gleichen Maße eigene Regeln durchsetzen zu können. Man kann aber darauf hoffen, dass Gesetze wie der Digital Services Act auch Ausstrahlung über Europa hinaus haben. Oftmals ist es für Plattformen leichter, bestimmte Änderungen global umzusetzen als nur in einem einzelnen Land oder nur in der EU.

**Was denken Sie, Frau Ballon?**

**Josephine Ballon:** Es muss auch noch eine gesellschaftliche Komponente hinzukommen. Wir haben lange darauf gehofft, dass die Plattformen irgendwann ein eigenes soziales Gewissen entwickeln würden – mussten dann aber feststellen, dass das leider nicht passiert ist. Auf der anderen Seite haben wir erlebt, dass gerade bei den großen Plattformen die Werbeeinnahmen ein wahnsinnig wichtiges Instrument sind. Aktionen wie „Stop Hate for Profit" haben offensichtlich etwas bewirkt: Große Unternehmen haben ihre Werbeetats von Facebook abgezogen, um Verbesserungen zu verlangen. Und es gibt immer mehr Unternehmen, die sagen: Ich möchte nicht, dass mein Produkt neben einem Enthauptungsvideo gezeigt wird.

**Und die Nutzer:innen?**

**Josephine Ballon:** Es gibt in unserer Gesellschaft schon einen starken Trend etwa zu Nachhaltigkeit. Ein ausgeprägtes gesellschaftliches Bewusstsein kann auch dabei helfen, den Druck auf die Plattformen zu erhöhen. Das wirkt. Denn denen geht es am Ende ja nicht darum, die Welt zu vernetzen, sondern wirtschaftlich profitabel zu sein.

# Facebook: Brandbeschleuniger für Konflikte

Hassrede, Datenmissbrauch, Desinformation – Facebook verspricht Zusammenhalt. Doch nicht nur im Globalen Süden zeigt sich: Der Plattformkonzern ist eine Gefahr für Demokratie und Gesellschaft.

Die Welt näher zusammenbringen, das ist nach eigener Aussage die Mission von Meta. Tatsächlich ist das Flaggschiff des Plattformkonzerns, der bis vor Kurzem noch Facebook hieß, das wohl erste wirklich globale Soziale Netzwerk: Facebook wird von Menschen in allen Regionen der Erde genutzt, knapp drei Milliarden monatliche Nutzer:innen hat der Dienst. Hinzu kommen WhatsApp und Instagram. Wäre Facebook ein Land, es wäre der mit Abstand bevölkerungsreichste Staat.

Doch ob die Bevölkerung dort sicher wäre, ob Frieden und Gerechtigkeit herrschen würden, daran darf gezweifelt werden. Standen im Nachgang des Arabischen Frühlings lange die von Facebook eröffneten Möglichkeiten für zivilgesellschaftliche Mobilisierung im Fokus, so ist die Kritik an Firmengründer Mark Zuckerberg zehn Jahre später so laut wie nie. Facebook scheitert an der eigenen Mission. Statt zu verbinden und zu empowern, fördert die Plattform allzu oft Chaos und Gewalt.

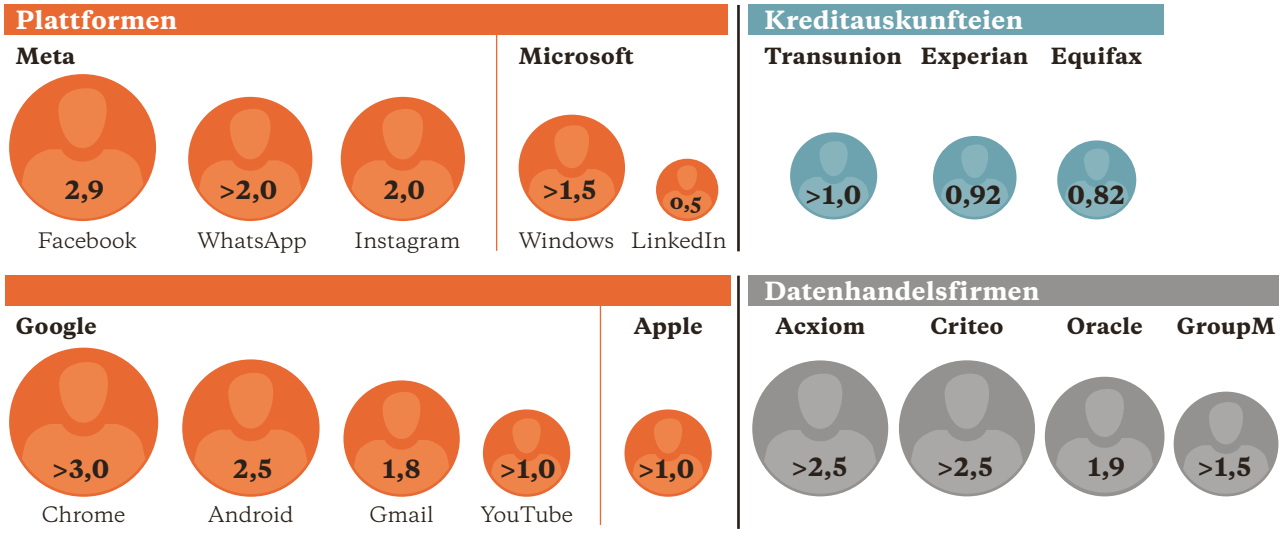
Selbst das Unternehmen kommt zu diesem Schluss. Zahlreiche interne Dokumente, die die ehemalige Facebook-Angestellte Frances Haugen 2021 zugänglich machte, zeigen: Während Instagram sich toxisch auf die Psyche junger Menschen auswirkt, hat Facebook häufig den gleichen Effekt auf das gesellschaftliche Klima.[18] Aktivist:innen aus dem Globalen Süden warnen seit Jahren: In liberalen Staaten mit gefestigter demokratischer Öffentlichkeit mag die Plattform schädlich wirken – Stichwort Donald Trump. In politisch fragileren Regionen aber, in denen Facebook oft die einzige Form der digitalen Öffentlichkeit bildet, wirkt sie geradezu verheerend.

## Einen Markt nach dem anderen erobert

Gemäß Zuckerbergs Motto „Move fast and break things" hat Facebook im vergangenen Jahrzehnt einen Markt nach dem anderen erobert – ohne sich für kulturelle Besonderheiten oder die politische Situation zu interessieren. Mehr als 70 Prozent der Nutzerschaft lebt nach Schätzungen des

## Sammelwut der Tech-Konzerne

So viele Menschen werden von den Firmen erfasst, in Milliarden.




Die Zahlen beruhen auf Angaben der Unternehmen aus den vergangenen Jahren.

Konzerns außerhalb von Europa und Nordamerika. Derweil gibt Facebook 87 Prozent des Budgets zur Klassifizierung von Fehlinformationen für die USA aus, wie die Facebook Papers zeigen. Für den Rest der Welt bleiben 13 Prozent.
In Myanmar etwa, wo seit Mitte der 2010er-Jahre ein Völkermord an der ethnischen Minderheit der Rohingya verübt wurde, ließ Facebook die Verbreitung von Gewaltaufrufen gegen die Volksgruppe zu. Eine Gruppe burmesischer NGOs und ein Report des Human Rights Council der UN stellten 2018 fest: Facebooks fehlende Moderation trug substanziell zur Gewalt bei.[19] Der Konzern hatte nicht genug Moderator:innen mit entsprechenden Sprachkenntnissen beschäftigt, um seine eigenen Regeln durchzusetzen und Hass einzudämmen.

## Via Posts zu Gewalt aufgerufen

Wie die Facebook Papers zeigen, wiederholt sich ähnliches in Äthiopien, wo seit Ende 2020 Bürgerkrieg herrscht.[20] Mitarbeiter:innen des Netzwerks warnten wiederholt davor, dass „problematische Akteure" Desinformationen verbreiten und zu Gewalt aufrufen. Doch Facebook passte seinen Moderationsaufwand nicht an. Für die 115 Millionen Einwohner:innen waren nur sechs Faktenprüfer:innen mit entsprechenden Sprachkenntnissen angestellt. Facebooks Algorithmen konnten Hate Speech lange Zeit nicht in Oromo und Amharisch verstehen, den verbreitetsten Sprachen im Land.
Interne Untersuchungen zeigen auch: Facebook scheitert nicht nur daran, Konflikte einzudämmen, es funktioniert selbst oft als Brandbeschleuniger. Dass die Plattform Emotionalisierung, Polarisierung und Desinformation fördert, liegt in der Logik ihres Geschäftsmodells.[21] Denn Geld verdient Facebook damit, die Aufmerksamkeit der Nutzer:innen an Werbekunden zu vermarkten. Für dieses Geschäft betreibt das Unternehmen eine der größten Datensammlungen der Welt. Was Werbekunden helfen soll, die Menschen zu erreichen, die sie am besten beeinflussen können, ist anfällig für Missbrauch und Manipulation. Zudem optimiert Facebook alle Prozesse so, dass Menschen möglichst lange auf der Plattform verbringen. Die Algorithmen, die die Kommunikationsflüsse bei Facebook sortieren, bevorzugen deshalb Beiträge, die viele Likes, Shares, Kommentare oder Emojis auslösen. Doch virale Beiträge enthalten laut einem internen Bericht von 2020 viermal so oft Falschinformationen wie andere.[22]
Es ist diese Kombination aus Datafizierung und Aufmerksamkeitsmaximierung, die Facebook so gefährlich und gleichzeitig so erfolgreich macht. Der Konzern gehört zu den wertvollsten der Welt, machte allein 2020 einen Netto-Gewinn von 29 Milliarden Dollar. Dass Facebook diesen Kurs von selbst ändert, ist nicht wahrscheinlich.

## „Kritisch analysieren, Quellen vergleichen"

**Frau Castañeda, Ihre Organisation CALANDRIA schult in Peru NGOs oderJournalist:innen in der Kommunikation. Klappt das dank Digitalisierung besser als vor 30 Jahren?**
**Marisol Castañeda:** Ja. Digitale Medien haben etliche Vorteile für unsere Bildungsarbeit: Wir erreichen über Lern-Plattformen wie Moodle oder Classroom sehr viel mehr Menschen. Digitalisierung ermöglicht, Wissen zu vermitteln und auszutauschen. Und sie erlaubt unseren Zielgruppen mehr Autonomie.

**Gibt es auch Nachteile?**
**Marisol Castañeda:** Die Menschen konsumieren heute mehr Informationen, auch Fake News. Für uns bedeutet das: Wir müssen in unseren Kursen noch stärker als bislang digitale Kompetenzen vermitteln: Kritisch analysieren, Quellen vergleichen.

**Erreichen Sie alle, die Sie erreichen wollen?**
**Marisol Castañeda:** Nein. Es gibt Gruppen, die digital ausgegrenzt sind und nicht an Sitzungen oder Workshops teilnehmen können. Das betrifft vor allem Ältere, Analphabeten – und Frauen. Hier ist die digitale Kluft besonders groß. Viele haben kein Smartphone. Oder müssen es mit den Kindern oder dem Mann teilen, damit die am virtuellen Schulunterricht teilnehmen oder arbeiten gehen können. Nur jeder siebte Peruaner besitzt einen PC oder Laptop. Im Amazonasgebiet, aber auch in den Anden, haben 70 bis 80 Prozent aller Haushalte nicht mal Internet. Dort braucht es weiterhin Anrufe, SMS und Gemeinschaftsradio, um alle anzusprechen.

**Braucht es auch persönliche Treffen?**
**Marisol Castañeda:** Ja. Ich verstehe Bildungsprozesse und Kommunikation als Dialog, und das impliziert Empathie und ein sich Kennenlernen. Kein digitales Werkzeug kann physische Treffen voll ersetzen. Man erfährt im Video-Meeting zwar, was jemand sagt. Aber nicht wirklich, was für ein Mensch das dort auf dem Bildschirm ist. Da geht etwas verloren.

**Was raten Sie anderen NGOs?**
**Marisol Castañeda:** Medienerziehung fördern und die digitale Kompetenz stärken, auch die eigene.

---

**Interview mit Marisol Castañeda** Präsidentin des Brot für die Welt-Partners CALANDRIA (www.calandria.org.pe)

# Kontrolle durch biometrische Überwachung

Wer in Indien keinen Fingerabdruck vorzeigt, bekommt kein verbilligtes Kochgas oder keine Rente mehr. Auch andere Staaten digitalisieren ihre Sozialleistungen, häufig mit der Hilfe von privaten Unternehmen. Die Risiken sind immens.

Kaum eine Technologie ruft europäische Menschenrechtsorganisationen und Aktivist:innen derzeit so auf den Plan wie Gesichtserkennung und biometrische Datenerfassung. „Holt euch euer Gesicht zurück!“, ruft eine gemeinsame Kampagne von zig Organisationen für digitale Grundrechte, die derzeit eine Million Unterschriften sammeln will. Ihre Forderung: Die EU soll alle Formen biometrischer Überwachung im öffentlichen Raum verbieten. Ihre Argumente: Biometrische Massenüberwachung bedroht sonst Grundrechte wie das Recht auf Redefreiheit, Versammlungsfreiheit oder das Recht auf Privatsphäre.

Doch während in der EU um die Einsatzmöglichkeiten und Gefahren von Biometrie gestritten und die Regulierung der künstlichen Intelligenz (der AI Act; siehe Seite 54) in Arbeit ist, die Hochrisikotechnologien in den Blick nimmt, setzen andere Staaten bereits biometrische Erfassung im ganz großen Stil ein.

Die größte biometrische Datenbank der Welt befindet sich in Indien. Das Identifikationssystem Aadhaar erfasst laut Regierung rund 1,4 Milliarden Menschen, das sind 99 Prozent der Bevölkerung. Der Aufbau der Datenbank wurde mit Geldern des Weltbank-Vorhabens ID for Development (ID4D) finanziert, das weltweit digitale Identifizierungssysteme entwickelt.[23] Für Indiens Regierungschef Narendra Modi ist die Datenbank eine wichtige Säule seiner „Digital India“-Kampagne, mit der er Indien fit für die Zukunft machen will. Derartige Systeme bergen jedoch gesellschaftliche Risiken: Sie können den Schutz der Persönlichkeit und die soziale Sicherheit bedrohen, fürchtet IT for Change, eine Partnerorganisation von Brot für die Welt im Land.

## So funktioniert Gesichtserkennung

Gesichtserkennung ist ein biometrisches Verfahren, mit dem sich Personen identifizieren lassen oder ihre Identität bestätigen können. Technisch wird dazu das Gesicht einer Person von einer Kamera zunächst erfasst. Dann analysiert eine Software die Geometrie des Gesichtes: Wichtige Faktoren sind etwa der Abstand zwischen den Augen oder der zwischen Stirn und Kinn. Die charakteristischen Züge eines Gesichtes werden dann zu Daten umgerechnet, das Gesicht wird zu einer mathematischen Formel und ist so einzigartig wie ein Fingerabdruck.

Dieser Abdruck kann mit einer Datenbank anderer bekannter Gesichter abgeglichen werden, um eine Übereinstimmung festzustellen. Dabei unterscheidet man zwischen 1-zu-1-Abgleich (ist die Person die, für die sie sich ausgibt?) und 1-zu-vielen-Abgleich (ist diese Person auf einer Liste von gesuchten Personen?). Letzteres setzen oft Strafverfolgungsbehörden ein.

## Für jede Person eine 12-stellige Nummer

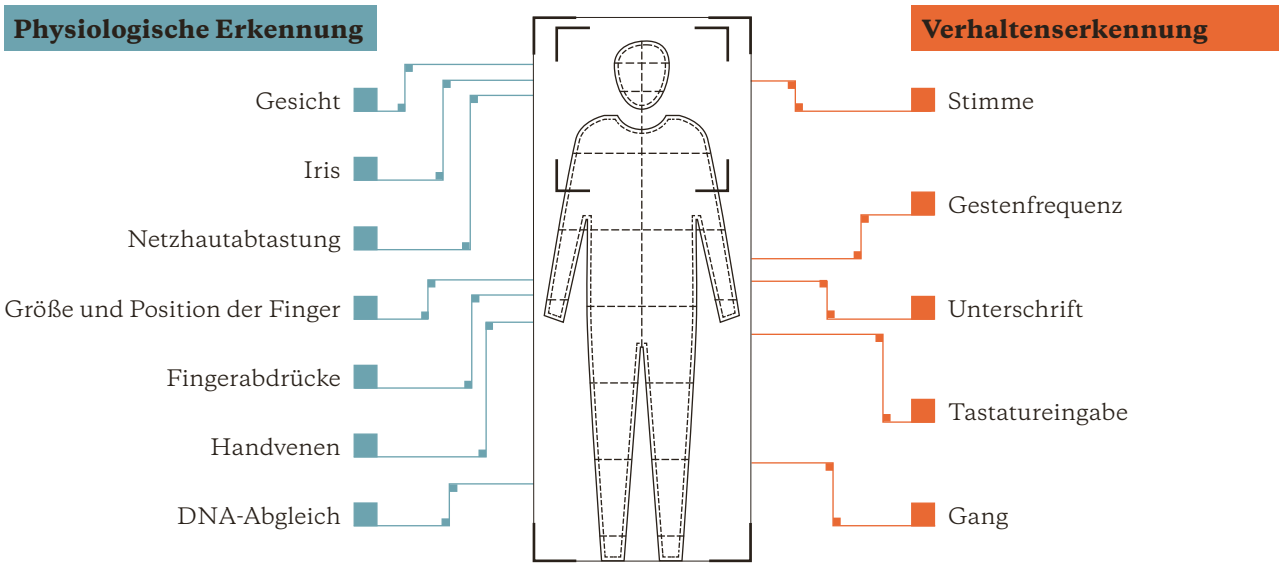
Wie funktioniert das System? Indiens Identifizierungsbehörde UIDAI vergibt an jede erfasste Person eine zwölfstellige Nummer (Aadhaar), unter der sie Angaben wie etwa Name, Geschlecht, Geburtsdatum und Adresse, aber auch biometrische Daten wie Fingerabdrücke, Iris-Scans und Fotos speichert. UIDAI hat diese Arbeit an sogenannte Registrare ausgelagert, das sind neben Behörden auch Privatunternehmen wie Banken und Versicherungen.

Diese wiederum dürfen Subunternehmen mit der Eintragung der Bürger:innen in das Aadhaar-System beauftragen. Obwohl es bis heute keinen gesetzlichen Persönlichkeitsschutz gibt, der verhindert, dass die so gespeicherten Daten weitergegeben oder gestohlen werden können, ist der Eintrag in die biometrische Datenbank Voraussetzung, um zahlreiche staatliche Dienstleistungen in Anspruch zu nehmen. Ohne Aadhaar kein subventioniertes Kochgas, keine Rentenzahlungen, Stipendien oder Jobs. Inzwischen verlangen auch immer mehr private Unternehmen die Aadhaar-Nummern: Banken für Konten und Kredite, Telekomfirmen für Sim-Karten, Versicherungen für ihre Policen sowie Start-ups für Dienstleistungen.[24]

Diese Digitalisierung der staatlichen Leistungen bedroht vor allem die ärmsten Inder:innen in ihrer sozialen Sicherheit. Aufgrund fehlender Aadhaar-Nummern wurden Millionen Menschen Lebensmittelrationen verweigert, Kinder von der Einschulung oder Schulspeisungen ausgeschlossen und alten Menschen die Rentenzahlungen gestoppt. Die Lesegeräte, mit denen die Fingerabdrücke geprüft werden, sind oft ebenso unzuverlässig wie die Internet- oder Mobilfunkverbindungen. Und wer schwer mit seinen Händen arbeitet, dessen Fingerabdrücke sind für die Scan-Geräte häufig unleserlich. Auch bei Augenkrankheiten versagen die Iris-Scanner oft.

## So erkennen Maschinen Menschen

Jeder Mensch ist einzigartig – das wird häufig missbraucht.




*Quelle: Brot für die Welt*

## Sicherheitsmängel: Datenlecks und Grundrechte

Zahlreiche Skandale enthüllten bereits die Sicherheitslücken des Aadhaar-Systems: Personenbezogene Aadhaar-Daten standen für weniger als umgerechnet zehn Euro online zum Verkauf. Millionen von Aadhaar-Nummern samt persönlichen Informationen fanden sich auf über 200 Regierungswebseiten. Amnesty International sieht die Grundrechte auch deshalb bedroht, weil die UIDAI die Nummern aus vielerlei Gründen deaktivieren darf. Die Betroffenen verlieren dadurch auf einen Schlag ihren Zugang zu staatlichen Leistungen.[25]

Auch in anderen Ländern des Globalen Südens werden biometrische Technologien zur Überprüfung der Identität von Sozialversicherten eingesetzt. In Mexiko müssen die 55,6 Millionen Versicherten von Seguro Popular, der staatlichen Krankenversicherung für die ärmsten Bürger, ihre biometrischen Daten an die Behörden weitergeben. In Südafrika erhalten 17,2 Millionen Empfänger von Sozialbeihilfen biometrische Smart Cards. Sozialversicherungsbehörden und private Unternehmen wie MasterCard oder Visa schließen häufig kommerzielle Vereinbarungen ab, um Smartcards für Sozialhilfeprogramme zu entwickeln oder Unternehmen die Annahme dieser Karten zu ermöglichen. Die biometrische Karte für Sozialhilfe ist in Südafrika etwa eine MasterCard. Solche Vereinbarungen enthalten in der Regel keine Rechtsbehelfe bei Daten- und Informationsmissbrauch. Privatunternehmen, Geberagenturen und die Weltbank rechtfertigen den Ausbau digitaler Identifizierungssysteme damit, dass der Einsatz von Iris- und Fingerabdruckscanner oder Gesichts- und Spracherkennung zusammen mit der Integration von Datenbanken die Effizienz steigert, Betrug bekämpft und Kosten senkt.

## Ganz leicht: die Verknüpfung mit Strafverfolgungsbehörden

Die Folgen sind weitreichend: Biometrische Daten, die einmal in der Datenbank eines Sozialschutzprogramms gespeichert sind, können mit anderen Systemen über eine gemeinsame Kennung verknüpft werden – beispielsweise Systeme zur Strafverfolgung. Nigerias nationale Identitätsdatenbank etwa ist mit verschiedenen Datenbanken verbunden – einschließlich derjenigen, die von Strafverfolgungsbehörden verwaltet werden, um etwa nach Kriminellen zu fahnden. Videokameras im öffentlichen Raum könnten dann jedes erfasste Gesicht mit Millionen Gesichtern in der Datenbank abgleichen und Alarm auslösen, wenn eine gesuchte Person auftaucht. Der Druck, sensible Daten der Sozialversicherungen, einschließlich biometrischer Identitätsfaktoren, mit der Strafverfolgung – sowohl im Inland als auch international – zu teilen, wird noch durch die Sorge über Terrorismus und Migration verstärkt. Das gefährdet nicht nur die Privatsphäre von Millionen von Menschen weltweit. Sondern auch die bürgerlichen Freiheiten.

# Überwachungsstaat: Made in Europe

Weltweit nutzen Autokraten Technologie aus Europa, um in ihren Ländern die Bevölkerung zu unterdrücken. Der Markt für Überwachungsprodukte wächst, die Europäische Union tut sich schwer damit, Exporte wirksam zu kontrollieren.

Der Pegasus-Skandal hat 2021 ein Schlaglicht auf die Hersteller von Überwachungstechnologien geworfen. Produziert und vertrieben wird die hochleistungsfähige Spähsoftware von der Firma NSO Group mit Sitz in Israel. Auch die USA gelten als Hotspot für Produzenten von Überwachungsprodukten. Außerdem spielen Deutschland und Europa laut einem 2018 von Privacy International veröffentlichten Ranking der weltweiten Überwachungsindustrie ganz oben mit. Hier ansässige Unternehmen beliefern westliche Geheimdienste offenbar genauso wie Kriminelle und autokratische Herrscher.[26] Hierzulande tragen die Hersteller der digitalen Waffensysteme klangvolle und häufig wechselnde Namen wie Advanced German Technologies, Trovicor oder FinFisher. Sie scheuen die Öffentlichkeit, doch ihre Produkte tauchen regelmäßig dort auf, wo Menschenrechte unter Druck sind.[27] 2017 beispielsweise wird der Trojaner Finspy der Münchner Firma FinFisher auf Webseiten in der Türkei gefunden. Die Seiten täuschen vor, Teil der türkischen Oppositionsbewegung zu sein und fordern Aktivist:innen zum Download einer Vernetzungs-App auf, mit der heimlich das Überwachungsprogramm installiert wird. Dass die Erdoğan-Regierung dahintersteckt, gilt als wahrscheinlich, konkrete Beweise fehlen.

## Vom Trojaner bis zum Lügendetektor

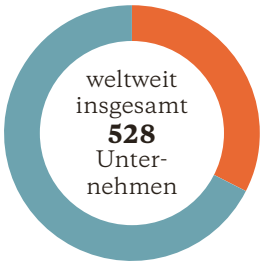
In Deutschland verklagt derweil ein zivilgesellschaftliches Bündnis den Hersteller, weil er keine Ausfuhrgenehmigung für die Türkei hat.[28] FinFisher streitet ab, Überwachungsprodukte an den Bosporus geliefert zu haben, doch seit 2019 ermittelt die Staatsanwaltschaft. 2020 durchsucht sie die Firmenzentrale, Ende 2021 meldet FinFisher Insolvenz an. Beobachter:innen vermuten, dass dieser Schritt einem Abschluss des Strafverfahrens zuvorkommen soll, die Mutter-Holding des Unternehmens besteht unter neuem Namen Vilicius weiter.[29] Doch dass es überhaupt so weit kommt, gilt trotzdem als Erfolg.

Seit Jahren ringt die EU darum, wie die Ausfuhr von Überwachungsprodukten zu kontrollieren ist. Der Markt wächst, die Angebotspalette reicht von Trojanern über biometrische Videoüberwachung bis zu smarten Lügendetektoren. Überwachungstechnologie gilt dabei juristisch nicht per se als kritisches Gut. Es handelt sich vielmehr um Produkte, die zwar bei Militär und Polizei zum Einsatz kommen können, sich aber auch für zivile Zwecke nutzen lassen. Solche Dual-Use-Produkte sind nicht verboten. Nach zähen Verhandlungen gelten seit September 2021 in der EU überarbeitete Regeln für den Export solcher Güter.[30] Erstmalig unterliegt der Dual-Use-Verordnung explizit auch Überwachungstechnologie. Für die Ausfuhr gelten seitdem neue Transparenzvorgaben und eine Verpflichtung für Hersteller, Risiken für die Menschenrechte zu prüfen. Die EU-Kommission soll zudem eine Kontrollliste von konkreten Technologien und Zielländern führen, bei denen der Export vorab genehmigt werden muss. Sie muss von den EU-Staaten einstimmig beschlossen werden, verpflichtet diese jedoch nicht, die Ausfuhr zu verbieten.

Menschenrechtsorganisationen sind von dem Kompromiss enttäuscht.[31] Sie hatten verbindlichere Kontrollvorgaben und umfassendere Sorgfaltspflichten gefordert und fürchten, dass europäische Unternehmen auch künftig Produkte an autoritäre Regime verkaufen können. Dass die EU tatsächlich willens ist, Menschenrechte über Marktpotenziale zu stellen, muss sie erst noch zeigen.

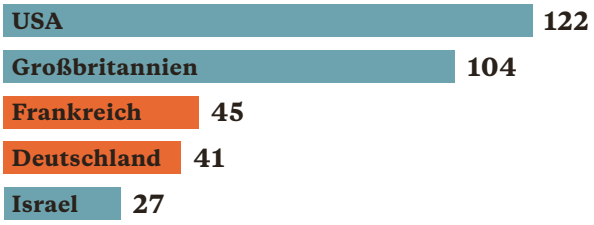
## Sitz der Exporteure

Jedes dritte Unternehmen, das Überwachungstechnologien verkauft, sitzt in der EU.




davon **171** in der EU

Länder mit den meisten Unternehmen:




*Quelle: Privacy International (2018): The Global Surveillance Industry*

# „Daten und Geld fließen nur in eine Richtung“

Es gibt einen neuen, digitalen Kolonialismus. Auch er beutet die Menschen im Globalen Süden aus.

**Interview mit Renata Avila**
CEO der Open Knowledge Foundation (https://okfn.org)

**Frau Avila, etliche Akteure der Entwicklungszusammenarbeit, auch die Weltbank, sehen in der digitalen Transformation eine große Chance, Armut und Ungleichheit im Globalen Süden zu verringern. Teilen Sie diese Euphorie?**
**Renata Avila:** Das kommt auf das Entwicklungsmodell an, das man vertritt. Ich glaube an eine nachhaltige, feministische und gerechte digitale Zukunft – und das steht im krassen Gegensatz zu dem Modell, das dem Globalen Süden aufgezwungen wird. Denn das kommt ausschließlich China und den USA zugute. Ihnen liefert der Süden die Materialien, Arbeitskräfte und Daten für den Aufbau ihrer digitalen Imperien. Hinzu kommt, dass die Tech-Giganten von globalen Handelsabkommen und komplizierten Steuerstrukturen profitieren und kaum Steuern an den Globalen Süden zahlen.

**Ist das eine neue Art von Kolonialismus?**
**Renata Avila:** Es ist eine Fortsetzung des Kolonialismus der Vergangenheit, diesmal digital. Wieder werden Ressourcen, Daten und Arbeitskräfte im Süden ausgebeutet. Nur sind es heute Technologieimperien, die die Welt durch die Kontrolle kritischer digitaler Infrastrukturen, Daten und den Besitz von Rechenleistung beherrschen. Ihnen hilft ein imperiales Welthandelssystem, das die führenden Mächte begünstigt und kleine Länder zwingt, unter ungleichen Bedingungen zu konkurrieren. Ein System, in dem Unternehmen mehr Einfluss haben als ganze Regionen. Das Ganze passiert mit voller Anerkennung und Komplizenschaft der Staaten, die sogar Tech-Botschafter im Silicon Valley ernennen.

**Wie manifestiert sich dieser digitale Kolonialismus?**
**Renata Avila:** Ein Beispiel: Bildung. Kinder auf der ganzen Welt lernen passiv Technologien, die sie nicht verbessern, anpassen oder ausbauen können. Die meisten der in Schulen verwendeten Technologien basieren nicht auf freier Software, sie gehören Big Tech. Das bremst digitale Innovation. Anstelle von Bausteinen wird Kindern eine fertige digitale Blackbox vorgesetzt – und Eltern finden das sogar meist toll. Die Folge: Tech-Konzerne formen die Kinder nicht nur. Bei ihnen landen auch die Daten, mit denen sie noch mehr Produkte entwickeln können, anstatt ein „Bildungsdaten-Gemeinwohl“ zu schaffen. Bei dieser Form des digitalen Kolonialismus fließen Daten und Geld nur in eine Richtung.

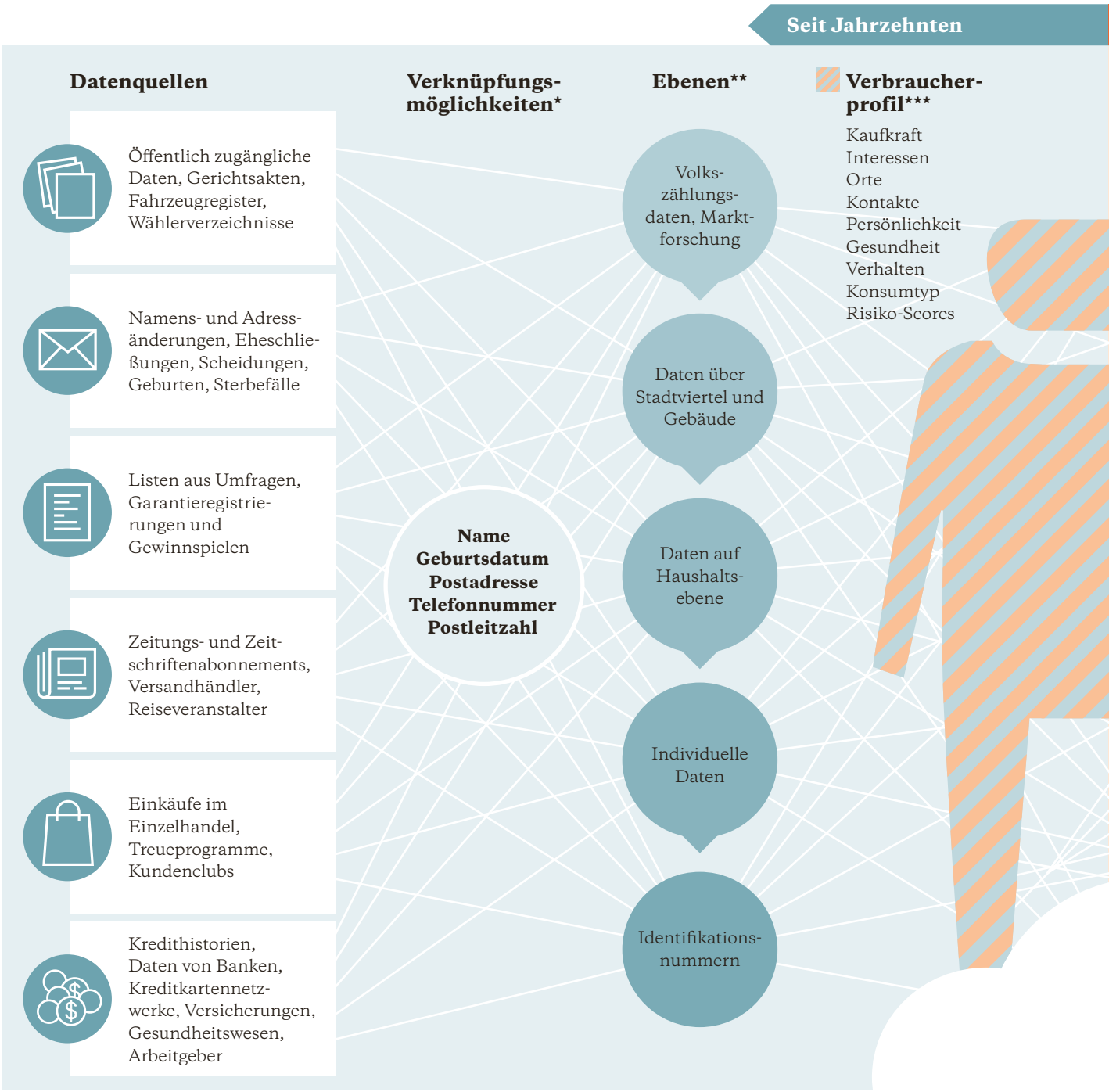
**Was bedeutet die Dominanz der Tech-Industrie für Demokratie und Entwicklung?**
**Renata Avila:** Länder haben die Kontrolle über wichtige Räume verloren: Die meisten digitalen Wahlkampagnen, Debatten und selbst öffentliche Gesundheitskampagnen finden auf privaten Plattformen statt. Für diese gilt meist kalifornisches Recht, dem sich dann alle unterwerfen müssen. Die Wahl- und Gesundheitsbehörden werden den lokalen Bedürfnissen nicht gerecht. Zudem ist das System anfällig für Übergriffe durch Machthabende, wie der Fall Cambridge Analytica zeigte. Und: Kleine, lokale Unternehmen haben keine Chance: Wenn WhatsApp neue Nutzungsbedingungen vorschreibt, muss jeder zustimmen. Da wird die marktbeherrschende Stellung eklatant missbraucht.

**Wie werden Entwicklungsländer digital souverän?**
**Renata Avila:** Das geht nicht ohne politische oder wirtschaftliche Souveränität. Für den Moment heißt das: Wir müssen den weiteren Vormarsch des digitalen Kolonialismus stoppen. Bürger:innen müssen lernen, sich die neuen Technologien zu eigen zu machen und ein Mitspracherecht bei der Regulierung einzufordern.

**Was müssen Deutschland und die EU dafür tun?**
**Renata Avila:** Sie sollten die Handelsauflagen aufheben, die den Entwicklungsländern die Hände fesseln. Es ist unfair und brutal, den Zugang zu Wissen, das Recht, Geräte zu reparieren, das Recht, Kopien von Inhalten anzufertigen, oder das Recht, Technologien zu basteln, einzuschränken, nur damit die Monopole noch reicher werden. Die Entwicklungsländer brauchen flexible Regeln, um innovativ zu sein. Und sie brauchen Raum, um Technologien zu entwickeln – ohne Preise oder Beschränkungen, die ihnen die Tech-Konzerne weltweit auferlegen. Der jetzt von Deutschland finanzierte Sovereign Tech Fund ist ein Schritt in die richtige Richtung: Das Geld hilft dem Globalen Süden, eine gerechtere, eine dekoloniale Technologie zu entwickeln.

# So werden unsere Daten erhoben: früher und heute

Mit Daten wollen Unternehmen das Verhalten und den Wert von Kund:innen vorhersagen. Schon lange sammeln sie deshalb Informationen. Im digitalen Zeitalter vervollständigen unzählige neue Datenquellen und -händler die Profile.

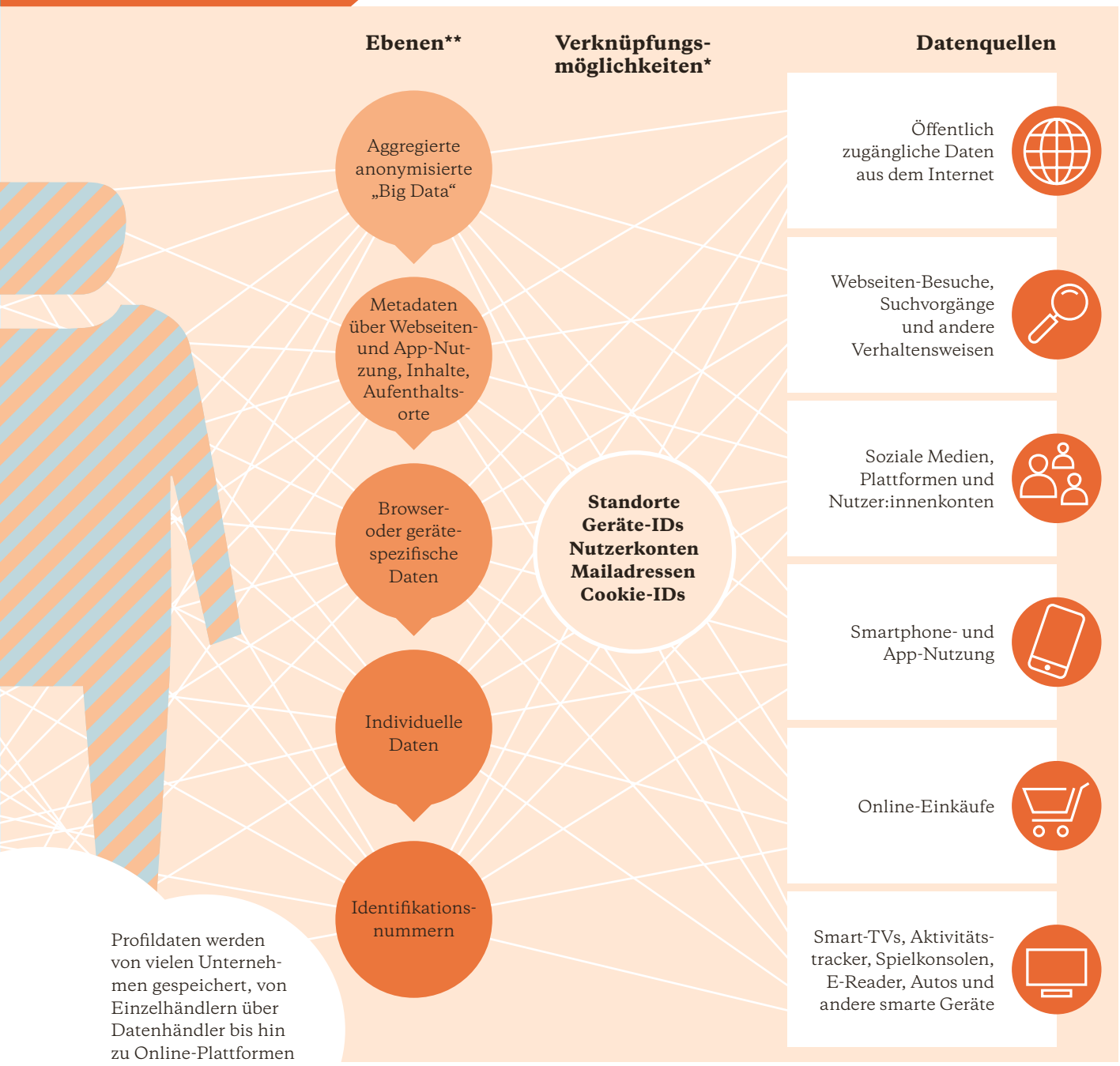



*die Daten werden anhand von unterschiedlichen Identifikationscodes miteinander verknüpft („Identifier“)

**Daten fließen auf unterschiedlichen Ebenen ein, von anonymisiert bis personalisiert

*Quelle: Pascale Osterwalder und Wolfie Christl, Studie „Corporate Surveillance in Everyday Life“ (Cracked Labs, 2017)*

**Seit den 2000er-Jahren**




*** Daten aus unterschiedlichen Quellen und Kontexten werden in individuellen Profilen zusammengeführt.

# Wenn Maschinen über Menschen entscheiden

In Österreich werden Arbeitslose automatisch in Kategorien sortiert, in den Niederlanden suchten Gemeinden automatisiert nach Sozialbetrüger:innen. Was macht es mit der Zivilgesellschaft, wenn Staaten High-Tech-Tools gegen ihr Volk richten?

Darf man arbeitslose Menschen nach Alter, Geschlecht oder Zahl ihrer Kinder sortieren und ihnen – je nach Kategorie – dann Fortbildungen verweigern? In Österreich liegt diese Frage Anfang 2021 beim Obersten Verwaltungsgerichtshof.[32] Er soll darüber befinden, ob die österreichischen Arbeitsmarktservices (AMS), vergleichbar mit den deutschen Jobcentern, in Zukunft in ganz Österreich ein Computersystem einsetzen dürfen, das Arbeitslose automatisch in Gruppen sortiert und so die Berater:innen bei ihrer Entscheidung über das weitere Vorgehen unterstützt.

Technisch ist die Sache nicht kompliziert: Das Arbeitsmarkt-Chancen-Modell, wie es offiziell heißt, teilt Jobsuchende in drei Kategorien ein. Entwickelt hat es eine Wiener Firma, die dazu das System mit Arbeitsmarktdaten aus den vergangenen Jahren fütterte, darunter Geschlecht, Alter, Staatsangehörigkeit, den Wohnort oder auch mögliche Betreuungspflichten, also Kinder oder zu pflegende Angehörige.[33] Auf Basis dieser Daten trifft das System für neue Jobsuchende nun eine Vorhersage darüber, wie wahrscheinlich es ist, dass er oder sie binnen einer bestimmten Frist wieder Arbeit findet. Entsprechende Förderung, zum Beispiel Weiterbildungen, bekommen nur diejenigen finanziert, deren Chancen passabel stehen. Aus einem Menschen wird eine statistische Wahrscheinlichkeit.

## Darf ein Staat seine Bürger:innen so behandeln?

Technisch mag das einfach sein. Moralisch und rechtlich wirft das Vorgehen der AMS hingegen schwierige Fragen auf. Darf ein Staat seinen Bewohner:innen die Unterstützung auf Grundlage solcher Vorhersagen verweigern? Und soll ein Algorithmus, also eine automatisierte Entscheidungsfindung, darüber urteilen? Ob jemand gefördert oder quasi aufgegeben wird, wirkt sich schließlich massiv auf das weitere Leben aus.

Die Antworten auf solche Fragen haben weitreichende Konsequenzen. Nicht nur für jede und jeden Einzelnen, sondern auch für die Zivilgesellschaft insgesamt. In Österreich hatten Forscher:innen und Bürgerrechtsorganisationen das System von Anfang an kritisiert.[34] Ihrer Meinung nach diskriminiert es jene, die ohnehin am Jobmarkt benachteiligt sind. Ältere Menschen oder Frauen erhalten per se einen Punktabzug – letztere noch mehr, wenn sie Kinder haben. Männer sind davon nicht betroffen.

Ist das sexistisch? Diskriminierend? Der AMS-Chef Johannes Kopf sagt: nein. Das System bilde lediglich die real existierenden Bedingungen auf dem Arbeitsmarkt ab.[35] Die Mathematikerin Paola Lopez, die zum Thema forscht, bezeichnet den AMS-Algorithmus hingegen als „Diskriminierungsbarometer", das man durchaus sinnvoll nutzen könnte – um eben diejenigen besonders zu fördern, die am stärksten benachteiligt sind.[36] Stattdessen werden sie vom System abgesägt.

## An die Rechte der Betroffenen denkt niemand

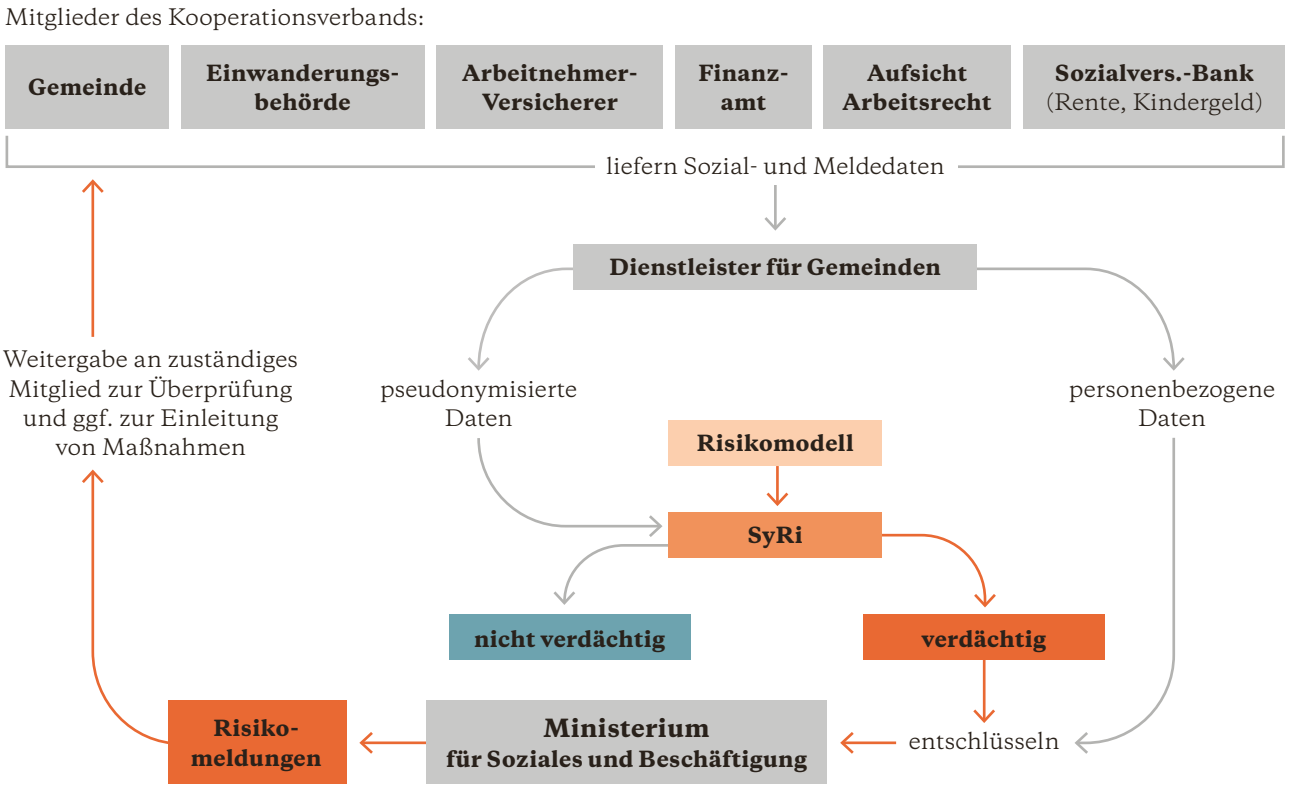
Die Hauptbetroffenen solcher Entscheidungen sind damit häufig Angehörige marginalisierter und sozial benachteiligter Gruppen. Sie haben es ohnehin schwerer als andere, an Willensbildungsprozessen zu partizipieren oder sich für Gleichbehandlung, soziale Sicherung oder Zugang zu Informationen zu engagieren. Automatisierte Entscheidungsprozesse machen es ihnen noch schwerer, für die materiellen Grundlagen eines selbstbestimmten Lebens sorgen zu können.

In Österreich tobt seit mehr als einem Jahr ein erbitterter Kampf. Nach einem Testbetrieb wollte das AMS das Modell Anfang 2021 eigentlich landesweit einführen. Dann schritt die Datenschutzbehörde ein. Das AMS betreibe ein „eingriffrelevantes Profiling" von Menschen, dafür müsse erst eine Rechtsgrundlage geschaffen werden. Die Behörde musste den Testbetrieb stoppen. Kurz darauf kassierte das Bundesverwaltungsgericht das Verbot wieder. Um den Förderbedarf zu beurteilen, dürfe das AMS sehr wohl die Daten von Arbeitssuchenden in das Modell einspeisen, urteilte es im Dezember 2020. Verboten sei nur, die Entscheidung gänzlich zu automatisieren. Damit steht dem Einsatz des Systems nun theoretisch der Weg frei.

Die Verantwortlichen der Agentur betonen immer wieder: Automatisch entschieden wird hier gar nichts. Das System

## Erst verdächtigt, dann diskriminiert

In den Niederlanden suchten Kommunen mithilfe des Big-Data-Analyse-Tools SyRi (siehe unten) nach Sozialbetrüger:innen – und erstellten damit für jeden Einzelnen ein Risikoprofil. Die Folge: Wer so unter – oft fälschlicherweise – Betrugsverdacht geriet, bekam weniger staatliche Hilfe.




*Quelle: Image/CC-BY, AlgorithmWatch*

diene lediglich dazu, Berater:innen bei ihrer Entscheidung zu unterstützen, am Ende entscheide immer eine Person. Kritiker:innen überzeugt das nicht. Sie verweisen auf Studien, die belegen: Wenn eine Maschine eine bestimmte Prognose ausspuckt, setzen sich Menschen in der Regel nicht darüber hinweg.

Dass man über den Algorithmus des AMS überhaupt so gut Bescheid weiß, ist eine absolute Besonderheit. Denn in der Regel bergen automatisierte Entscheidungsprozesse noch ein ganz anderes Problem: Sie sind eine Blackbox für die Betroffenen, von außen nicht nachvollziehbar. Der AMS-Algorithmus ist bekannt, weil die verantwortliche Firma die Formel zumindest beispielhaft für einige Fälle veröffentlicht hat.[37] Das Beispiel zeigt aber auch: Transparenz allein reicht nicht aus. Es braucht auch Widerspruchsmöglichkeiten. Was nützt es einer Jobsuchenden in Österreich, wenn offen dokumentiert ist, dass das System sie benachteiligt? Sie hat dennoch keine Möglichkeit, sich der Bewertung zu entziehen oder Widerspruch gegen die Prognose einzulegen.

## Verdächtig per Algorithmus

Menschenrechtsorganisationen und Aktivist:innen fordern deshalb klare Regeln dafür, wann solche Systeme überhaupt eingesetzt werden dürfen – egal ob von Unternehmen oder Staaten. Die Auseinandersetzung um das AMS ist zu einem Fallbeispiel dafür geworden, was alles schieflaufen kann, wenn öffentliche Stellen mit automatisierten Vorhersagen arbeiten, um Zugang zu Leistungen zu ermöglichen oder zu verwehren. Derzeit bewegen sie sich damit in einer rechtlichen Grauzone.

So kontrolliert die deutsche Finanzaufsicht BaFin etwa den Einsatz von Algorithmen im Hochgeschwindigkeitshandel an der Börse. Doch wenn etwa eine Gemeinde oder Behörde beschließt, mithilfe von automatisierten Prozessen Sozialbetrüger:innen und Schwarzarbeit aufzuspüren, also Algorithmen gegen Menschen einzusetzen, dann kontrolliert das niemand. So geschehen ist das in den Niederlanden, wo das Sozialministerium mit einem Programm namens SyRi, kurz für *Systeem*

Verfolgt, diskriminiert, verhaftet, getötet – die Unterdrückung der Zivilgesellschaft nimmt weltweit zu. Nur rund drei Prozent aller Menschen leben in Ländern mit uneingeschränkten zivilgesellschaftlichen Freiheiten. In vielen Ländern haben sich auch 2021 die Bedingungen weiter verschlechtert, unter denen Menschen ihre Meinung äußern oder für ihre Rechte kämpfen können.

Brot für die Welt gibt den Atlas der Zivilgesellschaft jährlich in Kooperation mit CIVICUS heraus, einem weltweiten Netzwerk für Bürgerbeteiligung. In dieser Ausgabe verdeutlichen Berichte aus fünf Weltregionen sowie aus den Ländern Indonesien, Mexiko, Tansania und Ukraine die gegenwärtige Situation. Ein eigener Schwerpunkt illustriert, wie die Digitalisierung viele Entwicklungen noch verstärkt – aber auch Menschen dabei hilft, mit ihrem zivilgesellschaftlichen Engagement jene besser erreichen zu können, die Hilfe benötigen.

In mehr als 90 Ländern befähigt Brot für die Welt arme und ausgegrenzte Menschen, aus eigener Kraft ihre Lebenssituation zu verbessern. Schwerpunkte der Arbeit sind: Neue Armuts- und Hungerkrisen bewältigen, den Klimawandel bekämpfen, Konflikte um Ressourcen und Gemeingüter überwinden, Frauen und Frauenrechte stärken sowie den digitalen Wandel gerecht gestalten.

**Brot für die Welt**
Evangelisches Werk für Diakonie
und Entwicklung e. V.

Caroline-Michaelis-Straße 1
10115 Berlin

Telefon +49 30 65211 0
Fax +49 30 65211 3333
info@brot-fuer-die-welt.de

**Spenden**
Brot für die Welt
Bank für Kirche und Diakonie
IBAN: DE10 1006 1006 0500 5005 00
BIC: GENODED1KDB

www.brot-fuer-die-welt.de
www.brot-fuer-die-welt.de/
atlas-zivilgesellschaft