Grundrechte im Digitalen

WIKIMEDIA
DEUTSCHLAND

1849
Paulskirchenverfassung

2

1919
Weimarer Reichsverfassung

1948
Allgemeine Erklärung der Menschenrechte

1949
Grundgesetz

1953
Europäische Menschenrechtskonvention

1966
Urheberrechtsgesetz

1983
Volkszählungsurteil des Bundesverfassungsgerichts erkennt das Recht auf informationelle Selbstbestimmung an

1989
UN-Kinderrechtskonvention

1995
Europäische Datenschutzrichtlinie

2000
Charta der Grundrechte der Europäischen Union

2000
Dotcom-Krise zeigt Verwundbarkeit digitaler Märkte

2001
Informationsfreiheitsverordnung der Europäischen Union

2002
Erste Creative-Commons-Lizenzen

2006
Das Informationsfreiheitsgesetz tritt in Kraft

2008
Das Bundesverfassungsgericht trifft die Entscheidung zur Online-Durchsuchung und etabliert ein IT-Grundrecht

2012
Transparenzgesetz in Hamburg

2013
Snowden-Enthüllungen decken weltweite Massenüberwachung auf

2016
Datenschutz-Grundverordnung (DSGVO) der Europäischen Union

2018
Skandal um Cambridge Analytica zeigt Missbrauch von Nutzerdaten zur Wahlbeeinflussung

2019
Europäischer Rechtsakt zur Barrierefreiheit

2020
Corona-Pandemie beschleunigt Digitalisierung von Bildung, Arbeit und Verwaltung

2021
Das Bundesverfassungsgericht bestätigt das Recht auf Bildung

2022
ChatGPT-Boom rückt künstliche Intelligenz ins Zentrum öffentlicher Debatten

2023
Europäisches Gesetz über digitale Dienste (Digital Services Act) tritt in Kraft

2024
EU-Richtlinie zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt

2024
75-jähriges Bestehen des Grundgesetzes

Vorwort

Grund-rechte im Digitalen

Liebe Leserinnen und Leser,

die Förderung des Freien Wissens ist seit der Vereinsgründung im Jahr 2004 das wichtigste Ziel von Wikimedia Deutschland. Freies Wissen ist weit mehr als ein technisches oder organisatorisches Konzept – es berührt grundlegende Fragen von Freiheit, Teilhabe und Demokratie. Denn der freie Zugang zu Informationen, die Möglichkeit zur Mitgestaltung von Wissen und die Offenheit digitaler Räume sind eng mit unseren Grundrechten verbunden: mit der Meinungs- und Informationsfreiheit, der Wissenschaftsfreiheit, dem Recht auf Bildung und dem Schutz der Privatsphäre.

In einer zunehmend digitalisierten Gesellschaft zeigt sich: Wer über Wissen verfügt – und darüber entscheidet, wer Zugang dazu hat –, verfügt über Macht. Deshalb ist es entscheidend, digitale Räume so zu gestalten, dass sie die Grundrechte schützen und stärken, anstatt sie einzuschränken. Der vorliegende Sammelband bringt Perspektiven zusammen, die zeigen, wie eng die Frage nach einem freien, offenen und gerechten digitalen Wissensraum mit dem rechtlichen Rahmen unserer Demokratie verknüpft ist.

Wir nutzen digitale Dienste – täglich. Sie begleiten unseren Alltag, aber wir sind uns nur wenig bewusst, welche Rechte dabei betroffen sind. In der digitalen Welt gewinnen die Grundrechte eine neue Bedeutung. Was früher im öffentlichen Raum sichtbar war, verlagert sich zunehmend in digitale Infrastrukturen, Plattformen und Algorithmen. Unser Recht auf Meinungsfreiheit, auf Bildung, auf Privatsphäre und auf Teilhabe wird heute nicht nur durch staatliches Handeln, sondern auch durch technische Systeme, Datenströme und wirtschaftliche Interessen geformt – und bedroht. Gerade weil die Digitalisierung tief in unseren Alltag eingreift, müssen wir die Grundrechte nicht neu erfinden, sondern konsequent auf neue Kontexte anwenden und entschlossen verteidigen.

Grundrechte sind keine abstrakten Prinzipien, sondern konkrete Schutzversprechen: Sie garantieren uns Freiheit, Gleichberechtigung und Würde – auch gegenüber digitalen Technologien. Doch diese Rechte setzen die Durchsetzung voraus. Sie müssen in Gesetzen festgeschrieben, in Gerichten verteidigt und im gesellschaftlichen

Bewusstsein verankert sein. Ob beim Einsatz von künstlicher Intelligenz in Schulen, bei der Moderation von Inhalten in sozialen Netzwerken oder beim Zugang zu staatlichen Informationen – überall zeigt sich: Grundrechte sind das Fundament einer demokratischen Gesellschaft. In der digitalen Welt gilt das mehr denn je.

Grundrechte im Digitalen verstehen

Wir haben Autorinnen und Autoren aus verschiedenen Bereichen – der Zivilgesellschaft, der Wirtschaft, der Wissenschaft – gefragt, welche Themen für unser digitales Leben wichtig sind und wo unsere Rechte durch Apps und Vernetzung eingeschränkt werden könnten.

Was heißt eigentlich „Grundrechte im Digitalen“ – und wo sind sie geregelt? Der erste Teil des Buchs gibt eine Orientierung: Er erklärt, wie klassische Grundrechte wie Meinungsfreiheit, Datenschutz oder Zugang zu Informationen im digitalen Raum eine neue Bedeutung bekommen. Außerdem zeigt er, wer in Deutschland und der EU für die Regulierung zuständig ist und wo die Grenzen bestehender Gesetze liegen. Vertiefende Kapitel widmen sich der Informationsfreiheit und dem Datenschutz – beides Themen, bei denen sich zeigt, wie wichtig Transparenz und Kontrolle im digitalen Alltag sind. Der Wert eines Rechts bemisst sich an seiner Durchsetzbarkeit. In einem weiteren Artikel erklären wir deshalb, wie Bürger*innen ihre Rechte vor Gericht einklagen können.

Verbrechensbekämpfung und öffentliche Sicherheit gehören zu den Bereichen, in denen algorithmische Systeme und künstliche Intelligenz besonders schnell zum Einsatz kommen – oft ohne transparente Prüfung oder wirksame Kontrolle. Doch Systeme zur Vorhersage von Straftaten, Gesichtserkennung oder automatisierte Risikobewertungen stellen nicht nur technische Innovationen dar, sondern berühren fundamentale Grundrechte: Datenschutz, Gleichbehandlung, das Recht auf informationelle Selbstbestimmung. Wie lassen sich Sicherheit und Freiheit in der digitalen Welt in Einklang bringen? Die Texte in diesem Abschnitt zeigen, dass KI-basierte Systeme nicht neutral

sind – sie reproduzieren gesellschaftliche Ungerechtigkeiten, wenn ihre Datengrundlagen verzerrt sind oder diskriminierende Muster enthalten. Gerade in staatlichen Anwendungsfeldern wie Polizei oder Verwaltung ist daher besondere Vorsicht geboten: Was technisch möglich ist, darf nicht automatisch zum Maßstab politischer Entscheidungen werden.

Digitale Technologien strukturieren nicht nur unseren Alltag, sondern auch Machtverhältnisse. Unsere Autor*innen gehen der Frage nach, wie digitale Prozesse Einfluss auf politische Meinungsbildung, Informationsfreiheit und demokratische Kontrolle nehmen. Wie verändert sich der Journalismus unter den Bedingungen algorithmischer Sichtbarkeit? Welche Rolle spielen Fake News und digitale Überwachung? Die Beiträge untersuchen, wie sich das Verhältnis zwischen Staat, Plattformen und Öffentlichkeit im digitalen Raum verschiebt – und was das für den Schutz individueller und kollektiver Rechte bedeutet.

Digitalisierung verändert Schulen, Lernprozesse und Teilhabechancen nicht immer zum Guten. Dieser Teil des Buches beleuchtet das Recht auf Bildung im digitalen Zeitalter: Welche Chancen bietet KI, welche Risiken entstehen für Schüler*innen und Lehrkräfte? Wie lässt sich digitale Teilhabe gerecht gestalten, gerade für Kinder, die besonderen Schutz brauchen? Die Beiträge fragen, wie Grundrechte konkret im Bildungsbereich gewahrt oder verletzt werden und was das für eine demokratische Gesellschaft bedeutet.

Grundrechte im Digitalen betreffen nicht nur Datenschutz und Meinungsfreiheit, sondern auch grundlegende Fragen von Gerechtigkeit, Schutz und ökologischer Verantwortung. In diesem Teil geht es um den Zusammenhang von digitaler Technologie und sozialer wie ökologischer Nachhaltigkeit: Was bedeutet Inklusion im digitalen Raum? Welche Verantwortung tragen digitale Infrastrukturen für Umwelt und Klima? Wie kann der digitale Raum geschlechtergerecht und diskriminierungsfrei gestaltet werden? Und was bedeutet Schutz vor Gewalt, wenn Überwachung, Belästigung oder Kontrolle über digitale Mittel stattfinden? Die Beiträge beleuchten, wie eng soziale, ökologische und digitale Fragen miteinander verbunden sind und wie wichtig es ist, Grundrechte in einer vernetzten Welt umfassend zu denken.

Zugang zu Wissen, Informationen und digitalen Kulturgütern ist ein grundlegendes demokratisches Recht – und eine zentrale Voraussetzung für die Öffentlichkeit im digitalen Raum. Doch was frei zugänglich sein sollte, wird immer häufiger durch restriktive

Nutzungsrechte, technische Barrieren oder wirtschaftliche Interessen eingeschränkt.

Die Beiträge in diesem Abschnitt beleuchten, wie der Zugang zu gemeinfreien Inhalten behindert wird – etwa wenn Museen neue Leistungsschutzrechte auf digitale Reproduktionen beanspruchen. Sie zeigen, welche Rolle offene Lizenzen wie Creative Commons für eine gemeinwohlorientierte Wissensordnung spielen und wie bestimmte urheberrechtliche Regelungen heute auch genutzt werden, um unliebsame Inhalte zu unterdrücken. Die Diskussion um das sogenannte „Zensurheberrecht" macht deutlich: Der Streit um den Zugang zu Informationen ist längst auch ein Streit um die Ausgestaltung unserer Demokratie.

Grundrechte im Digitalen gemeinsam gestalten

Die Texte in diesem Buch machen deutlich: Digitale Grundrechte sind kein Nischenthema. Sie betreffen uns alle – in der Schule, am Arbeitsplatz, in sozialen Netzwerken, bei der Nutzung öffentlicher Dienste oder beim Zugang zu Wissen. Umso wichtiger ist es, sich mit ihnen auseinanderzusetzen, Widersprüche sichtbar zu machen und demokratische Antworten zu finden. Denn die Frage, wie wir digitale Räume gestalten, ist immer auch die Frage, wie wir in Zukunft zusammenleben wollen. Dieses Buch lädt dazu ein, mitzureden, mitzudenken und digitale Grundrechte nicht nur als Schutz, sondern auch als Gestaltungsauftrag zu begreifen.

Franziska Heine
Geschäftsführende Vorständin
Wikimedia Deutschland e. V.

Inhalt

1 Digitale Grundrechte verstehen

2 Macht, Kontrolle und öffentliche Debatte

3 Bildung, Schule und Kinder

4 Gerechtigkeit, Schutz und Nachhaltigkeit

5 Zugang zu Wissen und digitalen Inhalten

Digitale Grundrechte verstehen

Malte Spitz

Was sind digitale Grund-rechte?

Im Jahr 2024 feierten wir das 75-jährige Bestehen unseres Grundgesetzes, das am 23. Mai 1949 verkündet wurde. Es umfasste 146 Artikel und eine vorangestellte Präambel. Von zentraler Bedeutung waren neben der föderalen Struktur vor allem die Grundrechte. Diese Grundrechte wirken und prägen bis heute unseren Rechtsstaat, unser Zusammenleben und unsere Demokratie. Ihre Zeitlosigkeit liegt darin, dass sie sich den jeweiligen Verhältnissen anpassen lassen. Sie können auf die Herausforderungen unserer Zeit eingehen und auf ein digitales Zusammenleben ausgelegt werden.

Die Grundrechte sichern die individuelle Freiheit des Einzelnen und bilden zugleich eine objektive Werteordnung für unser gesellschaftliches Zusammenleben. In ihrer Funktion als Abwehr-, Leistungs- und staatsbürgerliche Rechte binden sie alle Staatsgewalt. Grundrechte bilden den zentralen Kern unserer Verfassung, indem sie die Freiheit und Würde des Einzelnen schützen. Das Bundesverfassungsgericht sichert als Hüter der Verfassung die Durchsetzung und Fortentwicklung dieser Rechte. Den Grundrechten geht ideengeschichtlich eine lange historische Entwicklung voraus, die spätestens ab dem 18. Jahrhundert – etwa in der *Virginia Bill of Rights* von 1776 – Verrechtlichungen in Form geschriebener Verfassungen erfahren hat. Vorläufer in Deutschland fanden sich in begrenztem Umfang in der Paulskirchenverfassung von 1849 und der Weimarer Reichsverfassung von 1919. Welche Rolle Grundrechte spielen und wie sie verstanden werden, ist seit jeher einem stetigen Wandel unterworfen und immer Ausdruck der Herausforderungen und Problemstellungen der jeweiligen Zeit.

Die Grundrechte des Grundgesetzes haben verschiedene Funktionen. Man unterscheidet zwischen Abwehr-, Leistungs- und staatsbürgerlichen Rechten. Abwehrrechte sollen Bürger*innen vor Eingriffen in ihre Freiheit schützen. Leistungsrechte hingegen vermitteln einen Anspruch der Bürger*innen auf staatliche Leistungen. Daneben gibt es noch staatsbürgerliche Rechte, auch Teilhaberechte genannt. Sie garantieren, dass Bürger*innen am Staatsleben mitwirken können – zum Beispiel durch ihr Wahlrecht. Das Grundgesetz enthält aber nicht nur die Grundrechte. Es regelt auch ganz grundlegend, wie unser Staat aufgebaut ist und wie er funktionieren soll. Geregelt ist beispielsweise, welche Aufgaben Legislative, Exekutive und Judikative haben und in welchen Bereichen der Bund oder die Länder Gesetze erlassen dürfen.

Das Grundgesetz steht heute vor Herausforderungen, die 1949 noch nicht absehbar waren. Wir leben in einer Welt, die zunehmend von digitalen Interaktionen geprägt ist. Die massive Zunahme von Daten in unserem Leben und dessen Digitalisierung ist allgegenwärtig. Private Unternehmen agieren mit staatsähnlicher Macht und sind in der Lage, Grundrechte einzuschränken. Zugleich eröffnen sich neue Möglichkeiten: Menschen können sich auf bisher nie da gewesene Weise vernetzen, kommunizieren und ihre Meinung kundtun, geografische Grenzen überwinden und selbst Wissen schaffen und teilen.

Diese Entwicklungen wirken sich auf fast alle Grundrechte aus, sei es, weil die geschützten Bereiche des Lebens nun auch im digitalen Raum geschehen, sei es, weil durch die Digitalisierung ganz neue Risiken für Bürger*innen entstehen. Von besonderer Bedeutung sind im Kontext der Digitalisierung daher zum einen klassische Grundrechte wie das allgemeine Persönlichkeitsrecht, die Glaubens- und Gewissensfreiheit, die Meinungsfreiheit, die Pressefreiheit, die Kunst- und Wissenschaftsfreiheit oder das Post- und Fernmeldegeheimnis. Zudem hat das Bundesverfassungsgericht diese klassischen Grundrechte weiterentwickelt und zum Beispiel das Recht auf informationelle Selbstbestimmung oder das sogenannte IT-Grundrecht anerkannt.

Damit entstehen neue grundrechtliche Fragestellungen: Wie können die Grundrechte auch im digitalen Kontext effektiv geschützt werden? Welche Rolle spielen hierbei Privatakteur*innen wie beispielsweise Social-Media-Plattformbetreiber mit ihrer übermächtigen Marktstellung? Wie verhält sich die Grundrechtsordnung zu neu entstandenen Überwachungsmöglichkeiten? Ist es möglich, Hassrede im Internet zu verhindern, ohne die freiheitlichen Grundrechte zu gefährden?

Digitale Grundrechte – gibt es sie überhaupt?

Die Begriffe „digitales Grundrecht“ oder „Internet“ kommen im Grundgesetz nicht vor. Trotz großer politischer, gesellschaftlicher und technologischer Entwicklungen sind die Grundrechte in ihrem Wortlaut seit 1949 weitgehend

unverändert geblieben. Bedeutet dies, dass unsere Verfassung keine Antworten auf die drängenden Grundrechtsfragen bereithält, die sich im Zuge der Digitalisierung stellen? Das stimmt natürlich nicht. Vielmehr sind die Grundrechte selbstverständlich auf digitale Sachverhalte anwendbar. Über die Jahrzehnte haben sie durch die Rechtsprechung des Bundesverfassungsgerichts auch in digitalen Kontexten an Kontur gewonnen.

In seinem Volkszählungsurteil von 1983 hat das Bundesverfassungsgericht sich mit den besonderen Gefahren auseinandergesetzt, die die damals aufkommende automatisierte Datenverarbeitung mit sich bringen könnte. Es war die erste Entscheidung des Bundesverfassungsgerichts, in dem das Recht auf informationelle Selbstbestimmung anerkannt wurde. Es bildet bis heute die Grundlage für die maßgeblichen Entwicklungen des digitalen Grundrechtsschutzes. So ist laut Grundgesetz Selbstbestimmung für die Würde des Menschen von herausragender Bedeutung. In den Worten des Gerichts gewährleistet die Grundrechtsordnung, „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen." Das ergibt sich laut Gericht aus Artikel 2 Absatz 1: „Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt." Dieses Recht in Verbindung mit Artikel 1 Absatz 1 – „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt." – hat das Bundesverfassungsgericht klargestellt, dass der Staat nur unter engen Voraussetzungen persönliche Daten der Bürger*innen verarbeiten darf. Seit dieser Entscheidung ist das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts fester Bestandteil des deutschen Grundrechtssystems.

In zahlreichen Folgeentscheidungen – beispielsweise zur Telekommunikationsüberwachung oder zur Vorratsdatenspeicherung – wurde das Recht auf informationelle Selbstbestimmung konkretisiert. Es spielt bei verschiedenen aktuellen Debatten eine beachtliche Rolle, etwa während der Corona-Pandemie oder über die Digitalisierung des Gesundheitswesens, wenn es bei der elektronischen Patientenakte um die Frage von aktiver Einwilligung oder Widerspruch zu dieser geht.

Die Volkszählungsentscheidung sollte nicht der letzte Fall bleiben, in dem das allgemeine Persönlichkeitsrecht um weitere Facetten

ergänzt wurde, weil neue technische Entwicklungen dies notwendig machten. Anlässlich seiner Entscheidung zur Online-Durchsuchung entwickelte das Bundesverfassungsgericht im Jahr 2008 das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (das sogenannte IT-Grundrecht oder Computergrundrecht). Mit dieser Entscheidung wurde dem Rechnung getragen, dass Computer zunehmend von privaten Nutzenden verwendet wurden. Ihre Relevanz hat angesichts der inzwischen flächendeckenden Verbreitung von Smartphones und ähnlicher Geräte weiter zugenommen. Mittlerweile gibt es in nahezu jedem Haushalt eine Vielzahl von ihnen, die umfassend personenbezogene Daten sammeln oder deren Nutzung tiefgehende Einblicke in die Privatsphäre erlauben. Der (oftmals unbemerkte) Zugriff auf diese Daten – der durch Sicherheitsbehörden, aber auch durch Kriminelle erfolgen kann – ermöglicht es Dritten, sich ein umfangreiches Bild davon zu machen, was die betroffene Person interessiert und welche Eigenschaften und Vorlieben sie hat. Die Grundrechtsordnung sichert daher den gesellschaftlichen Konsens, dass solche Informationssysteme und die darauf gespeicherten personenbezogenen Daten vertraulich bleiben.

Grundrechte über Ländergrenzen hinweg

Die weltweite Vernetzung überwindet bisherige staatliche Grenzen. Informationen strömen ungehindert über Kontinente hinweg, und ein einziger Klick verbindet uns mit Servern – und Menschen – irgendwo auf der Welt. Doch was bedeutet das für unsere Rechte? Nationale Gesetze allein stoßen in dieser vernetzten Realität an ihre Grenzen. Hier setzt die Europäische Union mit ihrer Grundrechtecharta einen verlässlichen Rahmen. Sie setzt den Grundrechtsrahmen auf europäischer Ebene und verpflichtet Organe, Einrichtungen und sonstige Stellen der Europäische Union sowie die Mitgliedsstaaten zu diesen Grundrechten, wenn sie EU-Recht durchführen. Besonders die Artikel 7 und 8, die das Recht auf Achtung des Privatlebens und den Schutz personenbezogener Daten verankern,

sind in dieser global vernetzten Welt unverzichtbar. Sie verkörpern ein gemeinsames europäisches Verständnis von Freiheit und Selbstbestimmung und erinnern uns daran: Wir sind nicht bloß Datenpunkte, sondern Menschen mit unveräußerlichen Rechten.

Grundrechte gelten auch im digitalen Zeitalter. Der rechtsfreie Raum im Netz ist eine politische Erzählung, die nie der Realität entsprach. Es mag sein, dass das Internet insbesondere in der Vergangenheit als schwerer zu greifen oder abstrakter wahrgenommen wurde. Die Grundrechtsordnung ist aber in der Lage, dynamisch auf technologische Entwicklungen und neue Gefährdungslagen zu reagieren. Auch wenn inzwischen gewisse digitale Schutzstandards etabliert sind, ändert das nichts an der Tatsache, dass es notwendig ist, diese stetig an fortschreitende technologische Entwicklungen und neue Gefährdungslagen anzupassen. Digitale Sachverhalte betreffen regelmäßig nicht nur spezielle informations- und datenbezogene Grundrechte, sondern reichen in den Schutzbereich von Kunst-, Meinungs-, Berufs- und vielen weiteren Freiheiten. Auch hier ist eine besondere Sensibilität für die Besonderheiten digitaler Vorgänge erforderlich, etwa wenn es um Meinungsäußerungen in sozialen Netzwerken geht.

Die Macht der Plattformen

Zudem wirft gerade die Betrachtung digitaler Sachverhalte die Frage auf, inwieweit neben staatlichen Stellen auch private Unternehmen an die Grundrechte gebunden sind. Nach der ursprünglichen Konzeption des Grundgesetzes verpflichten Grundrechte unmittelbar nur den Staat, zum Beispiel die Polizei oder andere Behörden. Doch was passiert, wenn Bedrohungen und Beschränkungen nicht mehr vom Staat, sondern von privaten Akteur*innen ausgehen? Genau das erleben wir heute: Soziale Netzwerke, Online-Marktplätze und Suchmaschinen sind längst zentrale Bestandteile unseres Lebens – sie alle werden größtenteils von (nicht-europäischen) Unternehmen betrieben. Mit der fortschreitenden Digitalisierung, verstärkt durch Entwicklungen beim maschinellen Lernen und künstlicher Intelligenz, wird diese Abhängigkeit von privatwirtschaftlicher Technologie weiter zunehmen.

Die Macht dieser Unternehmen geht dabei weit über die von klassischen Dienstleistern hinaus. Sie legen fest, unter welchen Bedingungen wir von unseren Grundrechten Gebrauch machen können. Durch ihre Nutzungsbedingungen schaffen sie regelrechte Privatgesetze, bestimmen, was erlaubt ist, und entscheiden eigenständig über deren Anwendung und Auslegung. Sie entscheiden darüber, welche Meinungen sichtbar bleiben, was als Kunst akzeptiert wird und welchen Raum wissenschaftliche Forschung erhält. Ein oft zitiertes Beispiel ist die Zensur der weiblichen Brustwarze auf vielen Social-Media-Plattformen: Was in einem Kontext künstlerischer Ausdruck, Protest oder wissenschaftliche Aufklärung sein kann, wird pauschal unterdrückt – während die Darstellung männlicher Brustwarzen problemlos geduldet wird. Solche Entscheidungen sind nicht trivial. Sie werfen grundlegende Fragen auf: Wer definiert, was angeblich jugendgefährdend ist? Wer entscheidet, was wir sehen, sagen oder teilen dürfen?

Der Staat hat die Pflicht, unsere Rechte auch vor Eingriffen Dritter zu bewahren. Das ergibt sich unmittelbar aus der Grundrechtsbindung des Staates, auch wenn diese Pflicht nicht ausdrücklich dem Grundgesetz zu entnehmen ist. Doch was, wenn er dieser Pflicht nicht oder nur unzureichend nachkommt? Hier haben Gerichte klare Antworten gegeben: Wenn die Macht von privaten Unternehmen der des Staates in einzelnen Bereichen gleichkommt, können auch ihre Verpflichtungen den staatlichen Schutzpflichten gleichgestellt werden. Das heißt, dort, wo private Akteur*innen wie Staaten agieren, müssen sie auch wie Staaten Verantwortung übernehmen – insbesondere für die Wahrung von Grundrechten.

Tatsächlich haben Gerichte in diesem Kontext klare Bedingungen formuliert, die sonst nur für staatliches Handeln gelten: Plattformen müssen uns „anhören“, bevor sie in unsere Rechte eingreifen. Die Nutzenden haben das Recht, sich gegen solche Entscheidungen, etwa Moderationsentscheidungen oder Sperrungen von Accounts, zu wehren. Darüber hinaus dürfen Plattformen nicht willkürlich agieren – ihre Maßnahmen müssen auf sachlichen und objektiv nachvollziehbaren Gründen beruhen und die Grundrechte der Betroffenen berücksichtigen.

Neue Herausforderungen durch Algorithmen und generative KI

Dennoch treten immer wieder neue Gefahren für unsere Grundrechte auf. Neben bewussten Entscheidungen, die von Menschen getroffen werden, spielen zunehmend Algorithmen und künstliche Intelligenz eine bedeutende Rolle in der Entscheidungsfindung. Während erste Sprachmodelle noch offen rassistische und diskriminierende Antworten gaben, kommt es heute zum Glück kaum noch zu offenen Beleidigungen durch solche *Large Language Models* (zum Beispiel ChatGPT). Das macht sie jedoch nicht unbedingt weniger gefährlich.

Das grundlegende Problem besteht darin, dass solche Systeme bestehende Diskriminierungen erlernen und verstärken können. Zudem bleibt oft unklar, wie diese Systeme ihre Entscheidungen treffen. Ein Beispiel hierfür ist die Frage, welche Inhalte der Algorithmus auf einem sozialen Netzwerk für uns auswählt und welche er unterdrückt. Sind das qualitativ schlechte Inhalte? Geht der Algorithmus davon aus, dass sie mich nicht interessieren? Oder war der Beitrag vielleicht doch ein wenig zu feministisch? Enthält der Beitrag, der mir stattdessen angezeigt wird, vielleicht Desinformationen, über die mich aufrege und daher vielleicht noch ein wenig länger auf der Plattform bleibe?

Durch diese Entscheidungen wird zum Beispiel die Meinungsfreiheit erheblich beeinträchtigt. Wenn nicht nachvollziehbar ist, nach welchen Kriterien Inhalte gefiltert, priorisiert oder gelöscht werden, besteht die Gefahr, dass unerwünschte Meinungen systematisch benachteiligt oder unsichtbar gemacht werden, ohne dass die Betroffenen dies verstehen oder dagegen vorgehen können.

Zudem ist die KI nicht vorurteilsfrei: Wenn man sich mit einer Bilderstellungssoftware wie Midjourney oder Dall-E ein Bild einer Person mit Asperger-Syndrom erstellen lässt, zeichnet die KI oft ein Bild eines mehr oder weniger sympathischen, jungen, weißen Mannes. Ist das also ein positives Zeichen, weil eine neurodiverse Person nicht negativ dargestellt wird? Nicht ganz. Natürlich ist es gut, dass hier eine „durchschnittliche“ Person abgebildet wird. Doch fragt man mehrfach

nach derartigen Bildern, sind nahezu alle dargestellten Personen jung, weiß und männlich.

Dieses spezifische Problem wurde mittlerweile zwar schon weitgehend behoben, aber es verdeutlicht ein grundlegendes Problem: Es wird immer eine Herausforderung bleiben, gesellschaftliche Vorurteile nicht in die KI zu übertragen. Es zeigt sich, wie wichtig es ist, alle Ebenen zu bedenken, auf denen Diskriminierung auftreten kann – in den Daten, den Algorithmen und den Ergebnissen der Systeme.

Neue Wege staatlicher Überwachung

Nicht zuletzt ist staatliche Überwachung ein hochsensibles Thema, das zunehmend an Bedeutung gewinnt, insbesondere in einer Zeit, in der Technologien wie biometrische Erkennung, intelligente Analyse- und Erkennungssysteme mithilfe künstlicher Intelligenz und maschinellen Lernens immer mehr verbreitet sind. Nutzt ein Staat diese Technologien, eröffnen sich ihm neue Möglichkeiten, Menschen zu überwachen, zu analysieren und sogar in ihrem Verhalten zu beeinflussen. Doch mit dieser neuen Macht kommen auch erhebliche Risiken: Die Gefahr von willkürlichen Eingriffen in die Privatsphäre und von ungerechtfertigten Einschränkungen individueller Rechte ist real. Biometrische Daten wie Fingerabdrücke, Gesichtserkennung oder sogar Verhaltensmuster ermöglichen eine präzise Überwachung. Allein das Gefühl, vom Staat beobachtet zu werden, hat Einfluss auf die persönliche Lebensgestaltung und damit auf die Grundrechtsausübung. Doch wer kontrolliert, wie und wann diese Daten genutzt werden?

Künstliche Intelligenz und Algorithmen, die eingesetzt werden, um Verhaltensweisen zu analysieren und vorherzusagen, bergen die Gefahr, bestehende Vorurteile zu verstärken und Menschen ungerecht zu kategorisieren – *racial profiling* ist da nur ein Stichwort. Diese Technologien können zur instrumentellen Kontrolle von Bevölkerungsschichten führen, ohne dass die betroffenen Individuen die Möglichkeit haben, sich zu wehren. Es ist daher unabdingbar, dass jeder Schritt in

Richtung verstärkter staatlicher Überwachung einem intensiven rechtlichen und gesellschaftlichen Prüfprozess unterzogen wird. Der Schutz der Grundrechte darf nicht den technischen Fortschritten zum Opfer fallen – wir müssen sicherstellen, dass unsere Freiheit, unsere Privatsphäre und unser Recht auf Selbstbestimmung nicht durch den Missbrauch von Technologien untergraben werden.

Digitale Grundrechte brauchen aktive Verteidigung

Bei den digitalen Grundrechten gibt es also weiterhin offene Fragen, insbesondere in Bezug auf den Schutzumfang und die Grundrechtsbindung. Der gesellschaftliche Diskurs über digitale Grundrechte ist oftmals geprägt von politischen und wirtschaftlichen Interessen. Die Herausforderungen sind ebenso vielfältig wie die Chancen, die sich aus einer klugen Regulierung ergeben können, nämlich Grundrechte im Digitalen umfassend wirksam werden zu lassen. Recht ist kein starres Gebilde, denn es wandelt sich mit den Anforderungen der Zeit. Dabei wird der Wandel des Rechts oft nicht nur durch die Gesetzgebung, sondern auch durch die Rechtsprechung geprägt. Doch hier zeigt sich ein grundlegendes Problem: Es besteht ein Machtungleichgewicht in den Prozessen zwischen Einzelpersonen oder kleineren Organisationen und den übermächtigen Tech-Konzernen. Wie lässt sich in einem solchen asymmetrischen Verhältnis sicherstellen, dass diese Konzerne ihrer Verantwortung gerecht werden und die Grundrechte der Nutzenden tatsächlich schützen?

Eine Möglichkeit, digitale Grundrechte zu stärken, bieten strategische Klagen, die gezielt eingesetzt werden, um rechtliche und gesellschaftliche Veränderungen zu bewirken. Strategische Prozessführung ist ein zentraler Hebel, um Grund- und Menschenrechte effektiv durchzusetzen. Vor deutschen und europäischen Gerichten haben Präzedenzfälle eine wegweisende Bedeutung: Sie schaffen Orientierung und setzen Maßstäbe, die weit über den Einzelfall hinausreichen. Sie können staatliche Überwachung begrenzen, einseitige unternehmerische Interessen zurückweisen und so dazu beitragen, digitale

Grundrechte durchzusetzen. Das Bundesverfassungsgericht hat in der Vergangenheit etwa die Befugnisse von Geheimdiensten oder den Einsatz von Datenanalysetools durch die Polizei eingeschränkt.

Nur durch eine kontinuierliche Reflexion, Weiterentwicklung und Verteidigung digitaler Grundrechte kann sichergestellt werden, dass der Schutzanspruch des Grundgesetzes auch angesichts rasanter technologischer Entwicklungen und der damit verbundenen gesellschaftlichen Herausforderungen gewahrt bleibt. Diese Rechte sind das Fundament, auf dem wir unser Zusammenleben bauen. Es liegt an uns, sie mit Leben zu füllen – jeden Tag aufs Neue.

Danke an Carina Kurella und Michael Buttler für die Unterstützung und Vorarbeit für diesen Beitrag.

Malte Spitz ist Gründer und Generalsekretär der Gesellschaft für Freiheitsrechte (GFF). Die GFF setzt sich mit juristischen Interventionen für eine starke Demokratie, für ein gerechteres Zusammenleben und Freiheit im Digitalen ein. Er engagiert sich für Datenschutz, Netzneutralität und gegen Massenüberwachung. Als Autor und Aktivist prägt er die Debatte um Freiheitsrechte im digitalen Zeitalter. Er ist zudem Mitglied im Nationalen Normenkontrollrat der Bundesregierung.

Annika Eisenhardt

Grundrechte als Rahmenbedingung für die Digitalisierung von Staat und Gesellschaft

Digitalisierung als Politikfeld ist keinesfalls neu, sondern wird seit der Jahrtausendwende mit zunehmender Bedeutung in den Parteiprogrammen aufgegriffen. Digitalpolitik rückt so in den Fokus politischer wie gesellschaftlicher Diskurse. Neben Online-Handel auf wirtschaftlicher und Social Media auf gesellschaftlicher Seite spielt Digitalisierung auch für das Staatshandeln eine Rolle. Während im privaten Bereich digitale Medien inzwischen den Alltag durchdringen, findet Behörden- und Gerichtsarbeit noch nicht vollständig im digitalen Raum statt. Das ändert sich mittlerweile durch die Einführung elektronischer Akten und Postfächer bei Behörden, Gerichten und der Anwaltschaft. Doch was bedeuten diese Änderungen für die Grundrechte? Sie regeln schließlich, dass Bürger*innen ein privater Bereich frei von staatlichem Zugriff verbleiben soll. Bringt Digitalisierung neue Herausforderungen für die Grundrechte mit sich?

Nationale und internationale Rechtsquellen der Grundrechte

Wer in Gesetzen nach „Grundrechten“ sucht, wird an verschiedenen Stellen fündig. Zentral ist die deutsche Verfassung: das Grundgesetz für die Bundesrepublik Deutschland. Natürlich war die Digitalisierung bei dessen Inkrafttreten im Jahr 1949 noch in weiter Ferne. Aufmerksam Lesenden wird aber auffallen, dass auch 2025 weder das Wort „digital“ noch verwandte Begriffe wie „Daten“ im Grundrechtekatalog (Artikel 1 – 19) auftauchen.

Auch in der völkerrechtlichen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention) von 1953 gibt es Grundrechte. Daneben enthält die Charta der Grundrechte der Europäischen Union (Grundrechte-Charta) von 2009 Grundrechte für alle Bürger*innen der EU. Während das Grundgesetz und die Europäische Menschenrechtskonvention Digitalisierung begrifflich gar nicht kennen, regelt Artikel 8 der Grundrechte-Charta zumindest den Schutz personenbezogener Daten.

Grundgesetz
(Deutsches Verfassungsrecht)

Grundrechte Charta
(Unionsrecht)

Europäische Menschenrechtskonvention
(Völkerrechtlicher Vertrag)

Ausdrücklich werden digitale Grundrechte aber nirgends genannt. Das hängt damit zusammen, dass das Grundgesetz und damit die Grundrechte den Kern der Rechtsordnung bilden und dementsprechend nur besonders zentrale Aspekte regeln. Unter anderem deshalb sind Änderungen des Grundgesetzes an besondere Voraussetzungen geknüpft, zum Beispiel strengere Mehrheitsverhältnisse im Bundestag. Um solche Mehrheiten zu erreichen, sind komplexe politische Abstimmungsprozesse nötig. Daher werden Grundrechte nur selten geändert oder gar um neue Grundrechte ergänzt.

Digitalisierung als neue Verfassungswirklichkeit

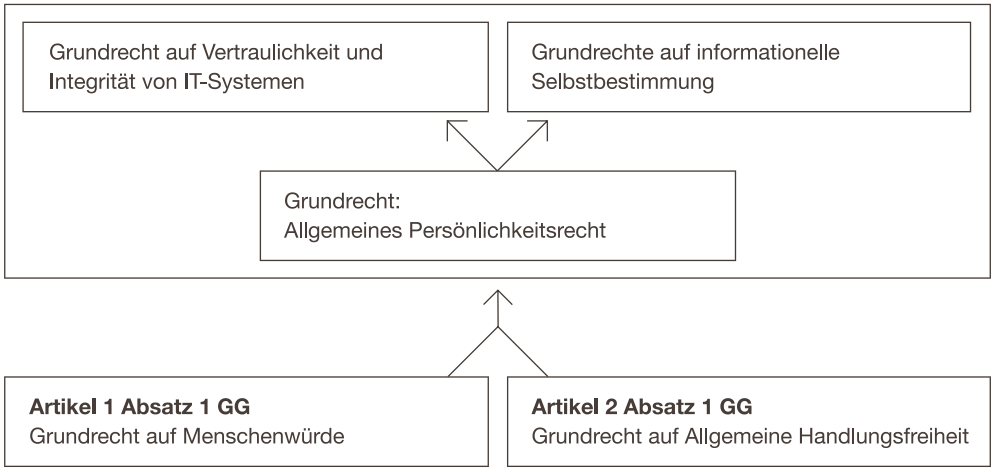
Unabhängig davon, ob es sich um deutsche oder europäische Gesetze handelt, bedarf es der Auslegung, wenn sie auf konkrete Einzelfälle angewendet werden sollen: Es muss also interpretiert werden, was der Gesetzestext meint. Das gilt ebenso für das Verständnis und die Anwendung der einzelnen Grundrechte. Die Auslegungsmethoden sind das Handwerkszeug von Jurist*innen. Ein Beispiel: Obwohl der ursprüngliche Begriff der Versammlung digitale Räume nicht kannte, ist zum Beispiel durch Auslegung des Artikels 8 des Grundgesetzes eine digitale Versammlung vorstellbar, die unter den Schutz des Grundrechts auf Versammlungsfreiheit fällt. So sind auch Meinungsäußerungen im digitalen Raum durch das Grundrecht auf Meinungsfreiheit aus Artikel 5 des Grundgesetzes geschützt.

Ist das Grundgesetz mit einer neuen Wirklichkeit konfrontiert – hier der Digitalisierung – kann das dazu führen, dass Auslegung

allein nicht genügt. Können solche neuen Umstände durch Auslegung nicht ausreichend erfasst werden, ist es möglich, neue Artikel und damit neue Grundrechte in das Grundgesetz einzufügen. Alternativ kann bestehenden Artikeln wegen der veränderten Umstände eine zusätzliche, neue Bedeutung gegeben werden. Das wird „Verfassungswandel“ genannt. Zum Teil erforschen das Rechtswissenschaftler*innen, doch auch das Bundesverfassungsgericht trägt durch seine Rechtsprechung stark zum Verständnis des Grundgesetzes bei. Seine Aufgabe ist, das Grundgesetz in strittigen Fällen richtig anzuwenden.

So entwickelte das Bundesverfassungsgericht schon 2008 das *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht),* was Bürger*innen beispielsweise davor schützt, dass von ihnen genutzte IT-Systeme durch den Staat ausgespäht werden. Dass auch einzelne Daten der Bürger*innen sensibel sind und der Staat nicht einfach so auf sie zugreifen darf, wurde lange vor der Digitalisierung im Volkszählungsurteil von 1983 entschieden: Bürger*innen kommt das *Grundrecht auf informationelle Selbstbestimmung* zu.

Beide Grundrechte entstanden durch Verfassungswandel. Das Bundesverfassungsgericht verankert sie im sogenannten Allgemeinen Persönlichkeitsrecht, das sich wiederum aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG ergibt.



Schon ohne neu ins Grundgesetz geschriebene digitale Grundrechte bieten die bereits jetzt niedergeschriebenen Grundrechte einen viel weiteren Schutz, als der bloße Text vermuten lässt. Obwohl die Auswirkungen der Digitalisierung für den Verfassungsgeber bei der Formulierung vor vielen Jahrzehnten nicht erkennbar waren, bieten die Grundrechte durch ihre Offenheit also einen umfassenden Schutz.

Digitalisierung des Staates gleich Konflikt mit Grundrechten?

Digitale Grundrechte sind relativ neu und in der Anwendung komplex, was auch den Staat vor Herausforderungen stellt. Die Idee, bei Verwaltungen stets digitale Anträge stellen zu können, ist grundsätzlich gut, weil dadurch beispielsweise Barrieren abgebaut würden. Umgekehrt sollen Bürger*innen in Wahrnehmung ihres Grundrechts auf informationelle Selbstbestimmung darüber entscheiden können, welche ihrer Daten sie preisgeben.

Wegen des IT-Grundrechts müssen von Behörden genutzte IT-Systeme gespeicherte Daten vor unbefugten staatlichen Zugriff ausreichend schützen. Zusätzlich gibt es neben dem Internet, was als ein solches IT-System eingeordnet wird, mittlerweile deutlich vielfältigere Algorithmen und Anwendungen der künstlichen Intelligenz. Deren (staatliche) Nutzung birgt neue Risiken, vor denen die Grundrechte Bürger*innen schützen müssen. Wegen dieser Risiken wird auch die Frage aufgeworfen, ob Grundrechte darüber hinaus vor besonders mächtigen privaten Akteur*innen schützen müssen, beispielsweise wenn sie Algorithmen und künstliche Intelligenz nutzen, um umfassende persönliche Datenprofile zu erstellen.

Akteur*innen für Digitalpolitik – gerechter Interessenausgleich als Ziel

Diese verschiedenen und häufig gegenläufigen Interessen müssen im staatlichen Gefüge sichtbar und berücksichtigt werden. In Deutschland sind dafür auf Bundesebene das *Bundesministerium des Inneren und für Heimat* (BMI) und das *Bundesministerium für Digitales und Staatsmodernisierung* (BMDS) zuständig. Auf europäischer Ebene ist für Digitalpolitik vor allem die *Europäische Kommission* zuständig, die Strategiepapiere, Ziele und Gesetzesentwürfe zur Förderung von Digitalisierung bei gleichzeitiger Wahrung der Rechte der Bürger*innen formuliert und vorstellt. Darüber hinaus gibt es zahlreiche nicht staatliche Interessenverbände mit unterschiedlichen Schwerpunkten: Bei künstlicher Intelligenz setzen sich einige für ihre Förderung und Deregulierung, andere für den Schutz der Bürger*innen und Regulierung ein.

Solche Interessen sind auch für die Grundrechte von Bedeutung, weil eine Grundrechtsverletzung dann eintritt, wenn der Staat keine gerechte Interessenabwägung vorgenommen hat. Hält sich eine Behörde oder ein Gesetzgeber also nicht an die Grundrechte, kann das durch – ebenfalls grundrechtsgebundene – Gerichte geprüft und schließlich durch das Bundesverfassungsgericht festgestellt werden. So kann ein Gesetz oder eine Maßnahme der Verwaltung für verfassungswidrig erklärt werden. Dann muss das Gesetz gegebenenfalls neu geschrieben, die Maßnahme korrigiert oder zurückgenommen werden. Für die Durchsetzung digitaler Grundrechte vor Gericht setzen sich insbesondere Nichtregierungsorganisationen (NGOs) ein, die Betroffene von Grundrechtsverletzungen bei Verfahren vertreten und Öffentlichkeitsarbeit leisten, um für Grundrechtsverstöße im digitalen Raum zu sensibilisieren. Sie tragen maßgeblich dazu bei, dass Gesetze und staatliches Handeln überprüft und bei Grundrechtsverstößen für verfassungswidrig erklärt werden.

Digitale Rechte im Wandel des Verfassungsverständnisses

Für die Durchsetzung digitaler Grundrechte sind im rechtsstaatlichen Gefüge also eine Vielzahl staatlicher und nicht staatlicher Akteur*innen zuständig. Auch wenn das Grundgesetz digitale Grundrechte begrifflich nicht kennt, sind Bürger*innen durch Auslegung der Grundrechte sowie den Verfassungswandel und das damit einhergehende, sich stetig fortentwickelnde Grundrechtsverständnis vor negativen Folgen der Digitalisierung geschützt.

Dr. Annika Eisenhardt ist Diplom-Juristin und schloss ihr Studium im Oktober 2023 mit der Ersten Prüfung ab. Seitdem ist sie wissenschaftliche Mitarbeiterin und Doktorandin an einem Lehrstuhl für Öffentliches Recht an der Universität Osnabrück. Sie ist dezentrale Gleichstellungsbeauftragte am Fachbereich Rechtswissenschaften und Vorstandsvorsitzende der Regionalgruppe Osnabrück des Deutschen Juristinnenbunds e. V..

Theodor Ahrens & Michelle Trimborn

Demokratie braucht Daten – Informationsfreiheit zwischen Anspruch und Wirklichkeit

Wissen ist Macht – und ein demokratisches Recht

Wir alle haben ein Recht auf amtliche Informationen. Dieses Recht nennt sich Informationsfreiheit und ist eine zentrale Voraussetzung und das Fundament für eine offene Gesellschaft und Demokratie – denn hier ist wortwörtlich Wissen Macht. Nur wer informiert ist, kann als Bürger*in mitbestimmen und teilhaben. Informationsfreiheit schafft Transparenz, denn sie ermöglicht es uns, den Staat zu überprüfen und somit auch Vertrauen in staatliche Strukturen zu stärken.

Digitale Technologien haben den Zugang zu Wissen radikal vereinfacht – zumindest auf den ersten Blick. Sie haben grundlegend verändert, wie Informationen erzeugt, gespeichert und verbreitet werden. Damit ist auch unser Zugriff auf staatliche Informationen im Wandel. Einerseits ermöglichen digitale Prozesse einen schnelleren, unkomplizierteren Zugriff auf Informationen – zumindest theoretisch. Andererseits gibt es aber zahlreiche Hürden: So arbeiten manche staatlichen Behörden weiterhin sehr analog; digitale informelle Kommunikation, etwa über Messenger-Dienste, macht politische Absprachen intransparent; große Datenmengen, Algorithmen und die omnipräsente Desinformation fordern von uns, den Begriff der Informationsfreiheit zu überdenken. Was wir brauchen, ist nicht nur ein Anfragerecht auf Informationen, sondern eine echte, aktive, barrierefreie und digitale Transparenzkultur, die uns allen hilft.

Das IFG – ein Werkzeug für Transparenz mit vielen Lücken

Das deutsche Informationsfreiheitsgesetz (IFG) ist seit seiner Einführung im Jahr 2006 ein unerlässliches Werkzeug gegen staatliche Intransparenz und Machtmissbrauch. Es ermöglicht allen Menschen, unabhängig von Wohnsitz oder Staatsbürgerschaft, den Zugang zu amtlichen Informationen deutscher Behörden. Dazu gehören zum Beispiel Einsicht in Verwaltungsentscheidungen, Gutachten, Lobbytermine von Minister*innen und politische Absprachen – ohne Begründung, Rechtfertigung oder eigene Betroffenheit.

Das IFG trat am 1. Januar 2006 in Kraft. Dem voraus ging eine langjährige gesellschaftliche und politische Debatte über die Forderung nach mehr Transparenz in der Bundesverwaltung. Schon in den 1990er-Jahren forderten zivilgesellschaftliche Organisationen, aber auch Journalist*innen mehr Transparenz über politische Prozesse. Als Berlin (1999) und Schleswig-Holstein (2000) Informationsfreiheitsgesetze auf Länderebene einführten, erhöhte das den Druck auf die Bundesregierung. Inzwischen haben 14 der 16 Bundesländer eigene Informationsfreiheitsgesetze für den Zugang zu Informationen auf Landesebene – nur Bayern und Niedersachsen verweigern bis heute die Einführung.

Die Informationsfreiheit ist ein Antragsrecht, das heißt, Bürger*innen fragen Informationen an, Behörden müssen antworten. Das Bundes-IFG regelt, von welchen Behörden welche Informationen angefragt werden können.

Paragraf 1 (1) des IFG besagt: „Jeder hat nach Maßgabe dieses Gesetzes gegenüber den Behörden des Bundes einen Anspruch auf Zugang zu amtlichen Informationen. Für sonstige Bundesorgane und -einrichtungen gilt dieses Gesetz, soweit sie öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen. Einer Behörde im Sinne dieser Vorschrift steht eine natürliche Person oder juristische Person des Privatrechts gleich, soweit eine Behörde sich dieser Person zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben bedient.“

Mit dem Bundes-IFG kann man also Informationen und Dokumente bei den Verwaltungseinrichtungen des Bundes anfragen. Dazu gehören die obersten Bundesbehörden, wie zum Beispiel Ministerien, genauso wie untergeordnete Behörden, also etwa das Bundesamt für Migration und Flüchtlinge (BAMF) oder die Bundeszentrale für politische Bildung. Die Landes-IFGs ermöglichen dementsprechend Anfragen bei Landesbehörden. Unter die Auskunftspflicht fallen zum Beispiel auch die öffentlich-rechtlichen Rundfunkanstalten, Schulen oder öffentliche Unternehmen. Gleichzeitig macht das IFG aber auch viele Ausnahmen dazu, was abfragbar ist, etwa mit Verweis auf Geschäftsgeheimnisse oder den Schutz besonderer öffentlicher Belange. Angefragt werden können zum Beispiel Protokolle, Gästelisten und Kalendereinträge von Terminen, dienstliche Korrespondenz in der Behörde oder auch mit Außenstehenden wie Unternehmen, Verträge und Weisungen. Nicht angefragt werden können zum Beispiel private Kommunikation und Dokumente, die nicht vorhanden sind (etwa wenn es zu einem Telefonat kein Protokoll gibt), da eine Behörde die angefragten Unterlagen nicht extra erstellen muss.

Über das Bundes- und die Länder-IFGs hinaus sind aber auch andere Informationsfreiheitsgesetze in Deutschland relevant. Beispiele sind etwa die EU-Verordnung Nr. 1049/2001, die den Zugang zu Dokumenten des Europäischen Parlaments, der Kommission und des Rates regelt. Außerdem ist bereits 1994 das Umweltinformationsgesetz (UIG) in Kraft getreten, das 2005 noch einmal durch die Umsetzung der internationalen Aarhus-Konvention gestärkt wurde. Das UIG regelt gesondert den Zugang zu Umweltinformationen bei Bundesbehörden, also zum Beispiel Informationen über den Wasserverbrauch großer Konzerne oder über die Feinstaubbelastung am eigenen Wohnort. Und über das Verbraucherinformationsgesetz (VIG) können zum Beispiel Berichte von Hygienekontrollen in Restaurants angefragt werden.

Die Informationsfreiheitsgesetze helfen dabei, Transparenz zu schaffen. Sie werden von interessierten Privatpersonen und Aktivist*innen genauso genutzt wie von investigativen Journalist*innen. Im Gegensatz zu Presseanfragen, bei denen Journalist*innen oft paraphrasierte Statements als Antwort erhalten, kann man über das IFG direkt Dokumente anfragen – etwa Protokolle von Treffen in Ministerien. So wurden durch Informationsfreiheitsgesetze vor allem Lobbyskandale über Einflussnahme von Unternehmen auf politische Vorgänge aufgedeckt. Zum

Beispiel kam so heraus, wie viel Einfluss die *Nord Stream 2 AG* auf die umstrittene Stiftung *Klima- und Umweltschutz MV* (Mecklenburg-Vorpommern) hatte oder dass Philipp Amthor (CDU) im Wirtschaftsministerium für ein windiges US-Sicherheitsunternehmen lobbyierte.

Aber es geht beim IFG nicht immer um Bundespolitik, sondern auch um unseren ganz normalen Alltag. Zum Beispiel konnten bei dem zivilgesellschaftlichen Projekt „Verschlusssache Prüfung" – dank 2.000 IFG-Anfragen an Bildungsbehörden – die Schul-Abschlussprüfungen aus den Vorjahren befreit werden, die Schüler*innen die Prüfungsvorbereitung erleichtern. Die Plattform *FragDenStaat* stellte sie dann kostenfrei online. Normalerweise hätten Schüler*innen die alten Prüfungen kaufen müssen, da die Behörden sie an private Verlage verkaufen.

Hürden, Taktiken, Rückschritte: Wo das IFG versagt

Was auf dem Papier ordentlich klingt, ist in der Praxis jedoch oft schwierig, denn von echter Transparenz sind die derzeitige Gesetzgebung und ihre behördliche Umsetzung nämlich noch weit entfernt. Zwar digitalisieren und erleichtern zivilgesellschaftliche Transparenzportale wie *FragDenStaat* den Anfrageprozess und die Kommunikation mit den Behörden – aber nur selten folgt auf eine Anfrage einfach das angefragte Dokument. Stattdessen gibt es Ablehnungen aus verschiedenen, oft fadenscheinigen Gründen (zum Beispiel Sicherheitsbedenken, Geschäftsgeheimnisse) oder lange Verzögerungstaktiken der Behörden. Wenn dann mal geantwortet wird, enthalten die Dokumente Hunderte geschwärzte Seiten ohne Mehrwert. Außerdem argumentieren Behörden immer wieder, dass die Beantwortung der Anfrage einen hohen Verwaltungsaufwand erfordert, und erheben oder drohen mit hohen Gebühren von bis zu 500 Euro. Zu guter Letzt müssen Informationen immer wieder vor Gericht eingeklagt werden, weil Behörden den Zugang unrechtmäßig verweigern. Das schreckt ab – was viele Behörden durchaus beabsichtigen.

Außerdem beschneidet das Bundesverwaltungsgericht Urteil um Urteil die Reichweite und Nutzbarkeit des IFG. 2024 entschied das

Gericht, dass anonyme IFG-Anträge nicht mehr zulässig seien. Behörden können jetzt bei jedem Antrag Name und Postadresse der*des Anfragenden fordern – und sogar per Post antworten. Hier machen die Digitalisierung und die ganze Informationsfreiheit also eine Rolle rückwärts, denn nicht jeder Mensch kann oder möchte Behörden eine Postanschrift liefern. Und statt mit einer schnellen Antwort per Mail müssen Anfragende jetzt immer damit rechnen, als Antwort von Behörden umfangreiche Aktenstapel in Papierform zu erhalten.

Mit all diesen Hindernissen verstärkt der behördliche Umgang mit der Informationsfreiheit oft eine Machtasymmetrie – denn wer hat Ressourcen, um zu klagen oder Hunderte Euro zu zahlen? Insbesondere marginalisierte Gruppen verlieren damit ihren Zugang zu Informationen, einige wenige werden hingegen durch die Strukturen privilegiert. Und damit ist das IFG am Ende oft weit entfernt von dem niedrigschwelligen und demokratiefördernden Transparenzwerkzeug, das es eigentlich sein soll.

Zwischen Datenflut und Desinformation: Chancen und Risiken der Digitalisierung

Das Informationsfreiheitsgesetz ist zurzeit also mit mehreren, teils konträren Herausforderungen konfrontiert. Auf der einen Seite kann die Digitalisierung die Verbreitung von Informationen erleichtern, rasant beschleunigen und demokratisieren. Gleichzeitig machen die Menge an Daten, der Einsatz von Algorithmen und künstlicher Intelligenz in der Informationsverarbeitung und -verbreitung, auch in der Verwaltung, es nicht nur einfacher, Transparenz in Prozesse zu bringen, sodass sie nachvollziehbarer sind. Und mittendrin stehen die Behörden, die per Gerichtsbeschluss zur Analogisierung zurückkehren können.

Dabei könnte die Digitalisierung der Informationsfreiheit eigentlich zuträglich sein: Zugang zu Informationen wird schneller und kostengünstiger, wir haben die Chance auf einen besseren Zugang

ohne großes Vorwissen und auf bessere Analyse und Visualisierung von Daten. Gleichzeitig birgt sie aber auch Risiken. Die zunehmende Verbreitung von „Fake News“ und Desinformationskampagnen im digitalen Raum, die für viele Menschen manchmal kaum erkennbar sind, gefährdet nicht zuletzt unser Vertrauen in die Politik.

Dabei wäre es ein Leichtes, dem mit besserer Transparenz entgegenzuwirken, denn das Informationsfreiheitsgesetz sorgt dafür, dass wir uns nicht auf Erzählungen verlassen müssen, sondern originale Dokumente und Quellen direkt beim Staat anfragen können. Dies stärkt nicht nur den Wahrheitsgehalt der Informationen im Umlauf und verbessert etwa die journalistische Berichterstattung, sondern macht politische Entscheidungen und Medienberichte leichter nachvollziehbar – was eigentlich gute Mittel gegen den Vertrauensverlust und für die Legitimation politischer Prozesse sind.

Dies funktioniert jedoch nur, wenn der Staat seiner Dokumentationspflicht nachkommt – und nicht etwa Informationen verschweigt, um seine Transparenzpflicht zu umgehen. Auch hier können transparenzfeindliche Behörden die Digitalisierung eher gegen als für die Informationsfreiheit einsetzen. Denn immer wieder sind angefragte Akten unvollständig. Das Problem besteht darin, dass politische Entscheidungen zunehmend über informelle Chats, SMS, Messenger-Nachrichten und E-Mails zustande kommen. Veraktet werden diese in der Regel nicht, auch wenn hier Entscheidungen von großer politischer Tragweite getroffen werden. Und es stellt sich ein weiteres Problem: Selbst wenn man versucht, diese Nachrichten einzuklagen, gehen diese schnell „verloren“, etwa wenn Diensthandys beim Ausscheiden von Mitarbeitenden auf Werkseinstellungen zurückgesetzt oder Mailaccounts gelöscht werden. All das zeigt, dass angesichts der Digitalisierung Reformen nicht nur bezüglich der Informationsfreiheit, sondern auch bei den zugrunde liegenden Behördenvorgängen zwingend notwendig sind.

Für ein echtes Transparenzgesetz – und eine demokratische Informationskultur

In einer Demokratie darf staatliches Wissen nicht verschlossen bleiben, sondern muss der Gesellschaft gehören. Darum dürfen wir uns nicht mit einem Zustand zufriedengeben, in dem Akten absichtlich unvollständig sind oder in dem nur wenige, privilegierte Menschen Zugang zu wichtigen amtlichen Informationen haben. Informationsfreiheit darf nicht länger ein Privileg für diejenigen sein, die es sich leisten können, sondern muss als radikales, universelles Grundrecht verstanden werden.

Viele zivilgesellschaftliche Organisationen und Projekte, aber auch Journalist*innen und Medienschaffende setzen sich darum nicht nur für eine starke Durchsetzung der Informationsfreiheit ein, sondern für die Weiterentwicklung des Informationsfreiheitsgesetzes hin zu einem Transparenzgesetz. Insbesondere konservative Politiker*innen sehen dies jedoch kritisch. Stand die Weiterentwicklung der Informationsfreiheit zum Transparenzgesetz unter der Ampel-Koalition 2021–2024 noch im Koalitionsvertrag[1], versuchten vor allem die Unionsparteien in den Koalitionsverhandlungen 2025, das Informationsfreiheitsgesetz ganz zu streichen.[2] Gegen diese massive Bedrohung der Transparenz lehnten sich nicht nur NGOs, sondern auch Hunderttausende Bürger*innen auf. Im aktuellen Koalitionsvertrag 2025 heißt es nun, dass das IFG reformiert werden soll.

Das wäre ein wichtiger Schritt – eine Reform hin zu einem echten Transparenzgesetz auf Bundesebene. Denn das würde vor allem eines bedeuten: eine proaktive und digitale Veröffentlichungspflicht für gewisse Dokumente, zum Beispiel Gesetzentwürfe und die entsprechenden Stellungnahmen dazu, Gutachten oder Verträge der öffentlichen Hand mit einer Summe von über 100.000 Euro. Dies würde die Informationsfreiheit tatsächlich demokratisieren und allen helfen – Bürger*innen wie Behörden. Während für Anfragende Hindernisse wie hohe Bearbeitungsgebühren und komplizierte Behördenkommunikation reduziert würden, würde sich auch das große Gegenargument der IFG-Gegnerinnen, nämlich der Verwaltungsaufwand, verkleinern. Würden

Dokumente proaktiv veröffentlicht, müssten Behördenmitarbeitende auf weniger Anfragen antworten, was einen Gewinn für alle bedeuten würde. Dass das möglich ist, macht übrigens Hamburg vor: Dort gibt es schon seit 2012 ein Transparenzgesetz. Weil die Politik jedoch zögert, hat die Zivilgesellschaft das Vorhaben Transparenzgesetz schon längst selbst in die Hand genommen und bereits 2022 einen Entwurf vorgelegt. Er müsste nur umgesetzt werden.

Wenn Wissen Macht ist, darf es in einer Demokratie nicht nur beim Staat liegen. Unser gemeinsames Ziel muss eine offene, digitale und barrierefreie Infrastruktur für Transparenz sein, die sich den Bedürfnissen der Menschen anpasst und ihnen die Kontrolle über den Informationsfluss ermöglicht. Wir als Bürger*innen haben ein Recht darauf, staatliche Macht und staatliches Wissen zu hinterfragen, um teilhaben zu können und um widerstandsfähig zu bleiben. Denn die Informationsfreiheit ist nicht nur ein Recht, sondern auch eine Verpflichtung, die wir alle gemeinschaftlich tragen, um unsere Demokratie lebendig und widerstandsfähig zu halten. Es ist unsere gemeinsame Verantwortung, dieses Grundrecht zu schützen, zu fördern und weiterzuentwickeln.

Theodor Ahrens macht einen Bundesfreiwilligendienst bei FragDenStaat.

Michelle Trimborn kümmert sich bei FragDenStaat um die Öffentlichkeitsarbeit und entwickelt politische Kommunikationsstrategien, vor allem zu den FragDenStaat-Klagen.

Quellen

1 Koalitionsvertrag 2021–2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90 / Die Grünen und den Freien Demokraten (FDP)
2 Arne Semsrott: Union will Informationsfreiheitsgesetz abschaffen, Frag Den Staat, 26.03.2025

Weiterführende Links

- Der zivilgesellschaftliche Entwurf für ein Transparenzgesetz: transparenzgesetz.de
- Die Plattform FragDenStaat erleichtert das Stellen von IFG-Anfragen: fragdenstaat.de

Mathis Rehse & Simone Ruf

Strategische Klagen gegen Big Brother und Big Tech

Wie strategische Prozessführung digitale Freiheitsrechte gegen Staat und Plattformen verteidigt

47

Grundrechte sichern Freiheitsräume von Personen gegenüber dem Staat ebenso wie gegenüber Unternehmen. Sie sind aber nur wirksam, wenn es Möglichkeiten gibt, dass sich Personen effektiv dagegen wehren können, wenn sie in ihren Grundrechten verletzt werden. Andernfalls verlieren sie an Wert und Bedeutung.

Gerichtsverfahren sind eine Möglichkeit, gegen die Bedrohung und Verletzung von Freiheitsrechten vorzugehen. Die Gesellschaft für Freiheitsrechte (GFF) nutzt deshalb das Mittel der sogenannten strategischen Prozessführung. Das Ziel dabei ist, nicht nur in Einzelfällen für Gerechtigkeit zu sorgen, sondern über Gerichtsverfahren grundsätzliche Fragen zu klären, die viele Menschen betreffen. Strategische Prozessführung nutzt also einzelne Verfahren, um strukturelle Missstände zu verändern – also Recht durch praktische Anwendung zu gestalten. Von den Prozessen sollen so in Zukunft auch andere Personen profitieren, die in ähnlichen Situationen in ihren Freiheitsrechten betroffen sind.

Gerade im technischen Bereich ist diese Art strategischer Prozessführung besonders relevant, denn neue Technologien bedeuten auch, dass es noch keine ausdifferenzierte Rechtsprechung gibt. Da wird sich schnell auf vermeintliche Grauzonen zurückgezogen. Durch den schnellen technischen Fortschritt ist es aber umso wichtiger, frühzeitig zu klären, wo die Grenzen verlaufen. Wie stellen wir sicher, dass KI nicht diskriminiert und welche Daten für deren Training verwendet werden dürfen? Welche Pflichten haben Plattformen, Marktplätze und Suchmaschinen gegenüber den Nutzenden? Unter welchen Bedingungen dürfen staatliche Behörden wie die Polizei oder der Verfassungsschutz neue technische Mittel einsetzen und damit in unsere Grundrechte eingreifen? Der Gesetzgeber ist nicht immer in der Lage, den rapiden technischen Entwicklungen hinterherzukommen. Auch neue Gesetze gewinnen häufig erst durch die Auslegung durch Gerichte an Konturen. Teilweise gehen Gesetze auch zu weit und es bedarf einer Einschränkung durch das Bundesverfassungsgericht oder den Europäischen Gerichtshof. Hinzu kommt, dass es vielen Personen nicht bewusst ist, wie Technologie funktioniert, und damit auch, welche Risiken bestehen. Hier helfen gerichtliche Entscheidungen bei der Aufklärung. All dies kann strategische Prozessführung erreichen.

Mit Verfassungsbeschwerden gegen staatliche Überwachung

Ein besonders wirksames Mittel hierfür ist die Verfassungsbeschwerde beim Bundesverfassungsgericht. Entscheidet das Bundesverfassungsgericht im Rahmen einer Verfassungsbeschwerde, dass ein Gesetz eine Person in ihren Grundrechten verletzt, erklärt es das Gesetz für verfassungswidrig. Von der Entscheidung profitiert dann nicht nur die Person, die Verfassungsbeschwerde erhoben hat, sondern alle Personen, die von dem Gesetz betroffen waren. Die Verfassungsbeschwerde ist also sehr effektiv für den Schutz von Freiheitsrechten. Damit eine Verfassungsbeschwerde Erfolg hat, muss sie allerdings gut begründet sein. Um eine gute Begründung zu formulieren, ist in der Regel viel Arbeit und juristischer Sachverstand erforderlich. Die GFF unterstützt die betroffenen Kläger*innen auf zwei Weisen: Indem sie selbst juristisches Fachwissen einbringt und/oder das Verfahren koordiniert. Dadurch werden die Erfolgschancen einer Verfassungsbeschwerde erhöht.

Die GFF setzt sich mit dem Mittel der Verfassungsbeschwerde zum Beispiel gegen übermäßige Überwachungsbefugnisse von Sicherheitsbehörden ein – etwa der Polizeibehörden des Bundes und der Länder, aber auch der Nachrichtendienste. Sowohl der Bund als auch die Länder schaffen immer wieder Gesetze, die es diesen Behörden erlauben, große Mengen an sensiblen Daten über Personen zu erheben, zu speichern und auszuwerten.

Die GFF ist konkret an einer Verfassungsbeschwerde gegen Befugnisnormen des sogenannten Artikel-10-Gesetzes beteiligt. Diese erlauben es Verfassungsschutzbehörden und Nachrichtendiensten, unter bestimmten Voraussetzungen auf IT-Systeme wie Smartphones zuzugreifen und die Kommunikation der betroffenen Person auszuspähen. Dazu gehören Telefonate, Sprachnachrichten, Chat-Nachrichten und SMS, in sozialen Netzwerken geteilte Inhalte, Kommentare, mit anderen Personen geteilte Daten, das Surfverhalten, hoch- oder heruntergeladene Dateien auch aus der Cloud und vieles mehr. Die Aufzählung zeigt, dass nahezu jeder Lebensbereich erfasst ist. Personen

wissen oft nicht, dass sie Betroffene von solchen Überwachungsmaßnahmen sind, weil alles heimlich abläuft. Von der Überwachung sind auch Menschen betroffen, die mit einer überwachten Person kommunizieren – also selbst gar nicht Ziel der Überwachung sind. Unter den Kläger*innen sind daher auch Rechtsanwält*innen und Journalist*innen, die genau dies befürchten.

Diese gesetzlichen Befugnisse beeinträchtigen die Grundrechte der betroffenen Personen. Zum einen ist das Fernmeldegeheimnis betroffen. Es schützt die Vertraulichkeit der Kommunikation. Der Staat darf sich von der Kommunikation grundsätzlich keine Kenntnis verschaffen. Daneben ist das allgemeine Persönlichkeitsrecht als Grundrecht betroffen. Denn auf Smartphones findet sich weit mehr als Kommunikation. Sie geben heutzutage um einiges mehr über die besitzende Person preis als zum Beispiel Tagebücher. Sie enthalten Standort- und Bewegungsdaten, Gesundheitsdaten, Fotos, Videos und vieles mehr. Nur unter sehr engen Voraussetzungen dürfen diese Rechte beschränkt werden. Wenn es um den sogenannten Kernbereich privater Lebensgestaltung geht, ist es dem Staat verboten, diesen auszuspionieren. Dazu gehört zum Beispiel das Sexualleben der betroffenen Person. Die Befugnisse des Artikel-10-Gesetzes reichen aber zu weit und verletzen deshalb die genannten Grundrechte.

Es bleibt abzuwarten, wie das Bundesverfassungsgericht entscheiden wird. Das Verfahren ist eines von mehreren im Bereich grundrechtsverletzender staatlicher Überwachung, gegen welche sich die GFF wendet. Erfolgreich geklagt hat die GFF unter anderem bereits gegen die automatisierte Datenanalyse durch Polizeisoftware in Hamburg und Hessen, bei der eine Vielzahl an Daten kombiniert wird, um so Straftaten vorherzusagen. Ein anderes erfolgreiches Verfahren richtete sich gegen die Befugnisse des bayerischen Verfassungsschutzes, beispielsweise V-Leute nahezu ohne Begrenzung einzusetzen und Handys und Wohnräume zu überwachen, ohne dass eine dringende Gefahr bestand.

Big Tech in die Schranken weisen

Freiheitsrechte spielen jedoch nicht nur im Verhältnis zwischen Bürger*innen und Staat eine Rolle. Große soziale Netzwerke wie X (ehemals Twitter), Instagram, Facebook oder Tiktok haben einen erheblichen Einfluss darauf, ob und wie Nutzende ihre Freiheitsrechte auf diesen Plattformen ausüben können. Sperrt eine Plattform Nutzende, werden sie ihrer digitalen Stimmen beraubt. Dies betrifft dann meist das Grundrecht der Meinungsfreiheit. Aber auch andere Grundrechte wie die Kunstfreiheit oder die damit verwandte Filmfreiheit können betroffen sein. Diese schützen nicht nur die Herstellung von Kunst und Filmen, sondern auch die Werbung für diese.

Grundrechte sind zwar in erster Linie als Abwehrrechte gegen staatliche Eingriffe konzipiert. Sie sind aber auch Teil der objektiven Werteordnung des Grundgesetzes. Daher werden sie auch im Verhältnis zwischen Privatpersonen berücksichtigt und fließen bei der Auslegung anderer Gesetze mit ein. Dies gilt ganz besonders gegenüber großen Plattformen. Diese kontrollieren, was sichtbar ist – und wer überhaupt gehört wird. Nutzende können sich deshalb zum Beispiel bei der Sperrung eines Accounts gegenüber den Plattformen auch auf ihre Grundrechte, insbesondere die Meinungsfreiheit berufen.

Teil der strategischen Prozessführung der GFF ist es, gegen willkürliches und grundrechtsverletzendes Verhalten von Plattformen vorzugehen, zum Beispiel, wenn diese Accounts oder einzelne Inhalte sperren.

Ein anschauliches Beispiel ist die von der GFF unterstützte Klage der Filmwerkstatt Düsseldorf gegen *Meta*, den Mutterkonzern von Facebook. Die Filmwerkstatt – ein Zusammenschluss von Filmschaffenden – hatte im Rahmen einer Filmankündigung ein Bild mit traditionell bekleideten indigenen Menschen auf Facebook gepostet. Facebook sperrte daraufhin den Account – mutmaßlich wegen eines vermeintlichen Verstoßes gegen die Gemeinschaftsstandards. Da die Sperrung Grundrechte verletzt, hat die GFF eine Klage gegen *Meta* unterstützt. Das Landgericht Düsseldorf sowie später das Oberlandesgericht gaben der Filmwerkstatt Recht.

Entscheidend war, dass die Filmwerkstatt Düsseldorf in Düsseldorf klagen konnte. Denn nur wenn ein Gericht örtlich zuständig ist, kann es auch in der Sache entscheiden. Das ist immer wieder problematisch, da große Plattformen ihren Sitz meist nicht in Deutschland, sondern in Irland haben. Dort zu klagen, wäre aber mit großem finanziellem Aufwand verbunden – vor allem für kleinere Organisationen ist das ein Problem. Im Verfahren der Filmwerkstatt konnte über das Kartellrecht ein Weg gefunden werden, *Meta* auch in Deutschland zu verklagen. Prozesse gegen Plattformen auch vor Ort zu führen, ist für die praktische Durchsetzung von Freiheitsrechten im digitalen Raum unabdingbar.

Das zeigt: Der Schutz digitaler Freiheitsrechte lebt von ihrer Durchsetzbarkeit. Mit gezielten Klagen gegen Staat und Konzerne stärkt die GFF systematisch den Schutz digitaler Freiheitsrechte.

Mathis Rehse studiert Rechtswissenschaft an der Universität Münster mit dem Schwerpunkt öffentliches Recht und absolviert im Rahmen des Studiums ein Praktikum bei der Gesellschaft für Freiheitsrechte (GFF) im Schwerpunkt „Freiheit im digitalen Zeitalter“.

Dr. Simone Ruf ist seit Oktober 2024 stellvertretende Leiterin des Center for User Rights, Volljuristin und Verfahrenskoordinatorin bei der GFF. Sie studierte in Passau und Augsburg Rechtswissenschaften mit dem Schwerpunkt Bio-, Medizin- und Gesundheitsrecht. Nach einer Promotion im Verfassungsrecht zum Thema „Die legislative Prognose“ absolvierte sie ihr Referendariat in Berlin.

Frederick Richter

Der Datenschutz und die Realität

Digitalisierung ohne Daten ist unmöglich. Für das Vertrauen in die Digitalisierung sind daher zwei Dinge unverzichtbar: gute IT-Sicherheit zum technischen Schutz von Daten und guter Datenschutz zur Wahrung der Grundrechte. Ziel moderner Daten- und Digitalpolitik sollte es sein, die Nutzung von Daten zum Wohle der Allgemeinheit zu fördern. Gleichzeitig sind die Rechte und Freiheiten der Menschen wirksam zu schützen. Doch wie gelingt das in der digitalen Welt?

Idee und Ideal

Wäre es nicht richtig und wichtig, wenn jeder Mensch selbst festlegen könnte, was andere Menschen und Institutionen über ihn wissen? Sollte nicht die einzelne Person, bis auf bestimmte Ausnahmen, souverän sein hinsichtlich der Informationsbestände, die über sie von anderen aufgebaut werden? Und müsste eine derartige Befugnis nicht erst recht gegenüber der Macht des Staates und seiner Apparate gelten? Gedanken wie diese haben dazu beigetragen, dass vor über vier Jahrzehnten in Deutschland ein neues Grundrecht geschaffen wurde. Ein Datenschutzgesetz gab es zu der Zeit sogar schon ein Jahrzehnt länger, jedenfalls in Hessen. Doch erst mit einem Urteil des Bundesverfassungsgerichts erhielt das sogenannte Recht auf informationelle Selbstbestimmung den Rang eines Grundrechts.

Seitdem ist viel passiert. Nicht mehr nur der Staat erscheint als potenziell datenmächtiger Riese, der die Menschen derart stark überwachen könnte, dass er durch starke Gesetze eingehegt werden muss. In den vergangenen Jahrzehnten entstanden durch technologischen Fortschritt auch diverse private Akteur*innen, denen eine Datenmacht zuwuchs, die geeignet ist, Menschen zu überwachen und ihre Rechtsgüter zu gefährden. Auch das Recht hat sich in dieser Zeit fortentwickelt. Nachdem das Datenschutzrecht in Europa nur vereinzelt und uneinheitlich geregelt war, wurde zu Beginn des Internetzeitalters 1995 die Europäische Datenschutzrichtlinie erlassen und gute zwanzig Jahre später die heute geltende Datenschutz-Grundverordnung (DSGVO).

Die Idee der informationellen Selbstbestimmung stellt für viele Datenschützende noch heute das anzustrebende Ideal für eine

humanistische Informationsgesellschaft dar. Diesem Ideal zufolge sollten Bürger*innen wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Doch konnte dieses Konstrukt des deutschen Verfassungsrechts der 1980er-Jahre keinen internationalen Siegeszug antreten. Der DSGVO liegt nämlich die Europäische Grundrechte-Charta zugrunde – und in der gibt es kein solches Recht auf informationelle Selbstbestimmung, sondern zum einen ein Grundrecht auf Privatsphäre und zum anderen ein Grundrecht auf Datenschutz.

Im Alltag sind solche juristischen Unterscheidungen für die Menschen aber gar nicht so wichtig – praktisch nutzbar ist das geltende Recht für die Selbstbestimmung und Selbsterkenntnis durchaus. Denn jede und jeder kann nach der DSGVO von jedem Unternehmen und jeder Behörde Auskunft darüber verlangen, welche Daten zur eigenen Person in der jeweiligen Einrichtung verarbeitet werden. Es ließe sich dennoch darüber nachdenken, ob es heutzutage überhaupt noch realistisch ist, einen Zustand zu erreichen, in dem ein Individuum tatsächlich wissen kann, wer was wann über die eigene Person weiß. Denn die Datenspuren, die Nutzende im digitalen Raum hinterlassen, sind ohne sehr großen Aufwand nicht mehr überschaubar. Und mit der zunehmenden Digitalisierung des Lebens in der Außenwelt wächst der digitale Raum immer mehr und der nicht mehr datentechnisch erfasste Teil des Lebens schrumpft.

Müssen wir pessimistisch sein? Kommen die Werkzeuge des Datenschutzes also bald an ihre Grenzen? Auf dem Papier sieht die Lage zunächst gut aus: Nutzende können von Datenverantwortlichen nicht nur Auskunft verlangen, sondern auch die Berichtigung falscher Daten oder deren Löschung, sobald keine Berechtigung zum Verarbeiten der die eigene Person betreffenden Daten mehr vorliegt. Auch die Mitnahme der sie betreffenden Daten zu einem anderen Anbieter sieht die DSGVO vor. Und sie können sich schließlich – jederzeit und kostenlos – bei der Datenschutzaufsicht beschweren. Diese Behörden haben dann diverse Möglichkeiten, um gegen Organisationen vorzugehen, die womöglich ihre Daten zuungunsten der Menschen verwenden. Angesichts der Masse der Fälle stellen sich aber zwei Probleme: die Unübersichtlichkeit der vernetzten Lebensumgebung einerseits und die Kapazitäten der behördlichen Datenschutzwächter andererseits.

Technik für mehr Überblick

Wer sich ein komplettes Bild davon machen will, an welchen Stellen eigene Daten verarbeitet werden, steht vor dem Problem, dass er oder sie nicht mehr weiß, wo er überall schon einer Verwendung der Daten zugestimmt hat oder wo er einen Vertrag geschlossen hat, der die Datenverarbeitung gestattet. Es fehlt der Überblick, und daran kann auch das Datenschutzgrundrecht nichts ändern. Es liefert zwar jeder Person starke Instrumente, aber es fehlt die Service-Komponente. Im Zeitalter des One-Click-Shoppings sind die Menschen einfache Prozesse gewöhnt und nutzen diese auch gern. Wenn es um die Durchsetzung eigener Datenrechte geht, ist es aber deutlich aufwendiger, voranzukommen. Dass die Leute selbst aktiv werden, bleibt daher meist die Ausnahme. Abhilfe könnten persönliche elektronische Datenschutzdienste bringen – zum Beispiel eine Privacy-App, mit der ich eine Übersicht erlangen kann, wer Daten mit Bezug zu mir verarbeitet. Allerdings gibt es solche Datenschutzassistenzen bisher nicht, aber sie würden die Position von Verbraucher*innen deutlich stärken können.

Wie schwierig es ist, in dieser Richtung weiterzukommen, zeigte sich im vergangenen Jahr in der deutschen Umsetzung der sogenannten ePrivacy-Richtlinie der EU. Eine Idee war es, Dienste zur Einwilligungsverwaltung zu fördern. Bei einem solchen Modell sollen Nutzende nur einmal festlegen müssen, wie beim Surfen im Netz mit den Anfragen in Cookie-Bannern umgegangen wird. Es könnte also möglich werden, dass mit einer einzigen Voreinstellung alle Cookie-Anfragen entweder abgelehnt oder zugelassen werden, woraufhin keine Banner mehr angezeigt werden müssten. Doch der Bundesgesetzgeber entschied sich für ein freiwilliges Modell, bei dem Werbetreibende die Voreinstellung der Nutzenden ignorieren dürfen und sie weiterhin immer wieder mit Cookie-Bannern nach ihrer Einwilligung fragen können. Ein solches Modell bringt den Nutzenden natürlich nichts.

Werbung könnte so datenschutzfreundlich sein

Noch einfacher wäre es übrigens, wenn Webseiten erst gar kein Werbe-Tracking anderer Unternehmen in ihre Internetpräsenzen einbinden würden; dann müssten Betreiber keine nervenden Banner und Klickboxen einrichten, denn sie bräuchten keine Datenschutz-Einwilligung der Nutzenden mehr. Doch weil viele Unternehmen nicht auf die Refinanzierung kostenloser Inhalte im Netz verzichten wollen, bewegt sich wenig. Die Nutzenden wiederum sind oft nicht bereit, für Inhalte im Netz zu bezahlen, weil sie über viele Jahre daran gewöhnt wurden, dass sie diese Inhalte zwar durchtränkt mit personalisierter und tracking-basierter Werbung, aber eben auch kostenlos angeboten bekommen. Auf diese Weise ist eine verfestigte Situation entstanden, die schwer aufzubrechen ist.

Eine Lösung wäre kontextbasierte Werbung. Anders als bei der personalisierten Werbung, für die das Nutzungs- und Surfverhalten der Menschen exakt beobachtet und über Seiten- und sogar Gerätegrenzen hinweg verfolgt und protokolliert wird, benötigt die kontextbasierte Werbung allein einen Bezug zum Inhalt der Webseite. Wie früher bei gedruckten Zeitungen fände sich neben Autoberichten dann Werbung für Autos und neben Reiseberichten Werbung für Reisen. Die Online-Verlage jedoch befürchten bei dieser Form der Ansprache von Konsumenten einen geringeren Ertrag und favorisieren die Werbung mit elektronischer Beobachtung.

Herausforderungen allerorten

Das Grundrecht auf Datenschutz und seine konkreten Instrumente sehen sich im digitalen Zeitalter großen Aufgaben gegenüber. Eine der größten ist die Erzeugung von immer mehr Daten durch die heutige Umwelt, in der immer mehr Dinge immer vernetzter werden, so beispielsweise Mobilität (vernetztes Fahren), Lebensorte und Energieversorgung (Smart City und Smart Metering) und Gesundheit (von der elektronischen Patientenakte bis zur dauerhaften Selbstvermessung mit dem Fitness-Tracker). Überall stellen sich dabei Datenschutzfragen, denn fast überall lassen sich die gesammelten und aufgezeichneten Informationen direkt oder indirekt auf eine individuelle Person beziehen. Diese Entwicklung ist global nicht zurückzudrehen – auch wenn sich manche mittlerweile ein Recht auf ein analoges Leben als weiteres Grundrecht wünschen.

Es geht dem Datenschutz nicht darum, die Digitalisierung aufzuhalten oder zurückzudrehen (was er faktisch auch nicht könnte). Sondern es muss ihm und all denen, die ihn durchsetzen, darum gehen, ihn menschenzentriert zu gestalten. Das heißt, dass jeweils der konkrete Nutzen im Mittelpunkt stehen sollte, den die Vorschriften zum Umgang mit Daten den Grundrechtsträger*innen bieten sollen. Eine solche Leitschnur sollte nicht nur im Datenschutzrecht bestehen, sondern auch in den benachbarten Gesetzen, die auf europäischer Ebene mehr und mehr quasi um die Datenschutz-Grundverordnung herum aufgestellt werden. Die Vorteile von wirksamem Datenschutz müssen für die Nutzenden erfahrbar werden, sodass sie nicht nur Cookie-Banner wahrnehmen, die sie beim Nutzen des World Wide Web nerven. Es gilt, sich zukünftig auf die wirklich wichtigen Risiken für Individuen und die freie Gesellschaft zu konzentrieren. So gilt es besonders, die großen Anbieter digitaler Dienstleistungen und sozialer Netzwerke im Blick zu behalten. Deren Datenmacht kann zu Beeinträchtigungen sowohl für Personen als auch für das Gemeinwesen führen und sollte ein Fokuspunkt der Regulierung sein. Wenn dagegen der Datenschutz in einer irgendwann komplett datafizierten Welt vor jeglichem noch so geringen Risiko vollumfänglich schützen will, wird er sich unweigerlich überheben.

Ein Datenschutz, der schlimmstenfalls auf dem Papier viel verspricht und in der realen Umsetzung mangels Unterstützung und mangels Kapazitäten zur Durchsetzung zu wenig hält, wird unweigerlich an gesellschaftlicher Akzeptanz und an politischem Rückhalt verlieren. Wohl verstanden und angemessen interpretiert, führt ein solcher humanzentrierter Datenschutz nicht zu wirkungsloser Bürokratie. Er muss auch keine innovativen Geschäftsmodelle oder gar die in Deutschland so dringend notwendige Verwaltungsdigitalisierung verhindern (beides scheitert oft genug an anderen Dingen), sondern er schützt die Menschen spürbar und erfahrbar vor Übergriffen durch Akteur*innen staatlicher Gewalt oder wirtschaftlicher Macht.

Frederick Richter, LL.M, ist seit 2013 Vorstand der Stiftung Datenschutz. Zuvor war er Referent im Deutschen Bundestag und Datenschutzbeauftragter eines Wirtschaftsverbandes. Frederick Richter studierte Rechtswissenschaften an der Universität Hamburg und erwarb einen Masterabschluss im IT-Recht an der Universität Wien. Er ist Mitglied des Beirates der Plattform Privatheit und des Praxisbeirates der Fachzeitschrift Recht der Datenverarbeitung, sowie ständiger Autor der Fachzeitschrift Privacy in Germany.

Macht, Kontrolle und öffentliche Debatte

Michael Kolain & Dennis-Kenji Kipker

Digitale Überwachung durch den Staat

Vom ersten Heimrechner über das Internet bis hin zu Smartphone, zu sozialen Netzwerken und ChatGPT: Wir sind immer stärker vernetzt und digital unterwegs. Wir pflegen weltweit Kontakte, dokumentieren unser Leben mit Bildern und Gedanken, vertrauen unseren digitalen Endgeräten fast alles an. Wer Zugang zu unseren Daten hat, weiß sehr viel über uns – und kann uns engmaschig überwachen.

Im Internet entstehen aber auch bislang unbekannte gesellschaftliche Bedrohungen – etwa, wenn sich Menschen in islamistischen Foren radikalisieren, Erwachsene organisiert Darstellungen sexueller Gewalt herstellen und verbreiten oder kriminelle Gruppen Betrugsmaschen über Messenger etablieren. Weitere Beispiele sind illegale Handelsplattformen im Darknet (etwa der Archetyp Market, den Sicherheitsbehörden kürzlich abgeschaltet haben); Shitstorms, um einzelne Menschen zu diffamieren (wie im „Drachenlord"-Fall); oder die dezentral vernetzte Planung von Anschlägen durch terroristische Organisationen. Neue Formen und Foren für Kriminalität sind eine Schattenseite der schönen neuen digitalen Welt.

Um uns vor Cybercrime und digital vernetzter Kriminalität zu schützen, entstehen im digitalen Zeitalter neue Ermittlungsmethoden. Im 21. Jahrhundert ermittelt die Polizei auch im Netz und nutzt komplexe Computerprogramme. Dabei stellt sich die Frage: Wie weit darf der Staat gehen, um die öffentliche Sicherheit zu schützen – und wo ziehen die Grundrechte einer digitalen Überwachung Grenzen?

Die Arbeit der Polizei im digitalen Zeitalter zwischen Sicherheit und Freiheit

Nach Gewalttaten, Anschlägen oder Festnahmen dreht sich die öffentliche Diskussion oft um die immer gleichen Fragen: Wie konnte so etwas mitten in Deutschland passieren? Warum haben die Sicherheitsbehörden die Taten nicht verhindert? Sind Polizei und Nachrichtendienste im digitalen Zeitalter überhaupt modern genug ausgestattet, um drohende Gefahren

abzuwehren und Straftaten zu verhindern? Oder ist gegen Kriminelle, die ihre Taten raffiniert planen oder im Affekt handeln, manchmal einfach kein Kraut gewachsen?

Die öffentliche Debatte schießt sich nach Anschlägen oder spektakulären Festnahmen besonders hitzig auf bestimmte Ermittlungsmaßnahmen ein, die den deutschen Sicherheitsbehörden nach geltendem Recht noch fehlen – und angeblich geholfen hätten, Leid von den Opfern und Angehörigen abzuwenden. Es fallen dann Schlagwörter wie Vorratsdatenspeicherung, biometrische Überwachung, Quellen-Telekommunikationsüberwachung (aka Staatstrojaner), Datenanalyse mit künstlicher Intelligenz und Chat-Kontrolle. Doch wo verläuft die Grenze zwischen moderner Polizeiarbeit und digitalem Überwachungsstaat? Wie viel Sicherheit ist in einer komplexen und globalisierten Gesellschaft überhaupt möglich?

Die Befürworter zusätzlicher Befugnisse für Polizei und Nachrichtendienste fordern, dass Sicherheitsbehörden in einer zunehmend digitalisierten Welt konsequent digital aufrüsten müssten, um neuen Formen der Kriminalität effektiv zu begegnen. Sie betonen, dass eine Aufgabe des Staates darin besteht, die öffentliche Sicherheit sicherzustellen – und berufen sich oftmals auf die zugespitzte Maxime „Opferschutz statt Datenschutz“.

Doch viele Stimmen, gerade aus Wissenschaft und digitaler Zivilgesellschaft, sehen den Ruf nach mehr digitalen Befugnissen kritisch. Sie sehen in der reflexhaften Forderung nach neuen digitalen Ermittlungsbefugnissen eine Form des politischen Aktionismus. Stattdessen müssten zunächst die Ursachen und Zusammenhänge analysiert werden, warum es überhaupt zu Anschlägen und Gewalttaten hat kommen können. Bürgerrechtler*innen verweisen auf Urteile des Bundesverfassungsgerichts, die Überwachungsbefugnisse für Sicherheitsbehörden in der Vergangenheit als unvereinbar mit grundrechtlichen Mindeststandards erklärt haben. Grundrechtliche Grenzen einer staatlichen Überwachung dürften, so die Kritiker*innen, nicht überschritten werden, wolle man dem Ruf nach Sicherheit nicht zugleich die Freiheit opfern.

Fallbeispiele: Daniela Klette und Sicherheitspaket 2024

Anhand von zwei aktuellen Beispielen wollen wir das Spannungsfeld und die Dynamik der politischen Debatte über Sicherheit und Freiheit exemplarisch illustrieren.

Als die Polizei im Februar 2024 das ehemalige Mitglied der linksterroristischen Roten Armee Fraktion (RAF) Daniela Klette in Berlin-Kreuzberg festnahm, ging ein Raunen durch die Öffentlichkeit. Denn Klette galt über Jahrzehnte als untergetaucht, überfiel angeblich mehrere Geldtransporter, wurde immer mal wieder auf dem Land oder im Ausland vermutet – lebte aber offenbar seit Jahren mitten in der deutschen Hauptstadt. Die Spur nach Kreuzberg begann mit dem Podcast „Legion – Most Wanted: Wo ist RAF-Terroristin Daniela Klette?“ In Zusammenarbeit mit einem Journalisten der Rechercheplattform *Bellingcat* hatten die Journalist*innen rund um Keshrau Behroz ein Fahndungsfoto von Klette in die Bilder-Suchmaschine *PimEyes* eingegeben – und stießen auf Fotos einer Berliner Capoeira-Gruppe, auf denen Klette zu sehen war. Die Suchmaschine *PimEyes* nutzt die Technik der „reverse image search“, um das gesamte Internet nach Treffern für ein eingegebenes Bild zu finden. Klette war diese Technologie offenbar nicht bekannt, als sie sich nach dem Training mit der Gruppe ablichten ließ.

Nachdem Klette festgenommen worden war, kam aus den Sicherheitsbehörden schnell die Forderung: Die Polizei sollte das Internet künftig auch biometrisch durchsuchen dürfen, so wie es „diese Podcaster“ gemacht hätten. Der Präsident des Landeskriminalamts Niedersachsen gab zu Protokoll: „Es ist schwer zu vermitteln, dass Softwareanwendungen quasi von jedermann auf dem Sofa genutzt werden dürfen, die Polizei diese bei Fahndung nach schwersten Gewalttätern jedoch nicht zum Einsatz bringen darf.“ Und die Exekutive griff das auf. So bereitete das Bundesministerium des Innern (BMI) im Sommer einen Gesetzentwurf vor, um dem Bundeskriminalamt (BKA) mit der Befugnis eines „biometrischen Internetabgleichs“ auszustatten. Die Stimme und das Gesicht einer verdächtigen Person sollte die Polizei mit dem gesamten Internet auf biometrische Treffer auf Bildern, Videos oder Audioaufnahmen absuchen dürfen.

Zweites Beispiel: Im Sommer 2024 kam es in Mannheim während einer politischen Kundgebung und in Solingen während der 650-Jahr-Feier der Stadt zu Messerangriffen im öffentlichen Raum. Viele unschuldige Menschen kamen ums Leben. Kurz vor den Landtagswahlen in Thüringen, Brandenburg und Sachsen im September 2024 kochte die Forderung hoch, dass die Politik endlich entschieden reagieren müsste. Die Regierung Scholz versuchte, mit dem sogenannten Sicherheitspaket – das die Ministerien im Eilverfahren verhandelt und ausformuliert hatten – schnell zu reagieren. In dem komplexen Regelwerk fanden sich neben einer Verschärfung des Waffen- und Migrationsrechts auch neue digitale Befugnisse für die Polizei wieder. Eine ganze Reihe von Behörden sollte die – im BMI bereits als Reaktion auf die Festnahme Daniela Klettes vorbereitete – Erlaubnis bekommen, mit biometrischen Merkmalen (Gesicht oder Stimme) im Internet nach Verdächtigen zu suchen: das Bundeskriminalamt (BKA) und die Bundespolizei zur Gefahrenabwehr, die Polizeibehörden bei der Ermittlung gegen Straftäter und die Migrationsbehörden, um die Identität eingereister Asylbewerber*innen ohne Ausweisdokumente festzustellen. Die Befugnisse landeten im Sicherheitspaket, obwohl die Täter in den genannten Fällen nach den Taten unmittelbar identifiziert und gefasst werden konnten, ein biometrischer Abgleich die Gewalttaten also gar nicht verhindert hätte. In dem Sicherheitspaket fand sich auch eine Befugnis für das BKA, polizeiliche Datenbanken mit einer „automatisierten Datenanalyse“ zu durchsuchen und mit den Daten eine künstliche Intelligenz durch private Unternehmen trainieren zu lassen.

Ein breites Bündnis zivilgesellschaftlicher Organisationen kritisierte die Entwürfe als „Überwachungspaket“, „blinden Aktionismus“ und Schritt hin zu einer „biometrischen Rundum-Überwachung“. Sie hielten die Maßnahme für einen offenen Verfassungsbruch, einen offensichtlich unverhältnismäßigen Eingriff in digitale Grundrechte und einen Verstoß gegen die Verbote im Anfang 2024 verabschiedeten *Gesetz über künstliche Intelligenz der Europäischen Union*. Auf der anderen Seite forderten die Sicherheitsbehörden und die CDU/CSU-Fraktion noch schärfere Maßnahmen.

Die Beispiele zeigen: Oftmals entsteht nach Anschlägen oder spektakulären Festnahmen der Eindruck, dass wir uns als Gesellschaft im Grunde zwischen Freiheit oder Sicherheit entscheiden müssen. Entweder geben wir den Sicherheitsbehörden alle Befugnisse und alle

technischen Überwachungswerkzeuge – oder wir lassen potenzielle Opfer von Straftaten im Regen stehen.

Ist Sicherheit um jeden Preis wünschenswert?

Sicherheit um jeden Preis ist aber keine Maxime eines liberalen Rechtsstaats, sondern eher Kennzeichen totalitärer Regime. Unter dem Deckmantel eines „starken" Staats, der alles überwacht, um abweichendes oder strafbares Verhalten zu unterbinden, stirbt allmählich die Freiheit. Ein Staat, der seinen (mit Waffengewalt ausgestatteten) Polizeibehörden alle Befugnisse überträgt, die überhaupt vorstellbar sind, gleitet – das zeigt die Geschichte – unweigerlich in einen autoritären Überwachungsstaat ab.

Gerade in Deutschland steht uns das Beispiel der „Staatssicherheit" eindrücklich vor Augen: Die „Stasi" spähte alle Bereiche des sozialen Lebens von DDR-Bürger*innen aus, unterdrückte Oppositionelle, unterband kritische Meinungen und sorgte für ein gesellschaftliches Klima der Angst. Heutzutage zeigt die Volksrepublik China, wie sich eine Gesellschaft in eine digitale Diktatur entwickeln kann, in der der Staat die Bürger*innen auf Schritt und Tritt überwacht. Aber auch die Enthüllungen des US-Whistleblowers Edward Snowden haben gezeigt, dass westliche Geheimdienste ihre Macht nutzen, um in riesigem Umfang auf private Kommunikation und die Datenpools der großen IT-Konzerne zuzugreifen.

Aufgrund der historischen Erfahrungen in Deutschland stehen Sicherheit und Freiheit im Grundgesetz der Bundesrepublik Deutschland nicht im Widerspruch. Wir müssen uns nicht entscheiden, ob wir frei *oder* sicher leben wollen. Verfassungsrechtlicher Auftrag ist es vielmehr, dass der Gesetzgeber dafür sorgt, dass beide Ziele erreicht werden. Die Verfassung erkennt das Spannungsverhältnis zwischen „möglichst viel Sicherheit" und „persönlicher und kollektiver Freiheit" an – und überträgt dem Gesetzgeber und den handelnden Beamten die Verantwortung, ein ausgewogenes Verhältnis zwischen beiden zu erreichen. Polizei und Nachrichtendienste sollen Gewalttaten im öffentlichen

Raum verhindern – ohne dadurch die rote Linie einer staatlichen Totalüberwachung zu überschreiten.

Sicherheitsbehörden in Deutschland und ihre Zuständigkeiten

Die Bundesrepublik Deutschland ist ein föderaler Bundesstaat. Die 16 Bundesländer mit ihren Landtagen und Landesregierungen sind verfassungsrechtlich eigenständige Staaten, die sich unter einer gemeinsamen Verfassung (dem Grundgesetz) zu einem Gesamtstaat zusammengeschlossen haben. Der Bund hält den Gesamtstaat als Klammer zusammen: Zentrale Akteur*innen auf Bundesebene sind Bundestag und Bundesregierung. Die genaue Aufgabenteilung zwischen Gesetzgebung und Exekutive sowie zwischen Bund und Ländern ist im Grundgesetz detailliert ausbuchstabiert. In Deutschland erlässt der Bund in vielen Bereichen die Gesetze, während deren Umsetzung in der Regel den Landesbehörden obliegt. An manchen Bundesgesetzen, die Auswirkungen auf den föderalen Gesamtstaat haben, wirken die Länder im Bundesrat an der Gesetzgebung mit.

In der Sicherheitspolitik sind die Aufgaben zwischen Bund und Ländern aufgeteilt. Als Grundlogik ist zwischen Landesverteidigung, nachrichtendienstlicher Tätigkeit und Polizeiarbeit zu unterscheiden.

Landesverteidigung – äußere Sicherheit

Für die Verteidigung gegen Bedrohungen von außen, also im Bereich des Militärs, ist die Bundesebene zuständig. Die Bundeswehr untersteht allein dem Bundesministerium für Verteidigung. Ebenso der Militärische Abschirmdienst (MAD), der als Nachrichtendienst der Bundeswehr dafür sorgen soll, dass die Bundeswehr nicht von Verfassungsfeinden oder ausländischen Mächten unterwandert wird. Die Länder sind aber nicht ohne Einfluss: Über den Bundesrat sind sie in die Gesetzgebung bezüglich der Landesverteidigung eingebunden.

Auch das Militär agiert digital. Die Bundeswehr kundschaftet bei Auslandseinsätzen gegnerische Stellungen mit Drohnen aus, nutzt digitale Tools (etwa einen eigenen Messenger) bei der Organisation der Streitkräfte oder fängt digitale Kommunikation ab. Ein sehr umstrittenes Werkzeug sind sogenannte *Hackbacks*: Im Rahmen solcher offensiver Cyberabwehr könnte das Militär etwa in die Rechenzentren und digitalen Schaltzentralen anderer Länder eindringen, um diese physisch zu zerstören. IT-Expert*innen lehnen offensive Maßnahmen ab: Der Staat solle sich auf die (passive) Sicherung der eigenen Infrastruktur beschränken. Für Hackbacks gibt es derzeit keine Grundlage im nationalen oder internationalen Recht.

Polizeiliche Tätigkeit: Gefahrenabwehr und Strafverfolgung

Die Polizei hat zwei unterschiedliche Aufgaben: einerseits Gefahren zu verhindern und andererseits Straftaten effektiv zu verfolgen. Im Normalfall sind die Länder für die Organisation zuständig, aber der Bund hat auch eigene Polizeibehörden.

Strafverfolgung: Wenn zum Beispiel ein Diebstahl begangen wird, ist die Polizei für die Ermittlungen zuständig und die Staatsanwaltschaft erhebt Anklage. Beides geschieht in der Regel auf Länderebene. Die rechtlichen Grundlagen dafür sind bundesweit einheitlich geregelt: Die Strafprozessordnung (StPO) legt fest, wie die Ermittlungsbehörden vorgehen dürfen. Weil die Länder diese Regeln umsetzen, braucht es für Änderungen der StPO die Zustimmung von Bundestag **und** Bundesrat.

Gefahrenabwehr: Greift die Polizei im Vorfeld ein, um Straftaten, Schäden oder sonstige Gefahren zu verhindern, handelt sie zum Zweck der Gefahrenabwehr. Beispiele sind Auseinandersetzungen zwischen verfeindeten Fangruppen bei Fußballspielen; die Beseitigung von Gefahrenquellen (in Zusammenarbeit mit der Feuerwehr oder dem Katastrophenschutz); oder die Unterstützung von verletzlichen Menschen. Hier greift die Polizei nicht nach einem Gesetzesbruch ein, sondern schützt vor konkreten Risiken für die öffentliche Sicherheit.

Je nachdem, ob Straftaten aufgeklärt oder Gefahren verhindert werden sollen, agiert die Polizei also in unterschiedlichen Rollen. In den allermeisten Fällen sind dafür die Bundesländer zuständig. Die Staatsanwaltschaften und die Polizeibehörden sind den Innenministerien der Länder unterstellt und handeln nach deren Weisungen. Die Landtage entscheiden eigenständig über ihre jeweiligen Polizeigesetze. Das bedeutet, dass die Polizeibehörden in Bayern oder Hamburg unterschiedliche Befugnisse haben und mit jeweils eigenen Beamten agieren.

Der Bund wiederum hat mit dem Bundeskriminalamt (BKA) und der Bundespolizei eigene Polizeibehörden mit speziellen Zuständigkeitsbereichen. Die Bundespolizei ist für die Gefahrenabwehr an Flughäfen, Bahnhöfen und den Außengrenzen der Bundesrepublik zuständig. Das BKA koordiniert die Polizeiarbeit im föderalen Staat und verfügt etwa bei der Abwehr terroristischer Bedrohungen über eigene Zuständigkeiten.

Nachrichtendienstliche Tätigkeit

Ein Nachrichtendienst (umgangssprachlich auch Geheimdienst genannt) ist eine staatliche Stelle, die Informationen über sicherheitsrelevante Vorgänge sammelt, auswertet und an politische Entscheidungsträger weitergibt – oft verdeckt. Ziel ist es, Gefahren für die innere oder äußere Sicherheit frühzeitig zu erkennen.

Nachrichtendienste verfügen – anders als die Polizei – über keine „repressiven Befugnisse“. Sprich: Sie dürfen nur Informationen beschaffen und auswerten – um sie dann an andere Behörden weiterzugeben oder zu veröffentlichen (zum Beispiel in den jährlichen Verfassungsschutzberichten). Sie dürfen jedoch keine Personen festnehmen oder Waffengewalt einsetzen, um beispielsweise ausländische Sabotageakte zu verhindern. Stößt ein Nachrichtendienst auf kriminelle Aktivitäten, muss er den Fall der Polizei übergeben. Nach dem sogenannten Trennungsgebot dürfen Polizeibehörden und Nachrichtendienste standardmäßig keine Informationen austauschen oder gemeinsame Ermittlungen führen.

Deutschland hat einen Auslandsnachrichtendienst und 17 Inlandsnachrichtendienste. Der Bundesnachrichtendienst ist dafür zuständig, im Ausland Informationen zu beschaffen und die deutsche Außenpolitik zu unterstützen. Innerhalb der deutschen Grenzen agiert das Bundesamt für Verfassungsschutz.

Für die Arbeit des *Auslandsgeheimdienst BND* ist allein der Bund

verantwortlich. Der BND darf nur außerhalb der deutschen Landesgrenzen tätig werden und sammelt dort Informationen über die politische Lage, die er dem Bundeskanzleramt zur Verfügung stellt. Im Gegensatz zu „normalen“ Diplomaten agieren die Agent*innen des BND im Geheimen. Der BND kann beispielsweise private Kommunikation ausländischer Personen abfangen, den Internetverkehr analysieren (strategische Fernmeldeaufklärung) oder Menschen heimlich überwachen. Wenn der BND heimlich Daten über Personen sammelt, greift er in ihre Grundrechte ein. Die verfassungsrechtliche Herausforderung besteht darin, dass er einerseits im Geheimen agiert, andererseits aber rechtsstaatlichen Vorgaben folgen muss. Bevor der BND grundrechtsintensive Maßnahmen durchführen darf – etwa die Telekommunikation überwachen oder einzelne Personen observieren – muss er sie deshalb speziellen, gerichtsähnlichen Gremien (etwa der G10-Kommission) zur Genehmigung vorlegen oder jedenfalls nachträglich über die Details der Durchführung informieren.

Der Geheimdienst im Inland heißt *Verfassungsschutz*. Als Inlandsgeheimdienste sind sowohl das *Bundesamt für Verfassungsschutz* als auch die *Landesämter für Verfassungsschutz* zuständig. Sie sammeln Informationen über Personen oder Gruppen, die verfassungsfeindliche Ziele verfolgen und sollen die Spionage durch ausländische Geheimdienste auf deutschem Territorium verhindern. So kann das Bundesamt für Verfassungsschutz eine politische Partei aufgrund gesammelter Erkenntnisse als „gesichert rechtsextremistische Bestrebung“ einstufen.

Um eine demokratische Kontrolle der Nachrichtendienste zu gewährleisten, kontrolliert der Bundestag im *Parlamentarischen Kontrollgremium* ihre Arbeit. Für die Landesämter für Verfassungsschutz gibt es vergleichbare Ausschüsse in den Landtagen.

Wann ist ein Eingriff in die Grundrechte zulässig?

In einem liberalen Rechtsstaat ist das Verhältnis zwischen Sicherheit und Freiheit stets eine komplexe Abwägung. Welche Art von digitaler Überwachung zulässig ist oder nicht, ist anhand konkreter Fälle, verfügbarer Technologien und einschränkender Vorschriften zu bewerten. Es ist deshalb nicht verwunderlich, dass sich das Bundesverfassungsgericht in zahlreichen Urteilen damit auseinandergesetzt hat, ob bestimmte Befugnisse, die der Gesetzgeber eingeführt hat oder die die Sicherheitsbehörden nutzen, mit dem Grundgesetz in Einklang stehen oder nicht.

Rechtsstaatlich gerechtfertigte Eingriffe in Grundrechte

Im deutschen Verfassungsrecht darf der Staat nur unter bestimmten hohen Voraussetzungen in die Grundrechte der Bürger*innen eingreifen. Der Zweck, den der Staat mit einer digitalen Überwachung verfolgt, muss so wichtig sein, dass in einer Abwägung die Grundrechte auf informationelle Selbstbestimmung (der Schutz personenbezogener Daten), die Telekommunikationsfreiheit oder die Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) zurückstehen müssen.

Ein Eingriff ist nur aufgrund eines Parlamentsgesetzes erlaubt. Das Gesetz – zum Beispiel ein Paragraf in einem Landespolizeigesetz – muss der Sicherheitsbehörde einen klaren Rahmen vorzeichnen, wie die Polizei die Maßnahme durchzuführen hat, welche Voraussetzungen dafür vorliegen müssen und wie eine (interne oder externe) Kontrolle gegen rechtswidrigen Einsatz auszusehen hat. Damit der Eingriff in die Grundrechte so gering wie möglich bleibt, also die Freiheitsrechte der Bürger*innen nur so weit wie unbedingt nötig eingeschränkt werden, muss der Gesetzgeber die negativen Auswirkungen durch rechtliche, organisatorische und technische Maßnahmen beschränken.

Typische gesetzliche Vorgaben, die einen Grundrechtseingriff abmildern können, sind etwa,

- dass ein dringender Tatverdacht vorliegen muss – vor allem bei intensiven Grundrechtseingriffen – und nicht nur ein bloßer Anfangsverdacht;
- dass die Maßnahmen nur beim Verdacht für besonders schwere Straftaten (Mord, Bildung einer terroristischen Vereinigung oder Spionage) angewendet werden dürfen;
- dass vor Beginn der Maßnahme ein Gericht zustimmen muss (der sogenannte Richtervorbehalt);
- dass es effektive polizeiinterne und gerichtliche Kontrollmöglichkeiten gibt, die einen Missbrauch der Instrumente für rechtswidrige Zwecke (zum Beispiel das Ausspionieren unliebsamer Nachbarn durch Polizist*innen) verhindern;
- dass sich die überwachte Person gegen den Eingriff juristisch zur Wehr setzen und – bei heimlichen Maßnahmen jedenfalls im Nachgang – die Gerichte anrufen kann.

Herzstück einer jeden Grundrechtsprüfung ist der Grundsatz der Verhältnismäßigkeit, auch „Übermaßverbot“ genannt. Sowohl die gesetzliche Rechtsgrundlage als auch die konkrete Durchführung der digitalen Ermittlungsmaßnahme muss

- einen legitimen Zweck verfolgen (zum Beispiel den Schutz der öffentlichen Sicherheit, Verhinderung von schweren Straftaten oder Informationsbeschaffung für geheimdienstliche Aufgaben auf der Grundlage eines begründeten Verdachts),
- sie muss für diesen Zweck geeignet sein,
- es darf keine Mittel geben, die denselben Zweck grundrechtsschonender erreichen (Erforderlichkeit),
- bei der Erreichung des Zwecks in einem angemessenen Verhältnis zu dem Eingriff in Grundrechte stehen (Angemessenheit).

Wenn das Bundesverfassungsgericht ein Gesetz oder eine Einzelmaßnahme der Sicherheitsbehörden prüft, stellt es eine umfassende Abwägung zwischen den Grundrechten der betroffenen Personen und

dem Ziel, die öffentliche Sicherheit und Ordnung durch digitale Überwachung zu schützen an. Wenn eine Maßnahme die Grundrechte unverhältnismäßig beeinträchtigt, ist sie verfassungswidrig.

Instrumente der digitalen Überwachung

Überwachung im öffentlichen Raum

Der digitale Wandel hat die Überwachung auf unseren Straßen und Plätzen verändert. Früher sah Videoüberwachung so aus, dass eine Kamera ihre Bildaufnahmen an eine Zentrale schickte, in der Sicherheitspersonal das Geschehen auf Monitoren beobachtete, mögliche Gefahren erkannte und notwendige Maßnahmen einleitete. Beobachtete ein Polizist etwa den Verkauf von Drogen in einem Bahnhofsgebäude, schickte er eine Streife los, um die verdächtige Person zu kontrollieren. Mit der Zeit wurde es möglich, die Aufnahmen – erst auf Band, später auch digital – dauerhaft abzuspeichern, sodass Videoaufnahmen sich nachträglich analysieren ließen. Bund und Länder führten Rechtsgrundlagen ein, um besonders kriminalitätsgefährdete Bereiche wie Flughäfen mit Kameras zu überwachen und die Aufnahmen auszuwerten. Eine Totalüberwachung des gesamten öffentlichen Raums blieb aber stets ein verfassungsrechtliches Tabu. Mit größeren Datenträgern wurde es möglich, softwarebasierte Analysen des Bildmaterials durchzuführen – etwa näher hereinzuzoomen oder Vorgänge zu analysieren, die dem menschlichen Auge verborgen geblieben wären.

Ein weiterer Paradigmenwechsel vollzog sich mit neuen Formen des Datenabgleichs: So ist es mittlerweile technisch möglich, auf Videoaufnahmen Gesichter zu erkennen und sie mit Datenbanken abzugleichen. Die sogenannte biometrische Videoüberwachung ist mittlerweile technisch in der Lage, Passant*innen zu identifizieren, indem sie die Videos mit staatlichen Datenbanken biometrischer Passfotos oder Bildern aus polizeilichen Datenbanken abgleicht. Die Bundespolizei testete ein solches System in einem umstrittenen Modellprojekt am Bahnhof Berlin-Südkreuz.

Die verschiedenen Formen der visuellen Überwachung

Videoübertragung: Die Bildaufnahmen werden lediglich an ein Monitorsystem übertragen, aber nicht aufgezeichnet.

Videoaufzeichnung: Die Kamera zeichnet die Aufnahmen analog oder digital auf, damit sie zu einem späteren Zeitpunkt ausgewertet werden können. Die Polizei darf solche Aufnahmen in der Regel nicht ohne Anlass analysieren, sondern nur dann, wenn ein Verdacht auf Straftaten oder sonstige Gefahren besteht. Die Polizei darf auch Aufzeichnungen privater Kameras beschlagnahmen.

Biometrische Videoüberwachung: Die Videoaufnahmen werden auf biometrische Muster überprüft, um einzelne Personen zu identifizieren. Biometrische Merkmale können das Gesicht, die Stimme, aber beispielsweise auch die Art, wie ein Mensch läuft, sein.

Bei einer Identifizierung **in Echtzeit** findet der Abgleich in engem zeitlichem Zusammenhang mit der Liveaufnahme auf demselben System statt (Kameraaufnahmen und Datenbankabgleich finden mehr oder weniger gleichzeitig statt).

Eine **nachträgliche** Identifizierung bedeutet, dass eine Videoaufzeichnung im Nachgang und bei Vorliegen eines bestimmten Verdachts auf biometrische Treffer analysiert wird. Ein Beispiel ist das – rechtlich hochumstrittene – Vorgehen der Hamburger Polizei, die Videoaufnahmen von gewalttätigen Ausschreitungen am Rande des G20-Gipfels nutzen wollte, um sie mit biometrischen Datenbanken abzugleichen.

Nicht personenbezogene Videoanalyse: Videoaufnahmen lassen sich auch auswerten, ohne einzelne Personen zu identifizieren. So sind beispielsweise in Mannheim Systeme im Einsatz, die gefährliche Situationen (etwa Schlägereien oder Drogenübergaben) erkennen sollen, ohne das Gesicht der beteiligten Personen zu analysieren. Ein anderes Beispiel ist das Erkennen von unbeaufsichtigten Gepäckstücken an Bahnhöfen oder Flughäfen.

Kennzeichenerfassung: Eine Form der Überwachung im öffentlichen Raum findet auf Deutschlands Straßen statt. Zunächst wurden die Kennzeichen von Lastwagen gescannt, um zu überprüfen, dass sie die Lkw-Maut bezahlt haben. Seitdem dreht sich die Diskussion darum, ob bei der Suche nach verdächtigen Personen alle Autokennzeichen auf Autobahnen erfasst und mit den gesuchten Nummernschildern abgeglichen werden sollten.

Überwachung von Kommunikation – mithören, mitlesen, Daten absaugen

Früher überwachte der Staat die Telekommunikation über Festnetzkabel und Briefe auf dem Postweg. Da der Staat die Kontrolle über die Post und Telefonkabel innehatte, konnten Polizei und Nachrichtendienste mit überschaubarem Aufwand Briefe oder Anrufe abfangen. Artikel 10 des Grundgesetzes wurde 1949 auf die damalige Realität maßgeschneidert: „Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich." Im analogen Zeitalter wurden die Anrufe oder Briefe einzelner Menschen nirgendwo strukturell archiviert, allenfalls durch die kommunizierenden Personen selbst. Ein nachträglicher Zugriff auf Anrufe oder versendete Briefe war schon technisch nicht möglich.

Heute nutzen wir kaum noch Festnetztelefonie oder Briefpost, sondern Mobilfunk, SMS, Messenger, Video- und Sprachanrufe. Bei all diesen Formen der Kommunikation findet eine Form der Speicherung statt – sei es im E-Mail-Postfach, auf Servern der Anbieter, in Zwischenspeichern der Mobilfunkanbieter oder auf unseren Smartphones. An all diesen Schnittstellen kann Kommunikation überwacht werden. Im digitalen Zeitalter werden zudem viel mehr private Kommunikationsdaten ausgetauscht – was früher im persönlichen Gespräch passierte, erfolgt heute oft digital. Das Risiko, dass ein staatlicher Zugriff auf unsere private Kommunikation zu einer Massenüberwachung führen kann, ist also um einiges höher als noch Mitte des. 20. Jahrhunderts. Zugleich befindet sich die digitale Infrastruktur heute nicht mehr im Besitz von Staatsbetrieben wie der Deutschen Bundespost, sondern liegt größtenteils in der Hand von privaten Unternehmen: von Telekom, Vodafone über Whatsapp, Instagram oder Tiktok bis hin zu Amazon, Apple oder dem Internetknoten DE-CIX. Wenn Sicherheitsbehörden digitale Kommunikation abhören wollen, müssen sie einzelne Daten oder Zugänge bei den Unternehmen anfragen oder gesetzliche Verpflichtungen schaffen, dass dies geschieht.

Gesetzlich erlaubt war lange Zeit nur die sogenannte *Telekommunikationsüberwachung* (TKÜ), bei der Sicherheitsbehörden einzelne Telefongespräche mithören und aufzeichnen durften. Sie nutzten die gesetzliche Erlaubnis später nicht nur für kabelgebundene Festnetzanrufe, sondern auch für Handytelefonate und SMS, die über Mobilfunkmasten versendet werden. Ab den 2000er-Jahren, als mehr und mehr

Menschen das Internet aktiv zu nutzen begannen, wollten Sicherheitsbehörden dann auch Chatnachrichten, Anrufe über Skype oder Whatsapp oder ganze E-Mails heimlich mitlesen. Damit sensible Daten nicht einfach massenhaft beim Staat landen, weil dieser sie auf dem Weg abfängt, etablierte sich mit der Zeit die Technologie der kryptografischen Verschlüsselung. Chatnachrichten über Messenger oder verschlüsselte E-Mails konnten infolgedessen nicht mehr auf der Strecke zwischen den Kommunikationspartnern abgefangen und direkt gelesen werden, da sie jetzt auf dem Transportweg verschlüsselt wurden (die sogenannte Ende-zu-Ende-Verschlüsselung). Dadurch wurde der direkte Zugriff auf das private Endgerät zur einzigen zuverlässigen Methode, an private Kommunikation heranzukommen.

Das Bundesverfassungsgericht setzte der Ausweitung der TKÜ durch die Sicherheitsbehörden in seiner Rechtsprechung Grenzen: Neue Formen der Kommunikationsüberwachung seien von der gesetzlichen Befugnis nicht mehr gedeckt – und bräuchten eine eigene gesetzliche Rechtsgrundlage. Allmählich etablierte sich folgende Systematik:

Formen der Kommunikationsüberwachung

Bei einer **Online-Durchsuchung** hackt sich die Polizei auf das digitale Endgerät einer verdächtigen Person und hat dadurch Vollzugriff auf das gesamte System. Das Bundesverfassungsgericht verglich die Maßnahme mit einer Hausdurchsuchung und hob das neue Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) aus der Taufe. In Paragraf 100b StPO lässt der Gesetzgeber die Maßnahme nur unter sehr hohen Voraussetzungen zu.

Bei einer **Quellen-Telekommunikationsüberwachung** verschafft sich die Polizei zwar auch Zugriff auf ein Endgerät, darf aber nur die „laufende Kommunikation“ auf eigene Systeme umleiten. Weil kein Vollzugriff auf ein IT-Gerät stattfindet, sind verfassungsrechtlich geringere Hürden anzulegen. Bis heute ist jedoch rechtlich und technisch umstritten, wie es zuverlässig möglich ist, die Vorgabe „nur laufende Kommunikation“ einzuhalten, ohne auch auf sonstige Daten auf dem Gerät zuzugreifen. In der Öffentlichkeit bekannt wurde unter anderem die Spyware „Pegasus“ – ein Produkt der israelischen Firma *NSO Group* – mit der Staaten weltweit Zugriff auf Endgeräte (vor allem Mobiltelefone) erhalten konnten und Journalist*innen oder Oppositionelle abhörten. Die digitale Zivilgesellschaft und Bürgerrechtlicher*innen kritisierten den Einsatz von „Staatstrojanern“ als unberechenbaren Eingriff in die Privatsphäre und

Gefahr für die IT-Sicherheit. Denn um auf Endgeräte Zugriff bekommen zu können, brauchen Sicherheitsbehörden technische Schwachstellen (sogenannte Exploits), die, wenn sie offen bleiben, auch von Kriminellen oder ausländischen Geheimdiensten verwendet werden können.

Das **Client-Side-Scanning** (auch bekannt als **„Chatkontrolle“**) geht noch einen Schritt weiter. Mit der Maßnahme würden Anbieter von Kommunikationsdiensten (zum Beispiel Messenger wie Whatsapp oder Signal) dazu verpflichtet, den Inhalt von Nachrichten präventiv zu prüfen, um sie auf kriminelle Inhalte zu prüfen oder sie direkt an Sicherheitsbehörden weiterzuleiten – und zwar, noch bevor der Verschlüsselungsvorgang einsetzt. Das Argument der Sicherheitsbehörden: Da ein Großteil der digitalen Kommunikation mittlerweile Ende-zu-Ende-verschlüsselt stattfindet und eine Quellen-TKÜ gegen einzelne Personen sehr aufwendig ist, sollte es künftig möglich sein, die Anbieter zu verpflichten, Daten vor dem Verschlüsseln mitzuschneiden. Kritiker sprachen von einem Angriff auf die IT-Sicherheit der gesamten Bevölkerung und der Gefahr einer anlasslosen Massenüberwachung, da der Staat so eine Hintertür in fast alle private Kommunikation erlangen könne und das Vertrauen in sichere Kommunikation verloren ginge. Auf EU-Ebene gab es mehrere Initiativen, um eine Chatkontrolle einzuführen, bislang gibt es jedoch – auch in Deutschland – keine gesetzliche Befugnis dafür.

Überwachung des Online-Verhaltens

Neben der Überwachung privater Kommunikation gibt es weitere Formen der Analyse unseres Online-Verhaltens. Sie setzen an unterschiedlichen Stellen an.

Bei der *Vorratsdatenspeicherung* (VDS) greift die Polizei auf Daten zu, die bei der Nutzung von Mobilfunk oder Internet anfallen. Das ist etwa die IP-Adresse von digitalen Endgeräten, die Port-Nummer von Routern oder die Standortdaten unserer Smartphones. Eine gesetzliche Befugnis zur Vorratsdatenspeicherung würde die Telekommunikationsanbieter dazu verpflichten, diese Daten von allen Bürger*innen für einen bestimmten Zeitraum zu speichern, damit die Polizei auf diese Datenpools nachträglich unter bestimmten Voraussetzungen zugreifen darf, um Straftaten aufzuklären. Das Bundesverfassungsgericht und der Europäische Gerichtshof haben sich damit in verschiedenen Gesetzen umfangreich beschäftigt und insbesondere moniert, dass bei

der VDS die Daten aller Bürger*innen anlasslos gespeichert werden, um gegen nur sehr wenige vorgehen zu können. Bislang gibt es keine Form der VDS, die vor höchsten Gerichten Bestand hatte. Als grundrechtsschonendere Alternative wird das Konzept *Quick Freeze* diskutiert: Hier werden die IP-Adressen oder Standortdaten von bestimmten Personen bei den Firmen „eingefroren", wenn ein Verdacht auf eine Straftat bekannt wird. Die Gefahr einer anlasslosen Massenüberwachung besteht dann nicht.

Bei einem *biometrischen Internetabgleich* suchen die Sicherheitsbehörden das Internet nach bestimmten Personen ab, um sie auf Fotos, Videos oder Audioaufnahmen zu identifizieren. Eine Person, die unter falscher Identität nach Deutschland einreist, könnte so etwa auf Videos der Taliban als potenzieller Attentäter erkannt werden. Aber auch peinliche Partybilder, die Babybilder von Momfluencern oder Bilder von Touristen, die nur zufällig im Hintergrund zu sehen sind, könnten so in die Hände der Sicherheitsbehörden landen. Die europäische Verordnung für künstliche Intelligenz verbietet solche Systeme in Art. 5 Buchstabe e.

Damit wir per Handy erreichbar sind, stehen unsere digitalen Endgeräte in ständigem Kontakt zu Mobilfunkmasten. Wir sind also stets in die nächstgelegene Funkzelle eingeloggt. Bei einer *Funkzellenabfrage* fragt die Polizei bei Mobilfunkanbietern ab, wer zu einem bestimmten Zeitpunkt mit dem Handy in einer bestimmten Funkzelle eingeloggt war. Die Abfrage gibt der Polizei einen Überblick, welche Mobilfunknummern sich im Radius der Funkzelle befunden haben. Durch eine Kombination mehrerer Funkzellenabfragen lässt sich nachvollziehen, wie sich eine einzelne Person beziehungsweise ein einzelnes Handy in einer Stadt bewegt hat. Solche Bewegungsprofile sind ein intensiver Eingriff in die Grundrechte, da sie dem Staat die Möglichkeit geben, heimlich zu beobachten, wo wir uns aufhalten und gegebenenfalls auch, wen wir wo treffen. Eine spezielle Technologie sind sogenannte *IMSI-Catcher* – mit ihnen kann die Polizei eine Funkzelle simulieren und etwa alle Handynummern der Teilnehmer*innen einer bestimmten Demonstration abfangen.

Klarnamenpflicht: Es kommt immer wieder zu öffentlichen Debatten darüber, ob es eine Pflicht geben sollte, dass sich jeder Mensch im Internet stets eindeutig zu erkennen gibt. Damit wäre man auf sozialen Netzwerken, in Foren, aber auch beim Lesen von Online-Publikationen immer identifizierbar. Jeder Klick würde aufgezeichnet und einer Person individuell zugeordnet. Technisch umsetzen ließe sich so eine Maßnahme, indem der Internetanbieter weitergibt, wer hinter der IP-Adresse, dem Router, dem Endgerät steckt – oder indem Menschen dazu verpflichtet werden, sich bei Facebook, X oder Instagram mit einem Ausweis zu identifizieren. Durch eine direkte Zuordnung von Online-Verhalten zur handelnden Person ließen sich strafbare und illegale Aktivitäten womöglich häufiger und leichter aufklären. In einer hochdigitalisierten Gesellschaft könnten Staat und Unternehmen dadurch jeden unserer Klicks lückenlos nachverfolgen. Es entstünde ein „gläserner Bürger" im digitalen Raum. Es wäre das Ende der anonymen Nutzbarkeit des Internets und ein enormer Freiheitsverlust, der unter dem Grundgesetz nicht rechtfertigbar wäre.

Eine mildere Maßnahme ist die sogenannte *Altersverifikation*. Der Vorschlag stammt vorwiegend aus dem Kinder- und Jugendmedienschutz. Ähnlich wie bei der Einteilung von Filmen oder Spielen in Altersgruppen (freigegeben ab 6, 12, 16 oder 18 Jahren) stünden dann Internetangebote nur für Personen zur Verfügung, die ein bestimmtes Mindestalter nachweisen können. So setzen sich die Landesmedienanstalten dafür ein, dass Pornoseiten im Netz – bei denen bisher die Altersabfrage leicht umgangen werden kann – schärfere Formen der Altersverifikation implementieren. Anders als in einer Videothek, bei der man einen Ausweis vorlegen konnte, greifen digitale Formen der Altersverifikation aber viel stärker in Grundrechte ein. Es bestünde die Gefahr, dass Staat oder Unternehmen das Online-Verhalten Einzelner umfangreich analysieren und daraus Nutzerprofile erstellen könnten. Was zum Schutz vor problematischen Inhalten im Netz konzipiert war, könnte in eine Form der Massenüberwachung münden. Eine „persönlichkeitsfeindliche Registrierung und Katalogisierung des Einzelnen" hat das BVerfG mehrfach als verfassungsrechtliche rote Linie markiert.

Zusammenführen und Analyse von Nutzerdaten

Wenn künstliche Intelligenz große Datenmengen auf Muster und Zusammenhänge untersuchen kann, weckt dies auch Begehrlichkeiten bei den Sicherheitsbehörden. Die Debatte ist in

Deutschland eng mit der Firma *Palantir* des US-Tech-Milliardärs Peter Thiel und seiner Software „Gotham“ verflochten. Einige Bundesländer haben bereits bei Palantir eingekauft und die Analyseplattform VeRA (Verfahrensübergreifendes Recherche- und Analysesystem) im Einsatz. Mit ihrer Hilfe lassen sich polizeiliche Daten, die in unterschiedlichen Formaten auf verschiedenen Servern vorliegen, schnell zusammenführen und auf Muster und Zusammenhänge durchsuchen.

Dabei kann es vorkommen, dass Daten, die in einem Strafverfahren vor Jahren angefallen sind, auf einmal in einem komplett neuen Kontext auftauchen. Doch die Polizei darf ihre Daten nicht einfach beliebig weiterverwenden. In einer sogenannten zweckändernden Verarbeitung persönlicher Daten kann vielmehr ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung liegen. Wer eine Straftat bei der Polizei angezeigt hat, muss nicht damit rechnen, dass private Details daraus herangezogen werden, um einen Anfangsverdacht zu begründen. Eine Zeugenaussage vor Gericht darf nicht ohne Weiteres in ganz andere Ermittlungen einfließen.

So hat das Bundesverfassungsgericht entschieden, dass die Daten von Opfern einer Straftat nicht automatisch in VeRA einfließen dürfen. Für die verfassungsrechtliche Bewertung ist aber nicht nur die Frage wichtig, wie das Gesetz konkret die Fragen regelt, wer auf welche Daten unter welchen Voraussetzungen zu welchem Zweck in welcher Detailtiefe zugreifen darf. Wichtig ist auch, wie sicher die Daten in der Software einer Privatfirma sind, also ob sie nicht etwa durch Hintertüren in die USA abfließen oder Hackern in die Hände fallen können. Zu den Details einer automatisierten Datenanalyse der Polizei hat das Bundesverfassungsgericht bereits mehrere detaillierte Urteile erlassen und den Bundesländern Hessen, Bayern und NRW Grenzen gezogen – und die „Gesellschaft für Freiheitsrechte“ habe bereits neue Verfahren gegen die Gesetze angekündigt.

Ausblick: Die Debatte zwischen Freiheit und Sicherheit geht weiter

Das Verhältnis zwischen Freiheit und Sicherheit im Rechtsstaat wird uns als Gesellschaft in Zukunft weiter beschäftigen. Die Grundrechte schützen die Freiheit der Bürger*innen und gesellschaftliche Entfaltungsräume ohne staatliche Beobachtung – die Sicherheitsbehörden sollen die öffentliche Sicherheit und Ordnung schützen, damit ein freies Leben überhaupt möglich ist. Doch das optimale Verhältnis aus individuellen und kollektiven Freiräumen auf der einen und rechtsstaatlichen Befugnissen der Sicherheitsbehörden auf der anderen Seite ist und bleibt Gegenstand einer intensiven verfassungsrechtlichen und gesellschaftlichen Debatte.

Gerade in Zeiten, in denen sich die staatliche Macht der Sicherheitsbehörden und wirtschaftlich-technologische Macht einzelner IT-Konzerne international immer weiter verschränken, droht sich eine „digitale Autokratie“ herauszubilden, in der Kontrolle und Profit wichtiger sind als die individuelle, kollektive und demokratische Selbstbestimmung. Wenn unsere gesamte Persönlichkeit digital vermessen ist, unsere Geheimnisse nicht mehr geheim sind, der öffentliche und digitale Raum weitläufig überwacht werden, wäre jedenfalls das Ende eines demokratischen Rechtsstaats erreicht. Bis dahin gilt es bei jeder neuen digitalen Ermittlungsbefugnis, die öffentlich diskutiert wird, genau hinzuschauen, ob sie verhältnismäßig und für eine liberale Gesellschaft zumutbar ist.

Prof. Dr. Dennis-Kenji Kipker ist Research Director am cyberintelligence.institute in Frankfurt a. M. Er forscht zu Themen an der Schnittstelle von Recht und Technik in der Cybersicherheit sowie zu digitaler Resilienz im Kontext globaler Krisen und berät Bundesregierung und Europäische Kommission. Ehrenamtlich beteiligt sich Kipker im Vorstand der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) in Berlin sowie am World Justice Project.

Michael Kolain ist Senior Fellow am cyberintelligence.institute, Experte für Digitalpolitik am Zentrum Digitalrechte und Demokratie, Research Associate am Centre for Ethics in Technology an der TUHH und im Vorstand der Robotics and AI Law Society. Als Volljurist arbeitet er an der Schnittstelle zwischen Gesetzgebung, interdisziplinärer Forschung und der Entwicklung digitaler Technologien.

Philipp Ehmann

Träumen elektrische Schafe von Robotern?

Die Wechselwirkung von künstlicher Intelligenz, Algorithmen und Grundrechten – Versuch einer Annäherung

Künstliche Intelligenz, Algorithmen, Big Data, maschinelles Lernen und neuronale Netzwerke – wovon reden wir eigentlich?

Künstliche Intelligenz (KI) ist Teil unseres Alltags – als automatische Übersetzungen, Bilderkennung, Textgenerator oder digitale Bürohilfskraft. Laut dem Branchendienst *Similarweb* war allein ChatGPT im Mai 2025 auf Nummer 5 der meistbesuchten Websites weltweit. Viel von dem, was Gesetzgeber und Aufsichtsbehörden als KI definieren, findet sich in Bürosoftware als Rechtschreibprogramm und Übersetzungstool, auf Smartphones als App, die verrät, welcher Song gerade im Radio läuft, oder auf dem heimischen PC in Bildbearbeitungsprogrammen. Suchmaschinen, die auf Anfrage Informationen aus dem World Wide Web auflisten, sind aus unserem Alltag nicht mehr wegzudenken. Auch im geschäftlichen Kontext gibt es zahllose Systeme, die mithilfe von Algorithmen Daten analysieren: Ausbreitung von Waldbränden, Austrocknung von Böden, Auswertung von Verträgen, Anfragen im Kundendienst – in all diesen Bereichen kommt künstliche Intelligenz zum Einsatz.

Dabei handelt es sich meist um sogenannte „schwache KI“: Systeme, die auf bestimmte Aufgaben spezialisiert sind – oft beeindruckend leistungsfähig, aber dennoch eng begrenzt in der Funktion. Daneben sprechen Expert*innen auch von AGI – „Artificial General Intelligence“. Diese unterscheidet sich von der „schwachen KI“ grundlegend. Sie kann flexibel denken, lernen, Probleme lösen und sich auf neue Situationen einstellen kann – also eine Art universelle Intelligenz. Solche Systeme gibt es bisher nicht, auch wenn Debatten darüber, wie weit wir davon entfernt sind, sehr unterschiedlich geführt werden.

Aktuell stehen wir an einem Punkt, an dem KI zwar keine eigene Absicht oder Bewusstheit hat, aber dennoch große Auswirkungen auf Kommunikation, Bildung, Politik und Gesellschaft entfaltet – gerade weil ihre Ergebnisse zunehmend plausibel und menschenähnlich

erscheinen. Die verschiedenen KI-Dienste verwenden und verarbeiten für ihre Funktionen Daten, aber es gibt dabei Unterschiede, wie sie diese Daten verarbeiten, welche Daten sie verarbeiten, und zu welchem Zweck diese Daten verwendet werden.

Zudem haben digitale Dienste und Apps kurze Innovationszyklen: Ständig erscheinen neue Versionen und Updates. Für Nutzende ist auf den ersten Blick nicht ersichtlich, welche Funktionen sich hinter den jeweiligen Diensten und Systemen verbergen. Dies erschwert die Einschätzung, ob und welche Grundrechte durch die jeweiligen Dienste betroffen sind. Gleichzeitig verändern sich durch die starke globale Vernetzung und Digitalisierung von Wissenschaft, Wirtschaft und Gesellschaft die Dienste, die Menschen zur Verfügung stehen. Daraus folgen weitere Fragen, zum Beispiel nach dem Ursprung und Zweck dieser Dienste. Fast alle uns bekannten sozialen Netzwerke, aber auch alle gängigen KI-Systeme, die den Nutzenden zur Verfügung stehen, haben ihren Hauptsitz entweder in den USA oder in der Volksrepublik China mit jeweils eigenen Konzepten von Privatsphäre und Rechtsordnung.

Das führt zur verstärkten Debatte darüber, wie sich künstliche Intelligenz und deren Einsatz auf die Grundrechte von Menschen auswirkt. Betrachtet man die Diskussionen über künstliche Intelligenz und Grundrechte, erkennt man bestimmte wiederkehrende Muster.

Künstliche Intelligenz und das Recht auf körperliche Unversehrtheit

Schon in Science-Fiction-Filmen der 1980er-Jahre wie „War Games“ oder „Terminator“ taucht die Sorge auf, dass Maschinen, die auf welche Art auch immer von künstlicher Intelligenz gesteuert werden, selbstständig Menschen töten könnten. Auch in der Philosophie und Wissenschaft wurde dieses Szenario diskutiert: Der schwedische Philosoph Nick Bostrom warnt in seinem Buch „Superintelligence“ (2014) vor einer Zukunft, in der eine künstliche Intelligenz außer Kontrolle geraten und die Menschheit

gefährden könnte. Das *Center for AI Safety* in den USA, dem unter anderem Forscher von *Google DeepMind* und *Anthropic* angehören, spricht von einem „extinction-level risk“ durch unkontrollierte KI-Systeme und fordert deshalb strikte internationale Regulierungen.

Betrachtet man jedoch heute den Einsatz von künstlicher Intelligenz im Militär, etwa bei der automatisierten Zielerkennung, zeigt sich, dass Gefahren meist nicht von der KI selbst ausgehen, sondern von zuvor von Menschen getroffenen Entscheidungen, zum Beispiel welche Ziele algorithmisch priorisiert werden. Künstliche Intelligenz, die von sich aus Menschen angreift, bleibt Science-Fiction.

Fremdbestimmung durch künstliche Intelligenz

Was geschieht, wenn künstliche Intelligenz oder algorithmische Systeme Entscheidungen treffen, die uns die Möglichkeit nehmen, diese Entscheidungen selbst zu treffen? Unser Grundrecht auf freie Meinungsäußerung und Informationsfreiheit gemäß Artikel 11 der EU-Grundrechtecharta und auch unser Grundrecht auf freie Entfaltung der Persönlichkeit gemäß Artikel 2 des Grundgesetzes könnten hiervon berührt sein. Diese Frage stellt sich einerseits vor dem Hintergrund der Diskussion um Deepfakes – also mittels künstlicher Intelligenz erstellter Videos oder Bilder – und „Dark Patterns“-Manipulationen – täuschend gestaltete Nutzeroberflächen auf Webseiten, die das Verhalten der Nutzenden in eine bestimmte Richtung lenken wollen – und andererseits durch den Einsatz von Systemen künstlicher Intelligenz zum Beispiel in der Strafverfolgung oder im Finanzwesen.

Auch wenn die Folgen in beiden Fällen recht eng beieinanderliegen, sind sie in ihrer grundsätzlichen Ausrichtung doch sehr unterschiedlich. Hinter dem Einsatz von Deepfakes oder Dark Patterns stehen menschliche Akteur*innen, die die Nutzenden in die Irre führen oder beeinflussen wollen. Auch Betrugsdelikte können mithilfe von Deepfakes begangen werden. Schon jetzt gibt es Leitfäden zum Umgang mit Deepfakes beispielsweise vom *Bundesamt für Sicherheit in der*

Informationstechnik, die auf die besonders relevanten Probleme eingehen. Bei Dark Patterns wird ebenfalls der Versuch unternommen, bei Personen ein bestimmtes Verhalten zu erzeugen. Dabei geht es oft darum, sie zum Kauf bestimmter Produkte oder Dienstleistungen zu animieren. Die Art und Weise, wie hier Nutzende beeinflusst werden, ist aber anders als bei Deepfakes deutlich komplexer. Am bekanntesten sind bei Dark Patterns derzeit Lockvogelangebote und verwirrend gestaltete Einwilligungsformulare zur Einwilligung in die Datenverarbeitung.

Diesen Phänomenen ist gemein, dass sie in der europäischen Verordnung zur künstlichen Intelligenz durch Transparenzvorgaben geregelt sind. Ihre Verwendung ist verboten. Die Justiz hat erste Urteile zum Einsatz von Deepfakes gefällt. Wie sich diese Rechtsprechung entwickelt, welchen Schutz sie Nutzenden bietet, bleibt abzuwarten. Es ist jedoch anzunehmen, dass von seriösen Anbietern keine größere Gefahr ausgeht, da die Sanktionen durch die europäische Verordnung sehr hoch sind.

Komplexer verhält es sich mit algorithmischen Entscheidungen künstlicher Intelligenz, die sich auf unser privates, gesellschaftliches oder wirtschaftliches Leben auswirken. Hier sind neben den zuvor genannten Gesetzen auch das Recht auf Achtung der Privatsphäre, wie sie in den Artikeln 7 und 9 der EU-Grundrechtecharta, sowie die Artikel 9, 11 und 12 des Grundgesetzes zur Freizügigkeit und zur freien Berufswahl benannt werden. Die Rechtslage ist seit 2016 durch die europäische Datenschutz-Grundverordnung klar. In der Praxis zeigt sich jedoch, dass die Bestimmungen der Datenschutz-Grundverordnung weiterer Auslegung bedürfen – zum Beispiel bei der Frage, ab wann eine Entscheidung automatisiert erfolgt, beziehungsweise ab wann davon auszugehen ist, dass die Entscheidung von einem Menschen und nicht vorrangig von künstlicher Intelligenz getroffen wurde.

Zuletzt beschäftigte diese Frage den Europäischen Gerichtshof im Rahmen der Diskussion um den Einsatz automatisierter Bewertungsverfahren bei der Kreditvergabe. Zwar mag der Fall eines einzelnen verweigerten Kredits trivial wirken, jedoch kann sich dahinter eine systematische Diskriminierung von Personen oder Personengruppen verbergen, zum Beispiel, wenn entsprechende Kreditwürdigkeitsbewertungen auf Grundlage von Wohnort oder Nationalität verweigert werden. Dies würde in der dargestellten Form einen Verstoß gegen Artikel 3 des Grundgesetzes und des dort verankerten Diskriminierungsverbots bedeuten.

Inwieweit Entscheidungen von künstlicher Intelligenz oder algorithmischen Systemen uns in unserem Alltag einschränken, lässt sich nicht allgemein beantworten. Die verschiedenen Systeme künstlicher Intelligenz müssen fortlaufend überprüft werden, um mögliche Diskriminierung auszuräumen. Die Verordnung zur künstlichen Intelligenz schreibt dies auch vor.

KI-Systeme verwenden nicht nur einen Faktor, auf den sie ihre Entscheidung stützen. Es muss daher genau analysiert werden, ob die KI diskriminierend arbeitet oder ob die Entscheidung objektiv nachvollziehbar ist. Offen bleibt indes, ob eine Entscheidung ohne künstliche Intelligenz eventuell nicht zu einem ähnlichen Ergebnis gekommen wäre. Es ist davon auszugehen, dass weitere Gerichtsentscheidungen – eventuell auch weitere Gesetze – Unternehmen und Anbieter von Systemen künstlicher Intelligenz zwingen werden, zusätzliche Maßnahmen zu ergreifen, um Bürger*innen vor ungerechtfertigter Einschränkung ihrer wirtschaftlichen oder persönlichen Entfaltung zu schützen.

Kontrollverlust durch künstliche Intelligenz

Die zentrale Diskussion, die bei fast allen digitalen Diensten geführt wird, ist die des Umgangs mit personenbezogenen Daten. Grundsätzlich ist dieser Umgang durch die Datenschutz-Grundverordnung bereits geregelt. Allerdings sollten wir hier etwas genauer hinschauen. Denn nicht jede KI verwendet alle Daten auf die gleiche Weise. Dies hängt vom Einsatz, dem verwendeten System und dem Nutzungskontext ab. Wie zum Beispiel können Systeme künstlicher Intelligenz ihre jeweiligen Funktionen „lernen“? Wie schafft es eine Suchmaschine, sinnvolle Vorschläge zu machen, auch wenn wir uns vertippt haben? Solche Informationen werden aus Daten von Nutzenden gewonnen. Deren Eingaben müssen kategorisiert und analysiert werden, um beispielsweise populäre Schreibfehler zu identifizieren und den passenden Ergebnissen zuzuordnen.

Ähnliches gilt für algorithmische Filmtipps bei Video-on-Demand-Diensten, Kaufempfehlungen in Online-Shops und die Werbung,

die wir im Netz sehen. Diese Formen der Datennutzung beeinträchtigen unseren Alltag nicht. Schwieriger wird es, wenn Regierungen, andere Firmen oder Vereinigungen versuchen, auf diese Daten zuzugreifen und daraus Profile erstellen oder sie für weitere Zwecke nutzen. Ein bekanntes Beispiel ist der Skandal um die Firma *Cambridge Analytica*, die 2016 Daten von Millionen Facebook-Nutzenden ohne deren Zustimmung sammelte und sie dann für politische Werbung im US-Präsidentschaftswahlkampf verwendete. Dieser Fall hat eine breite Debatte ausgelöst, weil viele befürchten, dass das Wahlverhalten durch solche personalisierten Kampagnen manipuliert werden kann – auch wenn der tatsächliche Einfluss bis heute umstritten ist.

Bei der Verwendung von Daten durch Regierungen ist die Problemlage jedoch deutlich dramatischer, wenn beispielsweise das Verhalten von Bürger*innen mithilfe von Videoüberwachung, Vorratsdatenspeicherung und Chatfiltern ausgespäht, durch künstliche Intelligenz ausgewertet und zur Bewertung und Kontrolle der Bürger*innen verwendet wird. Solche Systeme, bei denen Menschen auf Basis ihres Verhaltens „Punkte“ sammeln oder verlieren, werden unter dem Begriff „Social Scoring“ oder „Sozialkredit“ diskutiert – und sind durch Artikel 5 der EU-Verordnung über künstliche Intelligenz ausdrücklich verboten.

Insbesondere in der Volksrepublik China werden solche Systeme derzeit in Pilotprojekten eingesetzt, um etwa das Zahlungsverhalten, den Umgang mit Behörden oder die Onlineaktivitäten von Bürgerinnen zu bewerten – mit Auswirkungen auf Reisefreiheit, Kreditwürdigkeit oder den Zugang zu Bildung. Auch in Europa gab es kritische Diskussionen über vergleichbare Ansätze, etwa im Rahmen des Forschungsprojekts INDECT, das zwischen 2009 und 2014 von der EU gefördert wurde. Es hatte unter anderem zum Ziel, verdächtiges Verhalten im öffentlichen Raum durch automatisierte Überwachungstechnologien frühzeitig zu erkennen – und rief deshalb starke Bedenken hervor, dass durch die Überwachung Bürgerrechte verletzt würden.

Diese Angst vor dem Verlust der Kontrolle über die eigenen Daten ist eine zentrale und begründete Sorge von Bürger*innen. Zwar sieht die europäische Grundrechtecharta den Schutz der Privatsphäre in Artikel 7 und 8 vor. Und das Grundgesetz schützt das Geheimnis von Brief, Post und Fernmeldewesen, die Unverletzlichkeit der Wohnung sowie das Recht auf freie Entfaltung der Persönlichkeit und auf informationelle Selbstbestimmung. All diesen Rechten ist jedoch gemein,

dass sie nicht absolut sind, sondern jeweils mit anderen Rechtsgütern abgewogen werden müssen. Diese Gedanken finden sich auch in den zentralen Regelungen für den Datenschutz, der Datenschutzgrundverordnung und in den nationalen Ausführungsgesetzen.

Der Rechtsrahmen für künstliche Intelligenz in Europa

EU-KI-Verordnung (AI Act)
Die 2024 verabschiedete KI-Verordnung ist der erste umfassende Rechtsrahmen für künstliche Intelligenz weltweit. Sie klassifiziert KI-Systeme nach Risikostufen – von minimalem bis zu unvertretbarem Risiko – und legt für Hochrisiko-Systeme (z. B. in Bildung, Justiz oder Medizin) strenge Anforderungen fest. Bestimmte Anwendungen wie Social Scoring oder biometrische Echtzeitüberwachung im öffentlichen Raum sind verboten.

Datenschutz-Grundverordnung (DSGVO)
Die DSGVO schützt personenbezogene Daten in der EU und gilt auch für KI-Systeme. Sie schreibt unter anderem Transparenz, Zweckbindung und die Möglichkeit menschlicher Letztentscheidungen bei automatisierten Prozessen vor.

Weitere Rechtsakte (in Vorbereitung)
Neben dem AI Act entwickelt die EU derzeit ergänzende Vorschriften, zum Beispiel zu Urheberrechten bei KI-generierten Inhalten.

Neben der Art, welche Daten verarbeitet werden, ist ein weiterer Faktor entscheidend: Bürger*innen müssen verstehen können, was mit ihren Daten geschieht und warum. Die Frage, wie Transparenz für Entwicklung und Einsatz von künstlicher Intelligenz hergestellt werden kann, ist schwierig. Die Systeme sind in der Regel zu komplex, um von den Nutzenden in Gänze verstanden zu werden. Selbst ihre Entwickler haben Probleme damit, nachzuvollziehen, wie selbst lernende Systeme entscheiden. In der KI-Forschung wird dies als das Blackbox-Problem bezeichnet. Hier wird auch in Zukunft weiter zu diskutieren sein, wie die Anforderungen an die Transparenz von künstlicher Intelligenz so gestaltet werden können, sodass Bürger*innen die Technologie und ihre Anwendung verstehen und nachvollziehen können, was sie vermag und wo ihre Fähigkeiten enden.

Die Frage, ob eine künstliche Intelligenz also Daten von Bürger*innen nutzen darf, hängt davon ab, wozu diese Daten verwendet werden sollen und wie die Bürger*innen in die Nutzung der Daten einbezogen werden. Eine durch künstliche Intelligenz gestützte Übersetzungssoftware für den Hausgebrauch würde beispielsweise als weit weniger kritisch eingestuft als ein System, das Prognosen über die Rückfallwahrscheinlichkeit eines verurteilten Kriminellen machen soll. Und Unternehmen, die erklären, wozu sie welche Daten verarbeiten, werden als vertrauensvoller eingestuft als solche, die das nicht tun.

Ein besseres, würdevolleres Leben durch künstliche Intelligenz

Wenn es um die Wahrung von Grundrechten geht, gilt es, nicht nur die Risiken von KI zu beleuchten, sondern auch die Chancen. So können etwa Menschen mit Sehbeeinträchtigung mithilfe vernetzter Brillen Objekte identifizieren und Texte lesen. Sie können sich damit im Straßenverkehr bewegen und haben so die Möglichkeit, am öffentlichen Leben in einer Art und Weise teilzunehmen, die ihnen ohne diese Technologie verwehrt bliebe. Der Einsatz solcher Technologien erfolgte in Europa mit deutlicher Verzögerung.

Anwendungen der künstlichen Intelligenz können außerdem dazu beitragen, die Erkennung und Behandlung schwerer Erkrankungen maßgeblich zu verbessern und es den Betroffenen so ermöglichen, ein längeres und selbstbestimmtes Leben zu führen. Daneben kann künstliche Intelligenz auch wichtige Prognosen über die Entwicklung unseres Planeten liefern und die Auswirkungen des globalen Klimawandels besser handhabbar machen. Sie leistet dadurch einen wichtigen Beitrag zur Bekämpfung existenzieller Bedrohungen für viele Menschen.

Das macht KI-gestützte Analyse- und Übersetzungsprogramme in verschiedenen grundrechtssensiblen Bereichen zu weit mehr als zu einem hilfreichen Instrument. Die Technologie könnte zum zentralen

Hebel werden, um überhaupt erst handlungsfähig zu sein. Trotz der Diskussionen um das Diskriminierungspotenzial durch fehlerhaft programmierte oder auf falschen Annahmen basierte künstliche Intelligenz könnte diese, bei richtiger Einstellung und Programmierung, auch einen wichtigen Beitrag zur Beseitigung der Diskriminierung von Menschen liefern. Anders als Menschen ist sie für rassistische oder geschlechtliche Voreingenommenheit weit weniger anfällig, wenn auch nicht immun.

Künstliche Intelligenz ermöglicht Bürger*innen den Zugang zu Texten und Informationen in fremden Sprachen. Für viele Menschen bietet dies die Möglichkeit, sich jenseits der Propaganda ihrer eigenen Regierungen zu informieren. Für sie ist künstliche Intelligenz ein wichtiger Beitrag zur informationellen Selbstbestimmung. Insgesamt kann man festhalten, dass KI-basierte Anwendungen auf vielfältige Art und Weise einen zentralen Beitrag zum Schutz und zur Wahrnehmung von Grundrechten leisten kann.

Transparenz, Nachvollziehbarkeit, Einsatzweise – Plädoyer für eine sinnvolle Nutzung

Entscheidend für die Wechselwirkung von künstlicher Intelligenz und Grundrechten sind letztlich die Ausgestaltung der Technologie und die Art und Weise, wie sie genutzt wird. Wie die Ausführungen oben zeigen, korrespondiert mit fast jedem unterstellten Risiko eine entsprechende Chance. In welche Richtung sich die Entwicklung von künstlicher Intelligenz bewegt, entscheiden schlussendlich wir Menschen. Maßgeblich für die sichere und bürgerrechtskonforme Anwendung von künstlicher Intelligenz ist die Nachvollziehbarkeit dessen, was das System leistet – für Betreiber, Nutzende und für Personen, die vom Einsatz der KI betroffen sind. Zu einer ähnlichen Erkenntnis kam bereits 2018 die hochrangige Expert*innengruppe für künstliche Intelligenz bei der Europäischen Kommission

(*High Level Expert Group on Artificial Intelligence*). Je klarer Menschen verstehen, was künstliche Intelligenz macht, wie sie es macht und weshalb, desto eher sind sie imstande, die Entscheidungen eines solchen Systems zu akzeptieren, und desto bessere Möglichkeiten haben sie, sich im Zweifel auch bei Fehlern oder Missbrauch zu wehren.

Mit der europäischen KI-Verordnung und daraus abgeleiteten Rechtsakten, die derzeit entwickelt werden, sowie der Datenschutz-Grundverordnung ist ein Rechtsrahmen für den Einsatz von künstlicher Intelligenz bereits vorhanden. Er setzt teilweise sehr strikte Grenzen für den Einsatz solcher Systeme. Entscheidend ist es, den Zweck des Einsatzes der Systeme und die Einsatzweise nicht aus dem Auge zu verlieren. Es handelt sich bei künstlicher Intelligenz nach wie vor um eine von Menschen gestaltete Technologie, deren Nutzung der Mensch bestimmt. Sie erfüllt die Vorgaben ihrer Programmierung. Sie kann aber selbst nicht darüber hinauswachsen und eigene Visionen entwickeln – auch nicht von elektrischen Schafen und Robotern.

Philipp Ehmann wurde 1982 in Stuttgart geboren. Er absolvierte ein Studium der Politologie an der Freien Universität Berlin. Nach seinem Abschluss arbeitete er in Abgeordnetenbüros des Deutschen Bundestages und in Fachverbänden. Beruflich befasst er sich seit 2011 mit digitalen Themen und der Politik dazu. Seit 2025 leitet er das Berliner Büro von eco – Verband der Internetwirtschaft e. V.

Helene Hahn

Digitale Überwachung – eine geduldete Gefahr für Pressefreiheit und Demokratie

„News is what someone somewhere wants to keep secret. Everything else is advertising", soll Lord Northcliff, der britische Journalist und Zeitungsbesitzer des frühen 20. Jahrhunderts, gesagt haben. Dieser Satz hat auch heute noch seine Gültigkeit: Journalismus besteht darin, sorgfältig zu recherchieren, zu dokumentieren und zu veröffentlichen, was andere, oft mächtige Akteur*innen geheim halten wollen. Journalismus bedient damit ein gesellschaftliches Interesse nach Transparenz und spielt eine wesentliche Rolle bei der Verwirklichung demokratischer Rechte. Die Pressefreiheit als universell geltendes Menschenrecht und wichtiges Kommunikationsgrundrecht bildet dafür das Fundament. Es garantiert, dass Medien frei arbeiten können, abseits von staatlicher Zensur, Repression und Einschüchterung.

Wo Medien nicht über Unrecht, Machtmissbrauch oder Korruption berichten können, findet keine öffentliche Kontrolle des Regierungshandelns statt, keine freie Meinungsentfaltung und kein friedlicher Austausch von Interessen in einer Gesellschaft. Daher ist die Freiheit, zu informieren und informiert zu werden, ein wichtiger Gradmesser für eine funktionierende, gesunde Demokratie. Der freie Austausch von Informationen ist der erste Schritt zu gesellschaftspolitischen Veränderungen – deshalb fürchten nicht nur autoritäre Regierungen eine freie und unabhängige Berichterstattung.

In vielen Ländern Europas versuchen Regierungen, den Raum für unabhängigen Journalismus einzuschränken. Wer politisch unliebsame Berichterstattung bekämpfen will, geht zunehmend digital gegen Medienschaffende vor. Schadsoftware, Malware, Staatstrojaner – das sind verschiedene Begriffe für invasive Überwachungssoftware, die im staatlichen Auftrag oder durch staatliche Institutionen gegen politische Gegner*innen eingesetzt werden. Einmal auf das Gerät gelangt, können Anrufe mitgehört und sämtliche Daten eingesehen und manipuliert werden. Über die Aufnahmefunktion können Gespräche und Videos heimlich aufgezeichnet werden. E-Mails, Chat-Nachrichten, Kontakte, Passwörter, Bilder und Notizen – alles steht den Angreifenden in Echtzeit zur Verfügung. Überwachungssoftware ist so designt, dass sie keine Spuren des Angriffs hinterlässt und die Verantwortlichen verschleiert werden. Das macht es für von Überwachung betroffene Journalist*innen enorm schwer, eine Infektion zu erkennen und die Verantwortlichen vor Gericht zu bringen.

Als *Reporter ohne Grenzen* setzen wir uns für Informations- und Pressefreiheit ein. Wir kämpfen für einen umfassenden Schutz von Medienschaffenden weltweit. In unserer Arbeit begegnen wir immer wieder Journalist*innen, deren Computer beschlagnahmt, Mobiltelefone gehackt und Zugriff auf sämtliche Daten erlangt wurden. In vielen Fällen wurde ihre gesamte Kommunikation mit Quellen und Kolleg*innen über Monate mitgehört und Rechercheinhalte digital ausgespäht. Die Angriffe erfolgen heimlich, ohne Kenntnis der Betroffenen. Oft müssen sie nicht einmal eine Aktion ausführen – zum Beispiel auf einen Link klicken oder eine Datei öffnen –, damit ihre Geräte mit Schadsoftware infiziert werden.

Von EU-Staaten geförderte und genutzte Schattenindustrie

Digitale Überwachung ist unsichtbar und doch äußerst präsent. Das Pegasus-Projekt – eine internationale Recherche des journalistischen Netzwerks *Forbidden Stories* in Zusammenarbeit mit Amnesty International und Journalist*innen aus zahlreichen Medienorganisationen, darunter *Die Zeit*, *The Guardian*, *Washington Post* und viele mehr – gab 2021 der Öffentlichkeit einen zuvor nie da gewesenen Einblick in die geheime Arbeit der Überwachungsindustrie und ihrer staatlichen Kunden. Im Zentrum stand Pegasus, die Überwachungssoftware der Firma *NSO Group*. Mehr als 180 Journalist*innen befanden sich auf einer geleakten Liste von 50.000 identifizierten potenziellen Angriffszielen. Forensische Analysen des *Citizen Lab*, einem unabhängigen, interdisziplinären Recherchekollektiv an der Universität von Toronto, konnten den Einsatz von Pegasus in 45 Ländern der Welt zurückverfolgen. Auch in der EU haben 14 Regierungen die Schadsoftware eingekauft. Nach Angaben der Hersteller dient sie dem Kampf gegen Kriminalität und Terrorismus, tatsächlich wird sie jedoch dazu verwendet, mittels digitaler Überwachung weltweit Menschenrechtsverletzungen zu verüben.

In den vergangenen Jahren standen zahlreiche EU-Länder, die als demokratisch gelten, im Mittelpunkt von weitreichenden Überwachungsskandalen. Das Argument, die Überwachung diene dem Schutz der „nationalen Sicherheit“, ist ein häufig genutztes Mittel, um den Einsatz invasiver Software wie Pegasus zu rechtfertigen. Doch diese Begründung ist vage und juristisch so weit auslegbar, dass damit jegliche Schutzrechte von Journalist*innen ausgehebelt werden können. Richterliche Kontrollen werden umgangen oder Überwachungsmaßnahmen geheim gehalten. Eine unabhängige Überprüfung des Regierungshandelns wird dadurch verhindert, sodass die tatsächlichen Interessen hinter der Überwachung vor der Öffentlichkeit verschleiert werden.

Als die Überwachungsskandale in Polen, Spanien, Ungarn und Griechenland publik wurden, haben alle diese Regierungen auf dieses Argument zurückgegriffen. In Spanien verteidigte die Regierung den Einsatz von Pegasus zunächst mit dem Hinweis auf nationale Sicherheitsinteressen, insbesondere im Kontext des katalanischen Unabhängigkeitsreferendums. Über 60 Personen wurden zwischen 2017 und 2020 überwacht. Später stellte sich heraus, dass die Überwachung von Politiker*innen und Medienschaffenden ohne richterliche Genehmigung erfolgte.

In Griechenland wurden 13 Medienschaffende mit der Überwachungssoftware Predator der Firma *Intellexa Alliance* ausspioniert. Im Zentrum der Affäre steht seit 2022 der griechische Geheimdienst EYP, der direkt dem Premierminister unterstellt ist. Während die Regierung jegliche Verantwortung von sich wies, veröffentlichten Medien immer mehr Hinweise zu den Verstrickungen des Staates in die illegale Überwachung. Die Reporter Thanasis Koukakis und Tasos Telloglou hatten mit ihrem Team den Überwachungsskandal an die Öffentlichkeit gebracht. Durch ihre regierungskritische Berichterstattung gerieten sie selbst ins Visier der Behörden. Letztere versuchten, den Angaben der beiden Reporter zufolge, die Quellen der Journalisten zu identifizieren und Einblicke in die Berichterstattung zu erlangen. Konsequenzen gab es kaum: Zwar musste der Geheimdienstchef aufgrund des öffentlichen Drucks zurücktreten, die juristische Aufklärung ließ jedoch gerade den Geheimdienst bei der Untersuchung unberücksichtigt. Ein neues Gesetz verweigert nun sogar Betroffenen, Auskunft über die sie betreffenden Fälle und Akten zu erhalten – wieder mit Verweis auf die nationale Sicherheit.

Die Aufarbeitung der Fälle ist enorm schwierig, da die Regierungen die genauen Maßnahmen geheim halten; Betroffene werden alleingelassen. Auch der jüngste Überwachungsskandal in Italien zeigt ähnliche Tendenzen. Im Februar 2025 berichtete der britische *Guardian*, dass der italienische Journalist Francesco Cancellato mit der Spyware Graphite des Unternehmens *Paragon Solutions* ausspioniert wurde. Er recherchierte zu organisiertem Verbrechen und Rechtsextremismus, auch in der Jugendorganisation der Partei der italienischen Ministerpräsidentin Giorgia Meloni. Neben Cancellato wurden außerdem sechs Menschenrechtsaktivist*innen aus der Geflüchtetenhilfe überwacht. Insgesamt sind 90 Personen aus 14 Ländern betroffen, auch aus Deutschland. Es ist unklar, wer verantwortlich ist.

Die italienische Regierung reagierte widersprüchlich: Zunächst bestritt sie jegliche Überwachung von Medienschaffenden, verweigerte später aber dem Parlament unter Verweis auf Geheimhaltung weitere Auskünfte. Cancellato hat bereits Anzeige bei der Staatsanwaltschaft von Palermo gestellt. Obwohl seine Überwachung bis Dezember 2024 andauerte, kennt er bis heute weder den genauen Zeitraum noch den Auftraggeber.

Deutsche Behörden im Besitz von umstrittener Überwachungssoftware

Auch Deutschland nutzt invasive Überwachungssoftware. 2021 wurde bekannt, dass das Bundeskriminalamt (BKA) und der Bundesnachrichtendienst (BND) Pegasus erworben haben. Nach Angaben dieser Behörden handele es sich um eine modifizierte Version. Das kann allerdings nicht unabhängig verifiziert werden, weil Informationen und Hintergrundberichte zur Software als geheim eingestuft sind. Selbst dem Parlamentarischen Kontrollgremium, das für die Kontrolle des BND zuständig ist, verschwieg die Bundesregierung von CDU/CSU und SPD in ihrer letzten gemeinsamen Amtszeit, dass auch der deutsche Auslandsgeheimdienst die umstrittene Software nutzt.

Dass der BND an journalistischen Quellen Interesse hat, zeigt die Vergangenheit. 2017 berichtete beispielsweise der *Spiegel*, dass der BND bereits seit 1999 viele ausländische Medienschaffende und Redaktionen überwacht hat: Anschlüsse der BBC in Afghanistan und London, Redaktionen des *BBC World Service*, ein Anschluss der *New York Times* in Afghanistan, Anschlüsse von Mobil- und Satellitentelefonen der Nachrichtenagentur *Reuters* in Afghanistan, Pakistan und Nigeria standen auf der Liste der überwachten Medien. Der Geheimdienst zapfte über mehrere Monate die Kommunikation der *Spiegel*-Journalistin Susanne Koelbl an, als sie 2006 mit dem afghanischen Handelsminister in Kontakt stand.

Erst 2023 verwies das Rechtsportal *Legal Tribune Online* auf ein gerichtliches Schreiben des BND, in dem der Geheimdienst zugibt, dass er weiterhin auf Medienschaffende als nachrichtendienstliche Quellen zurückgreift – wohl entgegen den Weisungen des Bundeskanzleramts. Das ist hochproblematisch, weil diese Praxis die Glaubwürdigkeit der Medien ins Wanken bringt und gegen den journalistischen Quellenschutz verstößt. Darauf verweist der Pressekodex ausdrücklich, der journalistisch-ethische Grundregeln enthält und hohe Qualitätsstandards für den Journalismus definiert. Dort steht beispielsweise, dass nachrichtendienstliche Tätigkeiten von Journalist*innen und Verleger*innen mit den Pflichten aus dem Berufsgeheimnis und dem Ansehen der Presse nicht vereinbar sind.

Auch die *Zentrale Stelle für Informationstechnik im Sicherheitsbereich*, die deutsche „Hackerbehörde“, die für Polizei und Geheimdienste Überwachungstechnik entwickelt und einkauft, ist seit 2019 Kunde der international agierenden *Intellexa Alliance*. Jahre zuvor kauften deutsche Behörden den Staatstrojaner FinSpy der in Hamburg ansässigen Firma *FinFisher*. FinSpy war 2017 auf einer Webseite aufgetaucht, die als Mobilisierungswebseite der türkischen Oppositionsbewegung getarnt war, und ermöglichte so die Überwachung einer großen Zahl politischer Aktivist*innen und Medienschaffender durch den türkischen Geheimdienst MIT.

Der Export solcher Überwachungssoftware in Länder außerhalb der EU ist seit 2015 europaweit genehmigungspflichtig. Obwohl die Bundesregierung keine Exportgenehmigungen erteilt hat, tauchten Versionen des FinSpy-Trojaners in Ländern mit repressiven Regimen auf, etwa in Ägypten oder Myanmar. Die unregulierte Überwachungsindustrie

hat gelernt, Europas poröse Exportkontrollen zu ihren Gunsten zu nutzen – und das wird von EU-Mitgliedstaaten akzeptiert.

Forderungen: Höchste Zeit zu handeln

Digitale Überwachung greift Grundrechte wie die Pressefreiheit in ihren Fundamenten an, weil der Schutz der Quellen und das Redaktionsgeheimnis ausgehebelt werden. Die vertrauliche Kommunikation, der Schutz von Rechercheinhalten und von Redaktionsvorgängen sind für einen freien Journalismus unentbehrlich. Eine kritische Medienlandschaft ist auch auf demokratische Strukturen angewiesen, damit sie frei informieren kann und wir als Gesellschaft informiert bleiben.

Es muss ein global verbindlicher Rechtsrahmen für die Regulierung von Überwachungstechnologien entwickelt werden, der im Einklang mit den UN-Leitprinzipien für Wirtschaft und Menschenrechte steht. Unternehmen müssen gesetzlich verpflichtet werden, menschenrechtliche Sorgfaltspflichten einzuhalten und zu prüfen, ob ihre Aktivitäten Menschenrechte verletzen. Für Verstöße müssen sie strafrechtlich haftbar gemacht werden können. Für invasive Spähsoftware, die wie Pegasus, Predator und Co. gar nicht erst mit Menschenrechten vereinbar sind, muss ein internationales Verbot über den Einsatz, den Verkauf und die Weitergabe der Produkte und Dienstleistungen erwirkt werden. Der frühere UN-Sonderberichterstatter für Meinungsfreiheit, David Kaye, hat sich bereits 2021 für ein Moratorium ausgesprochen.

Firmen, ihre Führungskräfte und Förderer, deren Produkte nachweislich systemischen Missbrauch ermöglichen und gegen Menschenrechte verstoßen, müssen auf Sanktionslisten geführt und streng kontrolliert werden. Die EU-Mitgliedstaaten müssen sich zudem im Sinne einer effektiveren Exportkontrolle verpflichten, Informationen über genehmigte oder verweigerte Exporte von Überwachungstechnologien zu veröffentlichen. Länder wie Deutschland müssen letztendlich davon Abstand nehmen, Produkte dieser Firmen einzukaufen. Tun sie das nicht, sind sie als Kunden und Financiers für die

Menschenrechtsverbrechen an Journalist*innen und Menschenrechtsaktivist*innen mitverantwortlich.

Pressefreiheit ist selbst in Demokratien nicht selbstverständlich. Angesichts zunehmender weltpolitischer Konflikte und dem Erstarken autoritärer Bewegungen müssen Politiker*innen, die die Demokratie erhalten und schützen wollen, der Gefahr der digitalen Überwachung von Medienschaffenden deutlich mehr Aufmerksamkeit schenken und konsequente Maßnahmen ergreifen. Die private Überwachungsindustrie kann seit Jahren in und aus Europa ungehindert schalten und walten. Europäische Länder haben durch den Gebrauch der Überwachungssoftware nicht nur gegen ihre eigenen Menschenrechtsverpflichtungen verstoßen, sondern es versäumt, Skandale im Sinne der betroffenen Personen effektiv und transparent aufzuklären. Es ist höchste Zeit, zu handeln!

Helene Hahn setzt sich als Referentin für Internetfreiheit bei Reporter ohne Grenzen für die Presse- und Informationsfreiheit weltweit ein. Sie arbeitet und recherchiert zu Zensur, staatlicher Überwachung und der Regulierung von Plattformen. Zuvor hat sie international tätige Organisationen beraten, darunter das Büro des UN High Commissioner for Human Rights, das Goethe-Institut und das Auswärtige Amt. Sie hat einen Masterabschluss im internationalen Menschenrecht und Good Governance.

Literaturhinweise

- Pressekodex: https://www.presserat.de/pressekodex.html
- Abschlussbericht des EU-Sonderausschusses „PEGA“ zur Verbreitung und Nutzung von Pegasus und vergleichbarer Überwachungssoftware in der EU: https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html#_ftn662
- UN-Leitprinzipien für Wirtschaft und Menschenrechte: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
- Bericht über die Unvereinbarkeit von Überwachungstechnologien mit Menschenrechtsstandards, veröffentlicht durch den Hohen Kommissar für Menschenrechte der UN: https://repository.graduateinstitute.ch/record/301602?v=pdf

Thomas Greven

Wer schützt die Meinung? Europa, Amerika und der Kampf um die digitale Öffentlichkeit

In den USA wird Meinungsfreiheit traditionell sehr weit gefasst. Amerikaner*innen kennen das Konzept einer „wehrhaften Demokratie“ nicht, das in Deutschland aufgrund der Erfahrungen des Dritten Reiches entwickelt wurde, als die demokratische Ordnung der Weimarer Republik in einer demokratischen Wahl abgesetzt wurde. Aufgrund dieser und anderer historischer Erfahrungen hat sich in Europa eine andere, restriktivere Tradition der Meinungsfreiheit entwickelt als in den USA.

Doch auch die amerikanischen Internet-Unternehmen müssen sich mit diesen stärkeren Beschränkungen arrangieren – beispielsweise mit dem britischen Presserecht und seinen Verleumdungsgesetzen („Libel Laws“), dem Verbot von Volksverhetzung und insbesondere von Holocaust-Leugnung in Deutschland sowie den Regulierungen im *Digital Services Act* der Europäischen Union. Davon betroffen sind vor allem die Social-Media-Plattformen, da hier die politischen Debatten heißlaufen und unterschiedliche Meinungen und Tatsachenbehauptungen aufeinandertreffen.

Die großen Medienunternehmen sind alle US-Gründungen und drängen darauf, diese Beschränkungen loszuwerden. Das erklärt mutmaßlich die neue Unterwürfigkeit des Silicon Valley gegenüber US-Präsident Donald Trump. Unternehmer wie Mark Zuckerberg suchen opportunistisch die Hilfe der US-Regierung im Kampf gegen die EU-Regeln. Und die Regierung liefert: Außenminister Marco Rubio schrieb „Das ist keine Demokratie - das ist verkappte Tyrannei“, weil der deutsche Verfassungsschutz die AfD als „gesichert rechtsextremistisch“ klassifiziert hat, und das Innenministerium gegen Publikationen wie die rechtsextreme Monatszeitschrift Compact vorgeht.[1]

Bereits zuvor schockierte der amerikanische Vizepräsident JD Vance das Publikum der 61. Münchener Sicherheitskonferenz im Februar 2025. Er sprach nicht etwa vorrangig über die russische Aggression gegen die Ukraine und die mögliche Rolle der Regierung Trump bei der Beilegung des Konflikts, sondern attackierte die europäischen Regierungen für staatliche Einschränkungen der Meinungsfreiheit. „Die Bedrohung, die mir in Bezug auf Europa am meisten Sorgen bereitet, ist nicht Russland, nicht China, nicht irgendein anderer externer Akteur. Was mir Sorgen bereitet, ist die Bedrohung von innen. Der Rückzug Europas von einigen seiner grundlegendsten Werte“, erklärte er.

Cancel Culture oder notwendige Moderation?

Der scharfe Ton ist in dieser Debatte nicht ungewöhnlich, jedenfalls nicht in den USA. Dort wird gegen traditionelle Medien und Social-Media-Plattformen sowie gegen Universitäten lautstark der Vorwurf erhoben, konservative Stimmen zu unterdrücken. Lange ging es dabei vor allem um den „liberal bias“ von professionellen Journalist*innen und Professor*innen – also eine unterstellte linksliberale Voreingenommenheit in den intellektuellen Diskursen und den Medien. Zwar lässt sich empirisch tatsächlich belegen, dass die Medienschaffenden in den USA eher den Demokraten als den Republikanern zuneigen, doch ihr Einfluss wurde und wird von den eher konservativen Einstellungen der Eigner, Herausgeber und Chefredaktionen beschränkt: „Freedom of the press is limited to those who own one”, schrieb A. J. Liebling bereits 1960. So verhinderten die Milliardäre Jeff Bezos (*Amazon* und Eigentümer der *Washington Post*) und Patrick Soon-Shiong (früherer Pharmazieunternehmer und Eigentümer der *LA Times*), dass sich die Redaktionen der Zeitungen 2024 für die Wahl von Kamala Harris (und damit gegen Donald Trump) aussprachen.

Schon Roger Ailes nannte den „liberal media bias“ als Grund für die Schaffung des rechtskonservativen Nachrichtensenders *Fox News*. Inzwischen ist die rechte Medienkritik deutlich erweitert und verschärft worden. Laut konservativen Medienkritikern wie Mona Charen (*The Bulwark*) und republikanischen Politikern wie Jim Jordan (Ohio) herrsche eine linksliberale Meinungsdiktatur und eine Cancel Culture der politisch motivierten Unterdrückung konservativer Stimmen. Mittels nur vorgeblich objektiver Praktiken wie Faktenchecks, Inhaltemoderation und schließlich gezielter Ausschlüsse von Nutzenden durch Plattformen (sogenanntes *deplatforming*) wegen angeblicher Hassrede würden konservative Stimmen buchstäblich zum Schweigen gebracht. Diese Einschränkungen der in den USA traditionell sehr weit gefassten Meinungsfreiheit sei „unamerikanische Zensur“ und ihre Befürworter seien nichts als „Snowflakes“, die bei leidenschaftlich vorgetragener Kritik und Gegenmeinungen gleich schmelzen würden wie Schnee in der Sonne.

Diese Haltung spiegelt ein in den USA geflügeltes Wort, mit dem man schon Kinder für die harte Welt des Meinungsstreits präpariert: „Sticks and stones will break my bones, but words will never harm me.“ (sinngemäß: „Stöcke und Steine können mir wehtun, aber Worte niemals.“). Natürlich weiß man es auch in den USA besser; es ist wissenschaftlich ausreichend dokumentiert, welche negativen Folgen beispielsweise verbale Gewalt haben kann. Und selbstverständlich gibt es auch in den USA gesetzliche Grenzen für die vom ersten Verfassungszusatz umfassend geschützte und deshalb traditionell sehr weit gefasste Meinungsfreiheit.

Im Wikipedia-Artikel zu „United States free speech exceptions“ – Ausnahmen von der Redefreiheit in den Vereinigten Staaten – kann man etwa nachlesen:

„Categories of speech that are given lesser or no protection by the First Amendment include obscenity …, fraud, child pornography, speech integral to illegal conduct, speech that incites imminent lawless action, and regulation of commercial speech such as advertising. … other limitations on free speech balance rights to free speech and other rights, such as rights for authors over their works (copyright), protection from imminent or potential violence against particular persons, restrictions on the use of untruths to harm others (slander and libel), and communications while a person is in prison.“

„Sprachäußerungen, die durch den First Amendment nur eingeschränkt oder gar nicht geschützt werden, umfassen unter anderem Obszönität, Betrug, Kinderpornografie, Äußerungen im Zusammenhang mit illegalem Verhalten sowie Aufrufe zu unmittelbar bevorstehenden rechtswidrigen Handlungen. Auch kommerzielle Kommunikation wie Werbung unterliegt bestimmten Regulierungen. Weitere Einschränkungen der Meinungsfreiheit ergeben sich aus dem Ausgleich mit anderen Rechten – etwa dem Urheberrecht, dem Schutz vor unmittelbarer oder potenzieller Gewalt gegen bestimmte Personen, dem Verbot verleumderischer oder rufschädigender Falschbehauptungen (Verleumdung und Beleidigung) sowie der Kommunikation in Haft."

Private Akteur*innen dürfen die Meinungsfreiheit beschränken, sind aber nur in Ausnahmefällen dazu verpflichtet. Dies gilt auch für Social-Media-Plattformen, für die zudem bestimmte Regulierungen für journalistische Medien nicht gelten. Insbesondere nimmt Section 230 des *Communications Decency Act* von 1996 die Plattformen aus der rechtlichen Haftung für einen Großteil der von Nutzenden der Plattformen verbreiteten Inhalte. Zudem dürfen sie ihre eigenen Regeln für die Inhaltsmoderation aufstellen.

Inhaltsmoderation, Faktenchecks und politische Filter

Vor allem zwei Ereignisse der vergangenen Jahre haben dazu beigetragen, dass die meisten Betreiber von Plattformen sozialer Medien (zumindest zeitweise) verstärkt mit Faktenchecks und Inhaltsmoderation sowie mit Plattformentzug gearbeitet haben, um Hass, Hetze, gezielte Desinformation und Verschwörungserzählungen einzuhegen: die Covid-19-Pandemie und die „große Lüge" der angeblich gestohlenen US-Präsidentschaftswahl von 2020. Zum einen sollte zum Schutz der öffentlichen Gesundheit verhindert werden, dass Impfgegner im öffentlichen Diskurs die Oberhand gewinnen. Zum anderen gab es bereits vor dem „Sturm auf das Kapitol" am 6. Januar 2021 berechtigte Sorge, dass Donald Trump und andere radikale, populistische „Polarisierungsunternehmer", wie der

deutsche Soziologe Steffen Mau sie nennt, ihre Anhänger zu politischer Gewalt anstacheln können.

Klar war auch, dass sich insbesondere die sozialen Medien und ihre algorithmisch verstärkten Filterblasen für diese extrem emotionalisierte Art von Politik oder „Hyperpolitik“, wie sie der belgische Historiker Anton Jäger bezeichnet, eignen. Social-Media-Plattformen sind eben keine neutralen „Marktplätze der Ideen“, sondern sie werden tendenziell zu vermachteten Monopolstrukturen, die gemäß kommerzieller Motive gelenkt werden. In der Folge kam es auch dazu, dass die Accounts prominenter Protagonist*innen der Politik der Angst und Wut gesperrt wurden; insbesondere wurden Donald Trumps Möglichkeiten beschnitten, seine Millionen Follower direkt zu erreichen. Auch deshalb gründete er mit „truth.social“ eine eigene Plattform, die aber bisher nur mäßig erfolgreich ist.

Ist also etwas dran an den Vorwürfen von Zensur und Cancel Culture? War es deshalb nur recht und billig, dass Mark Zuckerberg auf den kulturellen Wendepunkt des zweiten Wahlsiegs Donald Trumps im November 2024 reagierte und auf den Meta-Plattformen wie Facebook und Instagram professionelle Faktenchecks und Inhaltsmoderation durch Community Notes ersetzte? Diese Hinweise von und für die Nutzenden sind weniger effektiv, aber eben auch weniger invasiv. Elon Musk hatte diesen Schritt nach der Übernahme von Twitter (jetzt X) bereits vollzogen, worauf die Verbreitung von Hassrede, Hetze und Desinformation stark anstieg.

Einerseits sind Faktenchecks und Inhaltsmoderation und die mit ihnen verbundenen Einschränkungen der Meinungsfreiheit zwangsläufig politisch. Es müssen Entscheidungen über Kriterien getroffen werden. Auch die Anwendung dieser Kriterien, wenn sie nicht automatisiert erfolgt, bedarf im Zweifelsfall menschlicher Bewertung. Es ist gut dokumentiert, dass diesbezügliche Entscheidungen politische Haltungen und Präferenzen derjenigen widerspiegeln, die in der Entscheiderposition sitzen, und bisweilen zuungunsten der Meinungsfreiheit ausgefallen sind.

Andererseits ist es ebenfalls gut dokumentiert, dass gezielte Desinformation, Hassrede und Hetze gegen Frauen, Minderheiten etc. überwiegend von Akteur*innen der radikalen und extremistischen Rechten – Menschen und gezielt eingesetzten Bots – verbreitet werden. Und deshalb sind politisch rechts stehende Nutzende bei den

vorgenommenen Einschränkungen der Meinungsfreiheit überrepräsentiert. In diesem Zusammenhang ist der Hinweis wichtig, dass es dabei entgegen der Behauptung der Zensurkritiker eben nicht in erster Linie um traditionell konservative Stimmen geht. Von Meinungseinschränkungen durch Faktenchecks und Inhaltsmoderation betroffen sind vor allem radikale Rechte, die demokratiefeindliche, autokratische und extremistische Positionen vertreten. Insofern sich diese Haltungen in ihren Meinungsäußerungen niederschlagen, sind sie selbstverständlich von einschränkenden Maßnahmen stärker betroffen.

Repression statt Debatte – Meinungsfreiheit unter Trump 2.0

Wie wohlfeil und heuchlerisch die Kritik an der Cancel Culture und der Snowflake-Vorwurf waren, wird auch daran deutlich, dass sich die Verhältnisse in den USA seit der zweiten Amtseinführung Trumps komplett in ihr Gegenteil verkehrt haben. Bereits während seiner ersten Amtszeit diffamierten er und seine Anhänger kritische Medien pauschal als Fake News und sogar als Volksfeinde („enemies of the people“). Eine Regierung, die sich nicht scheut, staatliche Macht zur Bestrafung ihrer politischen Gegner zu benutzen, geht inzwischen drastisch gegen unbequeme Meinungsäußerungen vor. Bisher sind davon vor allem Nicht-Staatsbürger*innen betroffen, beispielsweise Gaststudierende, die sich pro-palästinensisch äußern und abgeschoben werden, oder Trump-Kritiker*innen, denen die Einreise verwehrt wird. Aber die Angst vor Vergeltungsmaßnahmen greift um sich, wie selbst die republikanische Senatorin und Trump-Kritikerin Lisa Murkowski aus Alaska öffentlich bekannte.

Ein Zitat der *Stern*-Kolumnistin Jagoda Marinić zeigt deutlich, worauf die radikalen Rechten, ob in der Regierung oder in der Opposition, zielen: „Was Rechte sich eigentlich wünschen, ist Beleidigungsfreiheit gegen ihre Feinde bei gleichzeitigem Welpenschutz für sich selbst.“ Damit sind auch diejenigen gut beschrieben, die in Europa der

Kritik von JD Vance Applaus spendiert haben. Um wirkliche Meinungsfreiheit geht es dabei nicht.

Die europäischen und insbesondere deutschen historischen Erfahrungen zeigen, dass die Demokratie auch vor demokratiefeindlichen Äußerungen geschützt werden muss. Tatsächlich wird die Herausforderung durch die immer besseren KI-Deepfakes immer größer. Zudem sind westliche Gesellschaften durch Russlands Einflussstrategien bedroht, bei denen Troll-Farmen gezielt manipulative Desinformation über Bots, Doppelgänger-Websites und KI-gestützte Täuschung verbreiten.

Gerade weil restriktive Maßnahmen gegen die Meinungsfreiheit Teil des autokratischen Programms sind, das inzwischen auch in Demokratien – wie in der Türkei, Ungarn und jetzt in den USA – an Einfluss gewinnt, müssen Autokraten von der Macht ferngehalten werden, und zwar auch durch maßvolle Beschränkungen der Meinungsfreiheit. Ziel muss es dabei sein, die Vergiftung des politischen Diskurses und der politischen Kultur zu verhindern. Zugleich ist klar, dass mit Faktencheckern allein der von radikalen und extremistischen Rechten geführte Kulturkrieg nicht gewonnen werden kann (und auch gute Sachpolitik reicht dafür nicht mehr aus).

Die Verteidiger der Demokratie brauchen Emotionen und deshalb einen lebendigen öffentlichen Raum. Regulierung ist notwendig, um zu verhindern, dass eine „negative Öffentlichkeit“ dominiert – in sozialen Medien wie X ist das Zurückdrängen und das freiwillige Ausscheiden gemäßigter Stimmen immer dann zu beobachten, wenn Restriktionen wegfallen. Aber die dafür notwendigen Einschränkungen der Meinungsfreiheit stellen ein Dilemma dar, weil sie missbraucht werden können. Denn sie beruhen zwangsläufig auf politischen Entscheidungen und laufen Gefahr, unliebsame, oppositionelle Stimmen zu unterdrücken.

Das Dilemma der Demokratie – zwischen Schutz und Gefahr der Regulierung

Wenn es im Koalitionsvertrag zwischen CDU/CSU und SPD also heißt, dass die „bewusste Verbreitung falscher Tatsachenbehauptungen“ durch die Meinungsfreiheit nicht gedeckt sei, und „die staatsferne Medienaufsicht unter Wahrung der Meinungsfreiheit auf der Basis klarer gesetzlicher Vorgaben gegen Informationsmanipulation sowie Hass und Hetze vorgehen können“ muss, dann besteht zumindest die Gefahr, deutlich über das Ziel hinauszuschießen.

Bereits jetzt entsteht durch vergleichsweise harte Urteile nach Beleidigungen von Politiker*innen wie Nancy Faeser der Eindruck, dass diese als Personen des öffentlichen Lebens nicht mehr, sondern weniger Kritik aushalten müssen. Dabei heißt es doch, wie es dem US-Präsidenten Harry S. Truman zugeschrieben wird: „If you can’t stand the heat, get out of the kitchen.“ Andererseits sind insbesondere die weniger geschützten Lokalpolitiker*innen (Frauen gibt es unter ihnen immer weniger) inzwischen einer solchen Aggressivität – verbal und teilweise auch physisch – ausgesetzt, dass man nicht umhinkommt, den Handlungsbedarf anzuerkennen. Es geht also um eine Abwägung zugunsten eines zivilen öffentlichen Diskurses. Dabei sollten sich weder Meinungsfreiheitsabsolutisten noch Befürworter von Strafen für falsche Tatsachenbehauptungen durchsetzen.

Dr. phil. habil. Thomas Greven ist selbstständiger Autor, Referent und Politikberater sowie Privatdozent für Politikwissenschaft an der FU Berlin. Er hat an der FU und an der Western Michigan University studiert. Nach seiner Promotion 2000 an der FU war er wissenschaftlicher Mitarbeiter, nach seiner Habilitation 2009 Gast- und Vertretungsprofessor am Kennedy-Institut für Nordamerikastudien. Wissenschaftlich und publizistisch beschäftigt er sich u. a. mit US-Politik und der globalen radikalen Rechten.

Quellen

1 US-Regierung und die AfD Bundesregierung kontert Rubios „Tyrannei"-Vorwurf, Tagesschau.de, 03.05.2025 https://www.tagesschau.de/inland/innenpolitik/afd-verfassungsschutz-rubio-100.html

Katharina Nocun

Ich mache mir die Welt, wie sie mir gefällt? Desinformation und Fakes auf Social Media

Anfang 2025 löste ein auf Facebook kursierendes unscheinbares Bild hitzige Diskussionen aus. Darauf abgebildet war eine Gruppe von Kindern, die von zwei Erwachsenen durch eine verregnete Straße im beschaulichen Obernburg am Main gelotst wird. Soweit, so normal. Die schlichte Tatsache, dass eine Polizeibeamtin den Ausflug begleitete, ließ jedoch bei einigen Facebook-Nutzenden offenbar alle Sicherungen durchbrennen. Wenige Tage nachdem in Aschaffenburg ein Kleinkind und ein Erwachsener durch den Messerangriff eines offenbar psychisch kranken 28-jährigen Afghanen getötet und drei weitere Menschen schwer verletzt worden sind, zweifelten einige Menschen keine Sekunde daran, wie diese Szene zu deuten sei. Deutschland, so die einhellige Meinung in rechtsextremen Kreisen, sei infolge seiner Migrationspolitik eben nun endgültig im permanenten Ausnahmezustand angekommen. „Willkommen im besten Deutschland aller Zeiten: Kindergartengruppen mit Polizeischutz!“, polterte die AfD des Kreises Mayen-Koblenz wutschäumend auf Facebook.[1]

Angesichts dieser Empörungswelle sah sich die Polizei Unterfranken alsbald zu einer Stellungnahme genötigt. Die Erklärung war jedoch so einfach wie unspektakulär. Tatsächlich handelte es sich um einen ganz normalen Ausflug zur lokalen Dienststelle, wie er Jahr für Jahr tausendfach in unzähligen Kindergärten und Kitas stattfindet. „Die Gruppen werden immer zu Fuß am Bahnhof abgeholt und auch wieder dorthin zurückgebracht. Bei dieser Gelegenheit erklären wir gleich die wichtigsten Verkehrsregeln“, hieß es im Statement der Polizei. Vom großen Skandal, der in rechtsextremen Kreisen heraufbeschworen worden war, bliebt somit letztendlich nur sehr viel heiße Luft – und ein Haufen wütender Emojis.

Dass mitunter äußerst dreiste Behauptungen erstaunlich viele Menschen hinter sich versammeln können, ist beileibe kein auf das Internetzeitalter beschränktes Phänomen. Bereits im Jahr 1835 – lange bevor Reichsbürger sich in Online-Foren über mögliche extraterrestrische NS-Rückzugsorte austauschen konnten – bescherte eine sechsteilige Serie über angebliches Leben auf dem Mond der *New York Sun* eine Rekordauflage. Ebenfalls im 19. Jahrhundert – und somit eindeutig vor dem Aufkommen von Youtube und Co. – füllte der britische Autor Samuel Birley Rowbotham große Vortragshallen mit elaboriert klingenden, jedoch auf sachlicher Ebene gänzlich absurden Ausführungen über die flache Erde. Rowbothams Geschäftsmodell unterschied sich

dabei wohlgemerkt kaum von jenem zahlreicher Instagram-Accounts, die heutzutage Bücher und kostenpflichtige Vorträge fragwürdiger „Wahrheitsforscher“ anpreisen (inklusive der Forderung nach öffentlichen Streitgesprächen mit führenden Forschenden). Und wer meint, Verschwörungserzählungen und Desinformation würden erst seit Tiktok ihre toxische Kraft in politischen Debatten entfalten, sollte besser ein Geschichtsbuch zur Hand nehmen und es beim Abschnitt zum Nationalsozialismus aufschlagen. Auch wenn es verlockend erscheinen mag, gesellschaftlich missliebige Phänomene auf eine bestimmte Technik zu externalisieren – so einfach gelagert sind die Dinge dann eben doch nicht.

Soziale Netzwerke als Brandbeschleuniger

Bei aller Zeitlosigkeit des Phänomens fungieren soziale Netzwerke heute jedoch zweifellos als Brandbeschleuniger für Lügen jeder Art. Insbesondere Inhalte, die zeitliche Dringlichkeit suggerieren – oft verbunden mit politischen Forderungen – verbreiten sich online immer wieder in Windeseile. Empfehlungsalgorithmen gießen zusätzlich Öl ins Feuer. Denn Postings, die in kurzer Zeit besonders viele Reaktionen auslösen, bekommen durch die Plattformbetreiber immer wieder einen zusätzlichen Boost – in der Regel ungeachtet des Wahrheitsgehalts. Werden problematische Beiträge zudem auch noch von Accounts verbreitet, die einen Vertrauensvorschuss genießen, liegt für einige Nutzende die Annahme nahe, die jeweilige Person dürfte die Fakten schon geprüft haben. Tatsächlich steht aber oft genug am Ende einer langen Kette von vertrauensseligen Weiterleitungen eine gänzlich unbekannte Person, die beim Scrollen lediglich aus einem zufälligen Impuls heraus auf „Repost“ geklickt hatte. Diverse plattforminhärente Anreize verstärken das Problem, schließlich können Accounts, die als Erste eine „Breaking News“ posten, auf viele Likes und neue Followerschaft hoffen. Diese Verlockung wiegt zumindest für einige Menschen allem Anschein nach schwerer als das Risiko, Fakes zu verbreiten.

Der Fall der angeblichen Polizei-Eskorte verdeutlicht zudem, wie wirkmächtig in diesem Zusammenhang Bilder oder Videos sind. Auch das ist nicht neu. Als die *New York Sun* 1835 ihre Fantasiegeschichten vom Leben auf dem Mond abdruckte, durften darin Illustrationen der dort angeblich ansässigen Fledermausmenschen nicht fehlen. Und heute? Mittels Grafikprogramm oder KI manipulierte Bilder sowie Ausschnitte aus Videosequenzen populärer Shooter-Games sind beileibe nicht der einzige Fallstrick, vor dem wir uns in Acht nehmen sollten. Nicht umsonst werden bei militärischen Auseinandersetzungen regelmäßig Fotos aus lange zurückliegenden Kriegen verbreitet. Auch eine tendenziöse Auswahl des Bildausschnitts kann in die Irre führen. Die Entrüstung über den letztendlich vollkommen harmlosen Ausflug in Obernburg am Main zeigt zudem, dass selbst ein in der Sache authentisches Foto zu dramatischen Fehlschlüssen verleitet, wenn es nur mit tendenziösem Kommentar und viel emotional aufgeladener Empörungsenergie versehen in die Welt hinausposaunt wird.

Dass der Kindergarten-Post gerade in Kreisen mit extrem ablehnender Haltung zu Migration auf besonders fruchtbaren Boden fiel, liegt auch am sogenannten *Confirmation Bias*. Das ist eine kognitive Verzerrung, die zeigt, dass Menschen besonders unkritisch sind bei Inhalten, die sie in ihrem jeweiligen Weltbild bestätigen. Geschichten von angeblich bedrohten Kindern wecken außerdem starke Gefühle wie Wut oder auch Angst in uns. Eine solche Emotionalisierung begünstigt, dass wir anschließend in Sachen Plausibilität und Wahrheitsgehalt nicht ganz so genau hinschauen. Hinzu kommt, dass Geschichten, die uns vertraut vorkommen – die wir vielleicht öfter schon in unserer Timeline an uns vorbeihuschen gesehen haben, weil sie plötzlich innerhalb der eigenen Bubble in aller Munde sind – zugleich auch sehr schnell besonders wahr wirken. Nicht nur US-Präsident Donald Trump weiß um diese ungeheurere Macht der Wiederholung von Lügen. Auf unseren Fall übertragen bedeutet das: Wer sich online bevorzugt in rechtsextremen Kreisen bewegt, dürfte sich durch die Nachricht vom vermeintlichen Polizeischutz für Kinder in vielerlei Hinsicht bestätigt gefühlt haben – nicht nur in Bezug auf die jeweiligen Feindbilder. Schließlich gibt es viele Akteur*innen in diesem Milieu, die einem beständig einreden wollen, Deutschland stünde kurz vor dem Kollaps. Besonders im Umfeld von Anschlägen oder generell bei Krisen jeglicher Art lässt sich das Bedürfnis vieler Menschen nach schnellen und einfachen Antworten besonders einfach politisch instrumentalisieren.

Manipulation der öffentlichen Meinung: Desinformation und Propaganda

Im medialen Diskurs werden die Begriffe Falschinformation und Desinformation oft synonym benutzt. Während der Begriff der Falschinformation lediglich beschreibt, dass es sich um unwahre Inhalte handelt, impliziert Desinformation zusätzlich, dass hinter der Verbreitung auch eine bewusste Täuschungsabsicht steckt. Diese Unterscheidung ist wichtig, denn die Lüge war nicht ohne Grund schon immer ein äußerst effektiver Wegbegleiter politischer Propaganda, insbesondere für autoritäre Akteur*innen, die nur wenig auf Ideale wie Wissenschafts- und Pressefreiheit geben.

In diesem Kontext stellen Verschwörungserzählungen ein weiteres wirkmächtiges Werkzeug zur Manipulation der öffentlichen Meinung dar. Aus einzelnen Desinformationsbausteinen lässt sich nämlich mit etwas Geschick nach dem Motto „Connect the Dots!“ leicht ein größeres Narrativ weben, das die Anhängerschaft geradewegs in den Kaninchenbau einer eigenen Parallelrealität lotst. Auf Menschen, die nicht gut mit Unsicherheit und Kontrollverlust umgehen können, wirken solche Geschichten von einem großen Plan besonders attraktiv, da diese die Illusion einer vorhersehbaren Zukunft erschaffen. Hinzu kommt die Möglichkeit, sich und die eigene Gruppe mittels solcher Narrative emotional aufzuwerten – nicht umsonst erinnern Verschwörungserzählungen nur allzu oft an den Plot zweitklassiger Actionfilme, in denen Otto Normalbürger sich stolz aufmacht, die Welt vom absolut Bösen zu erlösen.

Wenn Gruppierungen zudem behaupten, Faktenchecks, seriöse Medien, Forschende bis hin zu globalen Wissensprojekten wie der Wikipedia seien Teil einer bösartigen Verschwörung, lässt sich die eigene Anhängerschaft dadurch äußerst effektiv von jeglicher Gegenrede abschirmen. Ein autoritärer Politiker kann sich dadurch die Welt geradezu ausmalen, wie es ihm gefällt – und nützlich erscheint. Einer freiheitlich demokratischen Gesellschaft wird so nach und nach der Boden unter den Füßen weggezogen. Zahlreiche Verschwörungsideologen

empören sich mit Vorliebe über die angebliche Einschränkung ihrer Meinungsfreiheit, aber innerhalb dieses Milieus wird die Bedeutung dieses Begriffs komplett verdreht. Was eigentlich ersehnt wird, ist eine Welt, in der diese Menschen keine Gegenrede mehr fürchten müssen, ohne nervige Faktenchecks, ohne Klagemöglichkeiten für Betroffene von Verleumdung, ohne journalistische Sorgfaltspflicht und Pressekodex. Passend dazu fordern nicht wenige im nächsten Atemzug übergangslos und ohne jede Scham „Nürnberger Prozesse 2.0“ für seriöse Journalist*innen.

Fakten zählen nicht mehr

Dieser Text könnte mit dem Versprechen schließen, dass mehr Medienkompetenz das Problem lösen werde. Oder mit der Hoffnung, dass wir alle wohl oder übel lernen müssen, uns angesichts hochemotionaler Postings besser im Griff zu haben, damit wir in Zukunft erst eine zweite und dritte seriöse Quelle suchen, bevor wir auf „Repost“ klicken. Wer wünscht sich nicht, dass uns das irgendwann gelingen wird. Auch mehr Geld für Bildungsarbeit in allen Altersgruppen wäre nicht verkehrt, denn dass die frühe und intensive Nutzung von digitalen Plattformen nicht zwingend mit hoher Medienkompetenz einhergehen muss, davor warnen Forschende seit Langem. So kam etwa kürzlich eine Studie der britischen Aufsichtsbehörde *Ofcom* zu dem Ergebnis, dass nur ein Drittel der befragten Jugendlichen in der Lage war, bezahlte Suchergebnisse bei Google als solche zu identifizieren. Zuversicht sieht anders aus.

Zur Wahrheit gehört die traurige Einsicht, dass uns das alles nicht retten wird. Jedenfalls nicht allein. Zu strukturell vergiftet präsentiert sich dafür die Ausgangslage. Denn wir leisten uns aktuell eine Welt, in der der reichste Mann der Welt sich nicht genötigt sieht, einen angemessenen Betrag in Content-Moderation bei X (ehemals Twitter) zu investieren, während ein von seiner Firma als PR-Gag hochgeschossener *Tesla Roadster* nach wie vor durchs Weltall schwebt. Prioritäten, I guess. Der *Meta*-Konzern hingegen, unter dessen Dach sich unter anderem Instagram, Facebook und Whatsapp versammeln, verkündete passend zum Regierungswechsel im Weißen Haus, man werde die

Kooperation mit Faktencheck-Organisationen in den USA vorerst auf Eis legen. Einen Präsidenten, der das Kunststück vollbrachte, zu Wahlkampfzeiten an einem einzigen Tag rund vierzig falsche Aussagen zu tätigen, werden derartige Schritte kaum betrüben. Mehr noch, sein Vize legte öffentlich nach, er halte Regulierungsbestrebungen vonseiten der EU für einen Angriff auf die Meinungsfreiheit.

Autoritäre Kräfte aus ganz Europa werden nicht müde, dies zu beklatschen. Das hat einen einfachen Grund. Denn Parteien, die offen die Gewaltenteilung, die Pressefreiheit und die Freiheit der Wissenschaft angreifen – und somit zentrale Errungenschaften der Aufklärung infrage stellen – ging es letztendlich nie um den Schutz der freien Rede. Was sie wollen, ist eine Welt, in der selbst die dreisteste Verdrehung weder Faktencheck noch wissenschaftliche Studien fürchten muss. Doch wenn die Lüge siegt, so viel ist sicher, befindet sich die Demokratie auf dem Rückzug. Aber womöglich ist ja dies mit der „guten alten Zeit" gemeint, nach der sich einige dieser Tage sehnen.

Katharina Nocun ist Publizistin und hat in Münster und Hamburg Politik- und Wirtschaftswissenschaften studiert. In ihrer Arbeit setzt sie sich mit dem Spannungsfeld Digitalisierung und Demokratie auseinander. Bücher: „Die Daten, die ich rief" (2018), sowie gemeinsam mit Pia Lamberty „Fake Facts" (2020), „True Facts" (2021) und „Gefährlicher Glaube" (2022).

Quellen

1 Falsche Foto-Beschreibung. Kindergartengruppe war zu Besuch bei Polizei, nicht unter Schutz, DPA Factchecking, 29.01.2025
https://dpa-factchecking.com/germany/250129-99-741857/

3

Bildung, Schule und Kinder

Birgita Dusse & Anne-Sophie Waag

Das Recht auf (digitale) Bildung

122

Das Recht auf Bildung muss im digitalen Zeitalter neu durchdacht werden. Zentrale Spannungsfelder tun sich auf zwischen digitaler Teilhabe, Datenschutz und dem Recht auf Nicht-Erreichbarkeit – für Schüler*innen ebenso wie für Lehrkräfte. Digitale Lernmittelfreiheit, die Nutzung umstrittener Plattformen, hybride Unterrichtsmodelle und die Balance zwischen pädagogischem Anspruch und technischer Realität sind nur einige Herausforderungen. Es braucht ein umfassendes Verständnis digitaler Grundrechte, das auch das Recht auf Medienbildung einschließt.

„Die GEW will die Grundrechte in der digitalisierten Welt stärken. Ziel ist ein gemeinsames Verständnis für Rechte in einem inklusiven, diskriminierungsfreien Bildungssystem."

Am Gewerkschaftstag 2021 hat die Gewerkschaft Erziehung und Wissenschaft (GEW) den Beschluss gefasst, einen Diskussionsprozess über digitale Grundrechte für Lernende und Lehrende zu starten, der zehn „digitale Grundrechte" vorschlägt. Wichtig dabei ist, dass die Grundrechte sowohl für die Lernenden als auch die Lehrkräfte an Bildungseinrichtungen gelten sollen. Ziel war, eine Debatte darüber anzustoßen, wie fundamentale und demokratische Grundrechte wie Datenschutz, Persönlichkeitsrechte, Meinungsfreiheit und Teilhabe im digitalen Zeitalter gesichert werden können.

Selbstverständlich sind diese Rechte keineswegs, denn in der alltäglichen Bildungspraxis werden die formulierten Grundrechte bei Weitem noch nicht eingehalten. Ein paar Beispiele: Sowohl Lehrkräfte als auch Schüler*innen haben ein Recht auf den Schutz der eigenen Daten und Achtung der Privatsphäre. Hier wurde mit der Datenschutz-Grundverordnung (DSGVO) der EU zwar eine gute Grundlage geschaffen, doch wer garantiert, dass die Apps, Tools und Lernmanagementsysteme, die heute an Schulen zum Einsatz kommen, wirklich datenschutzkonform sind? Häufig beruht diese Annahme auf einer Selbstauskunft der Anbieter.

Ein Projekt zur Datenschutzzertifizierung schulischer Informationssysteme DIRECTIONS soll – gefördert vom Bundesministerium für Bildung und Forschung – bis 2027 mit einer echten Datenschutzzertifizierung Abhilfe schaffen. Allein: Bis dahin sind viele Systeme schon seit Jahren in der Anwendung. Haben Eltern zum Beispiel die Wahl, wenn die Schule nicht mehr über E-Mails, sondern über die Kommunikations-App *Schoolfox* kommuniziert, die 2016 den Negativ-Preis „Big Brother Award“ bekommen hat? Kann eine Lehrkraft sich dagegen entscheiden, damit zu kommunizieren oder ein bestimmtes Videokonferenzsystem nicht zu nutzen?

2023 ging der hessische Hauptpersonalrat bis vor den Europäischen Gerichtshof (EuGH), um zu klären, ob Lehrkräfte dem Unterricht über ein Videokonferenzsystem zustimmen müssen. In der Covid-19-Pandemie war nämlich die Zustimmung von den Lehrkräften im Gegensatz zu den Schüler*innen nicht eingeholt worden. Der EuGH entschied, dass eine Zustimmung nötig ist, aber in bestimmten Fällen davon abgewichen werden kann. Das Land Hessen muss nun nachjustieren.

Das Recht auf Bildung

Im Kontext von Bildung in der digitalisierten Welt tut sich ein Spannungsbogen verschiedener Rechte und Rechtsprechungen aus, die teilweise widersprüchlich sind. Um ein Verständnis über die Zusammenhänge zu erhalten, blicken wir zunächst auf das Recht auf Bildung, wie es in der Allgemeinen Erklärung der Menschenrechte beschrieben ist, sowie auf einen Beschluss des Bundesverfassungsgerichts aus der Zeit der Covid-19-Pandemie. Im Anschluss gehen wir auf spezifische Rechte im Digitalen von Kindern, Beschäftigen, Lehrkräften und Lernenden ein und zeigen mögliche Widersprüche auf. Schlussendlich plädieren wir dafür, weniger das Recht auf digitale Bildung zu adressieren, als vielmehr den Fokus auf ein Recht auf Medienbildung zu legen und die digitalen Grundrechte von Bildungsakteur*innen zu schützen.

Das Recht auf Bildung wird im Artikel 26 der Allgemeinen Erklärung der Menschenrechte beschrieben. Dort heißt es unter anderem:

„Jeder Mensch hat das Recht auf Bildung. Die Bildung ist unentgeltlich, zum Mindesten der Grundschulunterricht und die grundlegende Bildung [...]. Die Bildung muss auf die volle Entfaltung der menschlichen Persönlichkeit und auf die Stärkung der Achtung vor den Menschenrechten und Grundfreiheiten gerichtet sein [...].“

Auch in Artikel 28 der UN-Kinderrechtskonvention wird das Recht auf Bildung, Schule und Berufsausbildung hervorgehoben, während der Artikel 29 die Bildungsziele adressiert, und dabei darauf abzielt, dass Kinder die Möglichkeit zur Entfaltung ihrer Persönlichkeit, ihrer Begabung und ihrer geistigen sowie körperlichen Fähigkeiten haben sollen.

Die Situation in Deutschland

In der Geschichte des deutschen Verfassungsrechts wurde das Recht auf Bildung erstmals im Rahmen des Beschlusses „Bundesnotbremse II“ des Bundesverfassungsgerichts vom 19. November 2021 bestätigt. Dort heißt es gleich zu Beginn:

„Aus Art. 2 Abs. 1 in Verbindung mit Art. 7 Abs. 1 GG folgt ein Recht der Kinder und Jugendlichen gegenüber dem Staat, ihre Entwicklung zu einer eigenverantwortlichen Persönlichkeit auch in der Gemeinschaft durch schulische Bildung zu unterstützen und zu fördern (Recht auf schulische Bildung).“

Bei den aufgeführten Kriterien, die sicherstellen sollen, dass dieses Recht auch umgesetzt wird, erwähnt das Bundesverfassungsgericht ein „Recht auf gleichen Zugang zu staatlichen Bildungsangeboten“. Interessant in diesem Kontext ist die bundesweit verbriefte Lernmittelfreiheit – also das Recht auf unentgeltlichen Zugang zu schulischen Lehr- und Lernmaterialien – auch wenn jedes Bundesland anders regelt, wer anspruchsberechtigt ist und wer für die Finanzierung und Organisation zuständig ist. Als Lernmittel gelten Arbeitsmaterialien, die Schüler*innen zur erfolgreichen Teilnahme am Unterricht benötigen. Dazu zählen Schulbücher und Lernmaterialien wie zum Beispiel Taschenrechner, Zirkel, Zeichengeräte, aber auch digitale Lehr- und Lernangebote.

In einem Positionspapier aus dem Jahr 2020 – also während des ersten Jahres der Covid-19-Pandemie – fordert die SPD-Fraktion im Bundestag „digitale Lernmittelfreiheit für alle“. Dabei legt sie neben der Bereitstellung von Endgeräten auch einen Fokus auf den Zugang zu freien und barrierefreien Bildungsinhalten (Open Educational Resources, OER). Mit einem Sofortprogramm stellte die Bundesregierung 2020 dann auch 500 Millionen Euro bereit, um Schüler*innen mit mobilen Endgeräten zu versorgen und Schulen eine Ausstattung zur Verfügung zu stellen, damit sie Online-Lehrmaterialien erstellen können.

Das Recht auf Bildung in der digitalen Welt

Spätestens die Covid-19-Pandemie und die oben aufgeführte Beschlussfassung des Bundesverfassungsgerichts zum Recht auf Bildung zeigen deutlich, dass dieses Recht heute im Kontext der Digitalität betrachtet werden muss. Es geht folglich um das Recht auf Bildung in einer digitalen Welt. In der formalen und institutionalisierten Bildung treffen außerdem mindestens zwei Zielgruppen aufeinander, deren Rechte beide beachtet und möglicherweise in einigen Fällen auch gegeneinander abgewogen werden müssen – auf der einen Seite die Rechte der Kinder und Jugendlichen und auf der anderen die Rechte der Beschäftigten, also der Lehrkräfte.

Kinderrechte in der digitalen Welt

Kinderrechte in der digitalen Welt bewegen sich im Spannungsfeld zwischen dem Recht auf Bildung und Information und dem Recht auf den Schutz der eigenen Daten und der Privatsphäre. Beispielhaft zeigte sich dieses Spannungsfeld während der Covid-19-Pandemie. Zeitweise konnte der Unterricht nur mittels digitaler Tools und Videokonferenzsysteme aufrechterhalten werden. Gleichzeitig stellten sich einige der eingesetzten Videokonferenzsysteme (etwa *Microsoft Teams*) und Online-Tools (zum Beispiel *Padlet*) als nicht datenschutzkonform heraus. Nicht nur in Hessen führte dies 2021 zu einer großen Kontroverse, ob der Landesdatenschutzbeauftragte berechtigt war war, die Nutzung von *Microsoft Teams* zu untersagen, oder dadurch das Lernen unter Pandemiebedingungen verunmögliche, da eine Umstellung auf datenschutzkonforme Alternativen als nicht praktikabel betrachtet wurde.

Im selben Jahr wurde die UN-Kinderrechtskonvention um eine allgemeine Bemerkung zu den Rechten von Kindern im digitalen Umfeld ergänzt. Hierzu gehören der Zugang zu Information, die Meinungs- und Informationsfreiheit, die Freiheit der Gedanken, die Vereinigungs- und Versammlungsfreiheit auch im Digitalen, die Privatsphäre (auch digitale Werkzeuge in der Bildung müssen diese schützen), das Verbot der kommerziellen Nutzung von Daten von Kindern und der Schutz vor Gewalt im digitalen Raum. In einem Bericht von *Human Rights Watch* 2022 wurden Verletzungen der Privatsphäre von Kindern während des Online-Unterrichts in der Covid-19 Pandemie auf globaler Ebene untersucht. Im Ergebnis zeigte sich, dass viele Anbieter von Bildungssoftware die Daten von Kindern zu kommerziellen Zwecken verwendet hatten.

Die Datenschutz-Grundverordnung (DSGVO) sieht vor, dass Einwilligungen zur Verarbeitung personenbezogener Daten erst für Jugendliche ab 16 rechtswirksam sind. Bis dahin sind die Eltern verantwortlich. Inwiefern betroffene Kinder, Jugendliche und Eltern jedoch eine informierte Entscheidung treffen können, bleibt fraglich und muss auch im Kontext des oben beschriebenen Spannungsfeldes betrachtet werden.

Die Rechte der Beschäftigten

Neben den beschulten Kindern und Jugendlichen sind auch die Lehrkräfte betroffen, wenn das Recht auf Bildung in der digitalen Welt diskutiert wird – und zwar auf unterschiedliche Weise.

Informationelle Selbstbestimmung und das Recht auf Nichterreichbarkeit

Beschäftigte in Lehrberufen fühlen sich durch die Digitalisierung zunehmend belastet. Das zeigt etwa die Sonderauswertung „Digitalisierung in Bildungsberufen" des DGB-Index *Gute Arbeit* von 2023, in der Menschen in Lehrberufen (an Hochschulen, Schulen und Erzieher*innen) über ihre Erfahrungen mit der Digitalisierung am Arbeitsplatz befragt wurden. Eine zentrale Herausforderung zunehmender Digitalisierung der Arbeit ist die Entgrenzung: Die Auswertung zeigt, dass digital arbeitende Menschen längere Arbeitszeiten aufweisen, mehr unbezahlte Überstunden machen und sich in Erholungszeiten stärker beeinträchtigt fühlen.

Dabei sind Lehrkräfte Pioniere mobilen Arbeitens, findet doch ein Teil der Arbeitszeit schon immer zu Hause und am Wochenende statt, vor allem die Unterrichtsvorbereitung und Korrekturen. Allerdings macht es einen großen Unterschied, ob man hierbei zusätzlich die Erwartung erfüllen muss, ständig erreichbar zu sein oder auf die letzte Chatnachricht im Klassenchat zu antworten. Deshalb bedarf es für diese Fälle klarer Abgrenzungen und Regelungen in Dienstvereinbarungen.

Dabei kommt den Personalräten eine besondere Rolle und Verantwortung zu. Bei der Einführung digitaler Arbeits- und Unterrichtstechnologien müssen gesetzliche Mitbestimmungs- und Beteiligungsrechte gewahrt werden. Arbeitszeit und Erreichbarkeit, aber auch der Datenschutz auf dienstlichen Endgeräten und E-Mail-Adressen sollte geprüft und dienstrechtlich festgehalten werden.

Dass dieses Unterfangen für Personalräte allerdings sehr voraussetzungsreich ist, schildert eindrücklich ein Bericht des stellvertretenden Landesvorsitzenden der GEW Baden-Württemberg und Digitalisierungsexperten David Warneck. Datenschutzstandards seien

vor allem bei den großen, kommerziellen Anbietern häufig schwer zu überblicken. Hier bräuchte es rechtssichere Lösungen aus öffentlicher Hand. Darüber hinaus dürften Lehrkräfte nicht dazu verpflichtet werden, biometrische Daten zu teilen (zum Beispiel durch eine Freigabe von Endgeräten durch Fingerabdruck oder Gesichtserkennung) oder das Recht am eigenen Bild aufzugeben (etwa durch Videofreigabe in Videokonferenzen). Auch führten digitale Arbeitsumgebungen dazu, dass Lehrkräfte einfacher überwacht werden könnten, zum Beispiel, indem nachvollziehbar würde, wann sie online sind oder Materialien und Korrekturen hochgeladen haben.

Das Bewusstsein für den dauerhaften Stress durch die ständige Erreichbarkeit zu schärfen, sollte auch Gegenstand des Unterrichts selbst sein. Denn Kinder und Jugendliche wachsen spätestens mit dem ersten Smartphone in einer Welt auf, die permanente Kommunikation verlangt. Kinder koordinieren sich per Klassenchat vor dem Frühstück und bis spät abends zu Schulfragen aller Art. Ein Blick ins Schulportal morgens, um zu schauen, welcher Unterricht ausfällt – ganz normal. Und so manche App trackt die Onlinezeiten der Kinder: Die in Grundschulen beliebte *Anton-App* zeigt Lehrkräften an, zu welcher Uhrzeit die Kinder wie lange welche Aufgaben bearbeitet oder eben nicht bearbeitet haben. Wenn wir über digitale Grundrechte von Lernenden und Lehrkräften sprechen, gehört das Recht auf Nichterreichbarkeit dazu.

Sollte es ein Recht auf Hybrid- / Onlineunterricht geben?

Während der Covid-19-Pandemie kam die Forderung nach einem Recht auf Hybridunterricht auf. Ein Bündnis aus dem Verband der Digitalwirtschaft *Bitkom*, der Bundesschülerkonferenz und dem Bundeselternrat veröffentlichte im Frühjahr 2022 ein Papier, das ein Recht auf digitale Bildung fordert. Damit sollen Chancengleichheit und Inklusion gefördert werden. Das Papier wurde mit Zahlen aus einer vom *Bitkom* in Auftrag gegebenen Umfrage unterfüttert.

Die GEW sieht das Forderungspapier kritisch. Ein Recht auf Hybridunterricht würde Lehrkräfte und Schulen vor große Herausforderungen stellen und fordert zugleich das Recht der Lehrkräfte auf informationelle Selbstbestimmung heraus. Für Schüler*innen, die längerfristig ausfallen, ist es natürlich wünschenswert, digital unterstützte Lösungen zu finden. Ein generell einklagbares Recht auf Hybridunterricht würde

jedoch unter den aktuellen Arbeitsbedingungen zu einer nicht absehbaren Mehrbelastung von Lehrkräften führen. Lehrkräfte müssen in hybriden Unterrichtssituationen zwei Settings bespielen und den verschiedenen Bedürfnissen der Schüler*innen online und vor Ort gerecht werden.

Der Hybridunterricht wird aber auch abseits der Covid-19-Pandemie als mögliche Lösung für den akuten Lehrkräftemangel diskutiert: Der Freistaat Sachsen startete 2022 ein Modellprojekt zum Hybridunterricht und auch im benachbarten Thüringen wurde über ähnliche Maßnahmen nachgedacht. Auch diese Vorstöße sieht die Bildungsgewerkschaft GEW kritisch und kommentierte dementsprechend nicht nur ein Modellprojekt zu Blended Learning an berufsbildenden Schulen in Sachsen-Anhalt, sondern auch das Gutachten der Ständigen Wissenschaftlichen Kommission der Kultusministerkonferenz zum Lehrkräftemangel, in dem als eine Lösung auch der Hybridunterricht vorgeschlagen wurde.

Auch wenn Gewerkschaften eine wohnortnahe Beschulung von Auszubildenden sehr begrüßen – was im Falle von Blended Learning möglich wäre – sehen sie durchaus einige Herausforderungen. Zum einen müsste im Berufsbildungsgesetz (BBiG) neben der Schule und dem Betrieb der häusliche Wohnort als weiterer Lernort abgebildet werden. Damit einhergehend stellten sich Folgefragen nach der geeigneten Ausstattung für die digitale Arbeit zu Hause, einer möglichen Bezuschussung von Internetkosten und nach allgemeinen Schutz- und Qualitätsmaßnahmen. Aufseiten der Lehrkräfte bestehen gleichzeitig Bedenken, dass sie fortan Unterricht nicht nur für rein analoge oder rein digitale Settings, sondern hybride Settings gestalten müssen, in denen ein Teil der Schüler*innen vor Ort und der andere Teil digital zugeschaltet ist. Insbesondere hybride Settings erhöhen den Vorbereitungsaufwand massiv und wären keine Entlastung bei bestehendem Lehrkräftemangel.

Das Recht auf Medienbildung

Statt ein Recht auf digitale Bildung zu fordern, was mit verschiedenen Herausforderungen und Widersprüchen einhergeht, die in diesem Artikel ausgeführt wurden, schlagen wir in Anlehnung an die GEW-„Offensive für mehr kritische Medienkompetenz“ ein Recht auf Medienbildung vor.

Hierbei geht es weniger darum, dass Lernende zu jeder Zeit ein digitales Angebot erhalten müssen. Stattdessen muss gewährleistet werden, dass Lernende sowie Lehrkräfte Medienbildung erfahren. Diese Forderung greift deutlich weiter, da es um den kompetenten, kritischen und mündigen Umgang mit Medien im Allgemeinen geht. Dies impliziert die praktische Auseinandersetzung mit digitalen Medien, setzt den Schwerpunkt allerdings auf die Reflexion darüber. Es geht nicht nur um das Erlernen digitaler Kompetenzen und Fähigkeiten, sondern um die Entwicklung eines grundlegenden Verständnisses darüber, wie digitale Medien funktionieren und gesellschaftlich wirken.

Die im November 2024 erschienene *ICILS-Studie 2023* zu IT- und Medienkompetenzen von Achtklässler*innen („International Computer and Information Literacy Study“) untersucht seit 2013 alle fünf Jahre die computer- und informationsbezogenen Kompetenzen von Schülerinnen und Schülern der 8. Jahrgangsstufe im internationalen Vergleich. Zu den digitalen Kompetenzen gehört zum Beispiel die Fähigkeit, digitale Geräte zu bedienen, Informationen im Internet zu suchen, auszuwerten und zielgerichtet zu nutzen, aber auch die Fähigkeit, Probleme logisch zu analysieren und in lösbare Teilschritte zu zerlegen. In der 2023-er-Studie zeigte sich ein starker Negativtrend bei der Medienkompetenz von Schüler*innen in Deutschland, da die mittlere erreichte Punktzahl im Vergleich zu den Studien von 2013 und 2018 statistisch signifikant zurückgegangen ist.

Die Studie verdeutlicht, dass die Stärkung der Medienbildung neben der technischen Ausstattung und Infrastruktur eine zentrale Voraussetzung für die Teilhabe und Partizipation in der digitalen Welt ist. Um die Medienkompetenz in der schulischen, außerschulischen Bildung und Hochschule zu vermitteln, bedarf es geeigneter Aus-, Fort- und Weiterbildungsmaßnahmen für Lehrkräfte in den Bildungseinrichtungen,

wie sie etwa mit dem Konzept der Grundbildung Medien für pädagogische Fachkräfte bereits 2011 von Horst Niesyto vorgeschlagen wurden. Bislang steht Deutschland hier immer noch am Anfang. Eine entsprechende Grundbildung in der Lehrkräfteausbildung ist nicht flächendeckend vorhanden, und in den Curricula ist die Medienbildung nicht in allen Bundesländern klar verankert. Wir bleiben daher dabei und wiederholen unseren Aufruf für eine Offensive für mehr Medienkompetenz!

Zwischen Recht auf Bildung und Schutz der Grundrechte

Es ist nachvollziehbar, wenn nach den Erfahrungen der Covid-19-Pandemie und der heutigen digitalisierten Welt für den Bildungsbereich ein Recht auf Bildung gefordert wird. Bei genauerer Betrachtung der verschiedenen damit zusammenhängenden Aspekte zeigt sich jedoch, dass eine solche Forderung allein zu kurz greift. Der Miteinbezug der verschiedenen Perspektiven der beteiligten Akteursgruppen zeigt Widersprüche auf. Sie changieren zwischen einem Recht auf schulische Bildung – auch in digitalen Lehr- und Lernsettings – dem Schutz der Grundrechte im digitalen Raum und einem Anrecht auf Dienstvereinbarungen mit klaren Grenzen der Erreichbarkeit und Erholungsphasen.

Um diese teils gegensätzlichen Bedürfnisse und Rechte miteinander in Einklang zu bringen, braucht es die frühzeitige Einbindung der betroffenen Gruppen und ihrer Vertretungen. Gemeinsam können dann geeignete Rahmenbedingungen und Regelungen ausgehandelt werden, die möglichst allen zugutekommen.

Dr. Birgita Dusse ist Politikwissenschaftlerin, Historikerin und Italianistin. Sie arbeitet als Referentin im Hauptvorstand der Gewerkschaft Erziehung und Wissenschaft und ist dort für den Arbeitsschwerpunkt „Bildung in der digitalen Welt“ zuständig. Nebenberuflich ist sie Dozentin an der Europäischen Akademie der Arbeit und hat viele Jahre Erfahrung in der Jugendbildungsarbeit, Erwachsenenbildung, Hochschullehre sowie Forschung.

Dr. Anne-Sophie Waag ist Bildungspsychologin. Bei Wikimedia Deutschland e. V. setzt sie sich als Referentin Bildungspolitik für Chancengleichheit beim Zugang zu Wissen und Bildung ein. Zentrale Ziele sind die rechtliche und strukturelle Verankerung der Prinzipien freier, offener Bildung im Bildungssystem und die gemeinwohlorientierte Ausrichtung digitaler Bildungsinfrastrukturen und -technologien.

Nina Galla

KI kann Schulen (noch) nicht entlasten

Künstliche Intelligenz (KI) in der Schule hat eine steile Karriere hingelegt – Anfang 2025 haben sehr viele Schulen KI-Systeme im Einsatz, die meisten Bundesländer haben sogar Landeslizenzen für spezielle Schul-KI eingekauft. Millionen Euro fließen dabei an privatwirtschaftliche Anbieter, weitere Millionen in das länderübergreifende Projekt *Adaptive Intelligente Systeme* (AIS) zur eigenen Entwicklung von KI-Werkzeugen für den Unterricht.

In der Praxis werden mithilfe von ChatGPT Hausarbeiten verfasst – zum Teil ist der Text-Generator sogar bei Klassenarbeiten zugelassen – Start-ups haben KI-Anwendungen entwickelt, mit denen Textarbeiten von Schüler*innen automatisiert auf Verbesserungspotenziale geprüft werden, KI kann Feedback geben und Vorschläge für Noten unterbreiten und Lehrkräfte darin unterstützen, Unterrichtsmaterial zu erstellen oder Schulstunden zu planen. Das Entlastungspotenzial scheint auf der Hand zu liegen. Sogar die Bildungsgerechtigkeit soll steigen, wenn KI-Systeme für jede Schülerin und jeden Schüler eigene Lernpfade berechnen.

Diese Investitionen von Bund und Ländern erwecken den Eindruck, als wolle Deutschland diesmal nicht den Anschluss an den digitalen Fortschritt verpassen – selbst wenn der pädagogische Nutzen und die Rechtssicherheit der Anwendungen nach wie vor fragwürdig sind. In der Debatte um KI in der Bildung müssen aktuelle und langfristige Risiken betrachtet werden: Wenn Bildung durch datenbasierte Berechnungs- und Analyseverfahren mithilfe von KI zunehmend automatisiert, systematisiert und formalisiert wird, gehen nicht nur soziales Lernen, Individualität und Kreativität von Einzelnen verloren, sondern Heranwachsende verlieren insgesamt den Bezug zu Gemeinsinn und Vielfalt – und das ist eine hochaktuelle Bedrohung von Demokratien weltweit.

Fehlentscheidungen und Diskriminierung durch Daten

Mit KI ziehen fundamentale Probleme und Risiken in die Klassenzimmer ein, die in der öffentlichen Debatte um Chancen und Innovationen zu wenig Beachtung finden. Das liegt an der Beschaffenheit von KI-Systemen, die sich von bisher bekannten, statischen Digitalprodukten unterscheiden. Systeme des maschinellen Lernens entwickeln sich während der Nutzung weiter und verändern möglicherweise mit der Zeit die Wege zur Ergebnisfindung, was für Lehrkräfte nur schwer oder erst spät erkennbar ist. Denn automatisierte oder KI-basierte Verfahren sind aufgrund ihrer Komplexität selbst für erfahrene Entwickler oft gar nicht oder nur schwer nachvollziehbar. KI-Systeme werden im Gegensatz zu Schulbüchern außerdem (noch) nicht von den Kultusministerien geprüft. Das bedeutet, dass nicht sichergestellt ist, dass KI-Systeme in der Schule stets so funktionieren, wie es erwartet und gewünscht ist.

Ein weiteres KI-immanentes Problem ist die Diskriminierung von unterrepräsentierten Menschengruppen. Da KI-Systeme immer auf Basis der Daten operieren, die dem System zugeführt oder zugänglich gemacht wurden, ist die Entscheidungsbasis für ein KI-System niemals neutral, da diese Daten nie vollständig die Realität abbilden können. Es kam aufgrund dieser unvollständigen Datenlage in anderen Anwendungsbereichen, wie zum Beispiel bei der Polizeiarbeit oder in Bewerbungsverfahren, bereits zu diskriminierenden Fehlentscheidungen zum Nachteil von Schwarzen Menschen und People of Color oder Frauen.

Diskriminierung durch KI kann auch im Bildungsbereich auftreten, wenn beispielsweise Schüler*innen aufgrund von nicht leistungsbezogenen Faktoren unterschiedliche Aufgaben zugewiesen werden. Wenn das KI-System nur die Leistungsdaten auswertet und einen Leistungsabfall ableitet, kann es nicht den Kontext betrachten, etwa, dass ein*e Schüler*in wegen eines Krankheitsfalls in der Familie vorübergehend mehr auf Geschwister aufpassen muss. KI-Systeme zeigen Korrelationen auf, ohne Kausalitäten zu berücksichtigen. Eine menschliche Lehrkraft hingegen könnte diesen Kontext kennen, würde begreifen, dass es sich um eine vorübergehende Zusatzbelastung handelt und folglich nicht an der grundsätzlichen Fähigkeit des Kindes zweifeln.

Diskriminierung durch KI-Systeme wird – ähnlich wie die fehlende Nachvollziehbarkeit von vielen automatisierten Prozessen – entweder nur sehr schwer oder gar nicht zu beheben sein. Bildungsgerechtigkeit wird dadurch eher verhindert als ermöglicht.

Was KI (nicht) kann – und warum das ein Problem ist

Es bleibt noch die Eigenschaft von KI-Systemen, dass sie kein Wissen reproduzieren oder gar schaffen, sondern mithilfe von statistischen Verfahren Ausgaben berechnen. Generative KI-Anwendungen sind bekannt für ihre „Fehler" und keinesfalls als Ersatz für Suchmaschinen tauglich – KI-generierte Informationen müssen immer mithilfe von anderen gesicherten Quellen überprüft werden.

Ergebnisse von KI-Anwendungen sind außerdem nicht reproduzierbar: Ein Test des Systems *Fobizz*, eines der bekanntesten KI-Systeme für Feedback und Bewertungen von Schüler*innenleistungen, ergab, dass das System für die gleiche Arbeit bei jedem Bewertungsvorgang verschiedene Noten vorschlägt – es kann also nicht von einer objektiven und gesicherten Bewertung ausgegangen werden, die die fachliche Einschätzung einer Lehrkraft ersetzt oder auch nur unterstützen kann.

KI in der Bildung wird zwar noch nicht so lange in der Praxis eingesetzt, Forschung dazu gibt es jedoch schon viel länger. Aber trotz jahrelanger Forschung und Beobachtungen in der Praxis kann der pädagogische Nutzen von KI-Anwendungen zum Lernen nicht nachgewiesen werden. Es gibt zwar einzelne Untersuchungen, die Lernfortschritte nach KI-Einsatz zeigen, jedoch erwähnen auch diese Studien, dass es noch Forschungsbedarf gibt. Die Studiendesigns legen nahe, dass die Erfolge entweder nicht nachhaltig oder repräsentativ sind, oder auf Faktoren zurückgeführt werden können, die mit KI nichts zu tun haben. Auch bei vielen Lern-Apps (ob mit oder ohne KI) ist überhaupt nicht messbar, ob überhaupt ein Lernprozess stattgefunden hat.

Medienkompetenz für Lehrkräfte und Lernende soll dabei helfen, grundsätzlich mit KI-Systemen und ihren Grenzen und Lücken

umzugehen. Es sollte dabei auch Fehlertoleranz gegenüber der Technologie, die im Alltag der meisten Menschen immer öfter vorkommt, entwickelt werden – falsche Hauptstädte in Schulbüchern oder erfundene historische Gegebenheiten, die Lehrkräfte herbeifantasieren, dürfen jedoch nicht akzeptiert werden. Fehlerhafte Technologie ist im Klassenzimmer genauso inakzeptabel wie Fehler in Schulbüchern. In Zeiten von Falsch- und Desinformation sollten Kinder nicht daran gewöhnt werden, dass es im digitalen Raum ganz normal ist, wenn mal etwas nicht ganz stimmt.

Nicht zuletzt ist da noch die immense Belastung für Menschen und Klima, was ein Thema für sich ist. Das Training von KI-Systemen und ihre Nutzung verbrauchen riesige Mengen an Energie und Wasser. Das Training der Systeme und die Contentmoderation, also die Bereinigung von Gewaltinhalten, wird oft in Niedriglohnländer des globalen Südens ausgelagert – mit unabsehbaren psychischen Folgen für die Beschäftigten und ihre Familien.

Die Rechtslage: KI-Verordnung, DSGVO und Schulgesetze

Ebenfalls vernachlässigt wird die Aufklärung zu den rechtlichen Herausforderungen, die auf Lehrkräfte und Schulleitungen zukommen werden.

Relevant für den Einsatz von KI an Schulen sind die neue KI-Verordnung der EU, die Datenschutz-Grundverordnung (DSGVO) und Schulgesetze der Bundesländer. Die KI-Verordnung klassifiziert Anwendungen im Bildungskontext als sogenannte Hochrisiko-Systeme. Dazu gehören Systeme, die bei der Zulassung zu Bildungseinrichtungen zum Einsatz kommen, bei der Bewertung und der Steuerung von Lernprozessen und der Überwachung bei Prüfungen. Für diese Systeme sieht die KI-Verordnung einen umfangreichen Anforderungskatalog für die Firmen vor, die solche Systeme anbieten. Werden diese Pflichten verletzt, drohen Bußgelder.

Aber auch für die Betreibenden von Hochrisiko-Systemen gibt es Pflichten und auch ihnen drohen Bußgelder. Wer im vielschichtigen Bildungswesen die oder der Betreibende einer KI-Anwendung im Sinne der KI-Verordnung ist, ist jedoch nicht geklärt – ist es das Bundesland, das das System beschafft, die Schule oder gar die einzelne Lehrkraft? Erschwerend kommt hinzu, dass sich die Rollen mit allen zugehörigen Pflichten ändern können: Wenn beispielsweise eine Schule ein nicht für Bildungszwecke gedachtes KI-Mehrzweck-System (wie beispielsweise einen Textgenerator) selbstständig so anpasst und trainiert, dass es zu einer Bildungsanwendung wird, könnte die Schule dadurch zu einer Anbieterin einer Schul-KI-Anwendung werden – und damit zu einer Anbieterin eines Hochrisiko-Systems mit allen umfangreichen Pflichten aus der KI-Verordnung. Die Schwelle (was muss passieren, damit diese Zweckänderung eintritt?) und die Transparenz (wann erfährt die einsetzende Person oder Einrichtung, dass sie verantwortlich für die Pflichten aus der KI-Verordnung ist?) sind ebenfalls ungeklärt.

Seit Februar 2025 sind laut der KI-Verordnung einige KI-Anwendungen verboten. Dazu gehören Anwendungen, die Emotionen und unter bestimmten Bedingungen auch biometrische Erkennungsverfahren erkennen können sollen. Zu biometrischen Daten gehören sowohl körperliche Merkmale wie Gesicht, Augen und Fingerabdrücke, aber auch Verhaltensmerkmale wie Bewegungsmuster und unkontrollierbare körperliche Funktionen wie der Puls. Die von Sicherheitsbehörden immer wieder geforderte Gesichtserkennung gehört zum Beispiel zu den biometrischen Erkennungsverfahren. Im Bildungskontext können dies Systeme sein, mit denen Augenbewegungen von Lernenden beim Lesen verfolgt werden oder die Veränderung von Körpertemperatur als Hinweis auf Stress beim Lernen.

Die Verbote sind sinnvoll, denn der Einsatz von Überwachungstechnologien zur Verhaltensanalyse von Schüler*innen kann die Privatsphäre verletzen oder eine mehr oder weniger bewusste Verhaltenssteuerung erzeugen – der sogenannte *chilling effect* sorgt dafür, dass Schüler*innen sich in ihrem Verhalten einschränken und auch legitime Bedürfnisse und Ansprüche nicht mehr äußern.

Leider lässt die KI-Verordnung zahlreiche Unklarheiten und Ausnahmen zu. Zum Beispiel kann die Emotionserkennung aus medizinischen Gründen oder Sicherheitsgründen doch eingesetzt werden. In den USA ist es bereits zu Situationen gekommen, in denen Chats

von Schüler*innen überwacht wurden, um Suizide zu verhindern. Leider nicht immer erfolgreich: So kam es zu Fehlalarmen, die Eltern unnötig erschreckt haben. Eine gefährdete Schülerin hatte den Schulchat einfach gemieden und konnte dann trotz KI-basierter Erkennungsverfahren nicht gerettet werden.

Das Verbot von biometrischer Echtzeit-Fernidentifizierung (so wird das Verfahren der Gesichtserkennung in der juristischen Fachsprache genannt) gilt nur in öffentlich zugänglichen Räumen (die Schule gehört nicht dazu) und zu Strafverfolgungszwecken (wiederum mit einigen Ausnahmen). Die KI-Verordnung lässt zwar zu, dass die Mitgliedsstaaten die biometrische Fernerkennung strenger regeln, jedoch nur im Bereich der Strafverfolgung. Die Datenschutz-Grundverordnung erlaubt jedoch auch strengere Regelungen für biometrische Erkennung. Die deutsche Bundesregierung sollte dringend für ein ausnahmsloses Verbot von automatisierten biometrischen Erkennungsverfahren in öffentlichen und privaten Räumen sorgen, damit auch Schulen und digitale Räume erfasst werden.

Die DSGVO schreibt außerdem vor, dass immer eine menschliche Letztentscheidung gewährleistet sein muss, sofern eine ausschließlich automatisierte Datenverarbeitung für die Betroffenen eine rechtliche Wirkung entfaltet. Das klingt schützend, vernachlässigt jedoch den Umstand, dass viele KI-Anwendungen nicht vollautomatisch sind. Die DSGVO hinterlässt also eine Lücke bei teilautomatisierten Prozessen, die unterstützend wirken sollen.

Diese Lücke schließt nun die KI-Verordnung mit ihren Pflichten für Hochrisiko-Systeme. Somit sind Lehrkräfte in jedem Fall verpflichtet, KI-Ergebnisse zu überprüfen, sofern diese beispielsweise Einfluss auf die Bewertung von Lernenden haben. Das erhöht zwar die Sicherheit der Entscheidungsgüte, aber die zeitliche Entlastung ist zweifelhaft, wenn eine Lehrkraft sowohl die Leistung der lernenden Person als auch die Korrektur- oder Bewertungsvorschläge der KI überprüfen muss. Der sogenannte menschliche Letztentscheid bei der Bewertung von Lernleistungen ignoriert jedoch den *automation bias*, also die Neigung von Menschen, einer computergenerierten Entscheidung oder Entscheidungsvorlage eher zu folgen, als sie infrage zu stellen.

Noch einmal zurück zur DSGVO: Die von Anbietern oft beworbene DSGVO-Konformität eines Systems ist übrigens keine Garantie dafür, dass Schüler*innendaten wirklich beim Anbieter verbleiben. Denn

die DSGVO erlaubt es durchaus, dass Daten weitergegeben werden – sofern die Nutzenden zustimmen. Das Lesen der Geschäftsbedingungen und Datenschutz-Erklärungen vor dem Zustimmungsklick bleibt einem also nicht erspart. So setzt *fobizz* beispielsweise die US-Anbieter Google und Meta für Analysezwecke ein und die Feedback-App *fiete* bindet das ebenfalls US-amerikanische Produkt ChatGPT ein. Das Datenschutzniveau in den USA ist jedoch viel niedriger als in Europa. Es bleibt in der Folge nur, darauf zu hoffen, dass personenbezogene Daten nicht abfließen.

Eine preisgekrönte Recherche von *Netzpolitik.org* hat vergangenes Jahr gezeigt, wie Datenhandel trotz der DSGVO funktioniert und dass die Daten von Kindern und Jugendlichen lukrativ sind. Sie verdienen jedoch einen ganz besonderen Schutz, da sich Heranwachsende noch in der Entwicklungsphase der eigenen Meinungsbildung befinden und die Persönlichkeit – und infolge dessen auch die Meinung – starken Schwankungen unterworfen ist. Sie kann auf Basis von Nutzungsdaten nicht zuverlässig automatisiert abgebildet werden. Automatisiert erstellte Profile auf Basis von Nutzungsdaten Minderjähriger dürfen keine Rolle bei späteren Lebensentscheidungen wie zum Beispiel bei der Jobsuche spielen.

Ergänzend zu KI-Verordnung und DSGVO gelten Schulgesetze, die zumindest in Berlin vorsehen, dass Lehrkräfte die Kriterien der Leistungsbeurteilung und die der Unterrichtsplanung erklären können müssen. Die KI-Verordnung schreibt ergänzend das Recht fest, zu erfahren, welchen Anteil ein KI-System an einer Entscheidung hat. Fließt eine KI-basierte Bewertung in die Note ein, kann dies aufgrund der beschriebenen Problematik, dass automatisierte Verfahren meist gar nicht oder nur in Teilen nachvollziehbar sind, zu Konflikten mit Eltern führen.

Trotz mehrerer Gesetze ist die Rechtssicherheit sowohl für Anbietende als auch für Betreibende und Betroffene undurchsichtig, ungeklärt und lückenhaft. Ob es unter diesen Umständen zu einer Entlastung von Lehrkräften durch KI kommt, ist mehr als fraglich.

Was wir stattdessen brauchen: menschliche Bildungspolitik

Vorab: Unbestritten ist insgesamt, dass KI als Lerninhalt in die Lehrpläne gehört. Sowohl für Lehrkräfte als auch Schüler*innen ist es unverzichtbar, Grundkenntnisse über Aufbau, Chancen und Risiken sowie soziale Auswirkungen von KI-Systemen zu haben, um sich mit KI in allen Bereichen des Alltags auseinandersetzen zu können.

Bevor jedoch ein (womöglich kostenintensives) KI-System beschafft wird, sollte sich jede Organisation fragen, welches Problem denn überhaupt gelöst werden muss und ob die Problemlösung tatsächlich die Analyse von riesigen Datensätzen erfordert.

Im Bildungswesen sind die Probleme hinlänglich bekannt: Es fehlt überall an Geld, Lehrkräften und multiprofessionellen Teams. Diese Probleme können nicht dadurch gelöst werden, dass das Lernverhalten von Schülerinnen und Schülern mit KI analysiert wird. Auf keinen Fall dürfen Regierungen aufhören, in die Ausbildung und Gewinnung von Lehrkräften zu investieren – jeder Euro für ein KI-System fehlt an anderer Stelle im Bildungshaushalt.

Um eventuelle Chancen von KI im Bildungswesen tatsächlich nachhaltig zu nutzen, müssen noch mehrere Voraussetzungen erfüllt sein:

- Anbieter von KI-Systemen müssen Nutzenden und Forschenden Zugang zu ihren Entwicklungs- und Trainingsbedingungen gewähren und aktiv daran mitwirken, dass KI so nachvollziehbar wie möglich wird.
- KI muss ökologisch und sozial nachhaltig werden; der Nutzen für pädagogische Zwecke wissenschaftlich bewiesen sein.
- Es braucht Prüf- und Zulassungsverfahren für schulische KI-Anwendungen durch befähigte und unabhängige Aufsichtseinrichtungen.
- Es muss Rechtssicherheit für alle Beteiligten hergestellt sein.

Aktuell liegen die Potenziale von KI im Bildungswesen woanders. Anstelle die personenbezogenen Daten minderjähriger Schüler*innen für fragwürdige und unbewiesene Optimierungen von Lernleistungen zu nutzen, könnten nicht personenbezogene offene Daten genutzt werden, um die systemischen Ebenen des Bildungswesens zu analysieren und zu optimieren, zum Beispiel, um Lehrkräftebedarfe besser zu berechnen oder Finanzmittel des Bundes gerechter auf die Länder zu verteilen. Vielleicht besteht die eigentliche Chance von KI in der Bildung ja darin, den Lehrberuf wieder attraktiv zu machen, um ausreichende Unterrichtsversorgung und individuelle Beziehungen zwischen Lehrkräften und Schüler*innen zu ermöglichen. Entlastungen und Bildungsgerechtigkeit können nämlich eher durch Menschen als durch teure und fehlerhafte Technologie erreicht werden.

Nina Galla ist heute Pressesprecherin bei AlgorithmWatch. Zuvor hat sie fünf Jahre lang als Referentin und wissenschaftliche Mitarbeiterin für KI im Deutschen Bundestag gearbeitet und unter anderem in der Enquete-Kommission KI mitgewirkt. Mit ihrer Berufserfahrung in der digitalen Bildung vernetzt sie die Themen KI und Bildung seit 2019 regelmäßig als Autorin und Speakerin.

Zum Weiterlesen

• Rainer Muehlhoff, Marte Henningsen: Chatbots im Schulunterricht: Wir testen das Fobizz-Tool zur automatischen Bewertung von Hausaufgaben, 2024: https://arxiv.org/abs/2412.06651
• Sigrid Hartong/André Renz (Hg.): Digitale Lerntechnologien. Von der Mystifizierung zur reflektierten Gestaltung von EdTech, transcript Verlag, Bielefeld 2024: https://www.transcript-verlag.de/978-3-8376-6893-3/digitale-lerntechnologien/?c=313032838&number=978-3-8394-6893-7
• Leitfaden „Automatisierte Lernsysteme und KI-Anwendungen an Schulen“, GEW 2023: https://www.gew.de/fileadmin/media/publikationen/hv/Bildung-digital/230731-Leitfaden-ADM-KI-Schule-final.pdf

David Rott

Drei Fragen zu Kinder-rechten im digitalen Raum

Warum brauchen Kinder im digitalen Raum besonderen Schutz – und worin bestehen die größten Gefahren?

Mit Kindern sind im Sinne der UN-Kinderrechtskonvention alle Menschen zwischen 0 und 18 Jahren gemeint. Sie bewegen sich ab dem Grundschulalter in wachsendem Ausmaß im Netz. Sie nutzen das Internet, um Informationen zu gewinnen, zu spielen, Lernhilfen zu bekommen oder um sich mit anderen auszutauschen. Es bietet viele Möglichkeiten, birgt aber auch Gefahren.

Die UN-Kinderrechtskonvention ist eine Ausdifferenzierung der Allgemeinen Erklärung der Menschenrechte und nimmt besonders die Gruppe der Menschen unter 18 Jahren in den Blick. Die UN-Kinderrechtskonvention umfasst drei Rechtsbereiche: Schutz, Förderung und Partizipation. Grundlegend ist das sogenannte Kindeswohl. Damit sind die Dinge gemeint, die Kindern helfen, sich gut entwickeln zu können. Im Sinne der Beteiligung der Kinder geht es vor allem auch darum, zu fragen, was sie selbst brauchen. Es sind also nicht nur die Erwachsenen, die hier entscheiden. Deutschland hat die Konvention ratifiziert und muss sie deshalb in geltendes Recht überführen.

Das heißt, Kinder müssen Schutz erfahren. Aber sie müssen auch selbstbestimmt in der Lage sein, gute Entscheidungen zu treffen. Personalisierte Werbung oder Kostenfallen in Spielen sind ebenso problematisch wie die unreflektierte Nutzung von KI-Chatbots und das Freigeben von persönlichen Daten. Das Recht auf die Privatsphäre ist im Netz bedroht und die freie Meinungsbildung und -äußerung kann durch die Algorithmen eingeschränkt sein. Kinder können von anderen Menschen ausgebeutet werden, etwa wenn sie Videos, Bilder oder Informationen an Fremde weitergeben.

Allerdings kann ich schon allein wegen der Altersspanne – 0 bis 18 Jahre – keine allgemeingültige Antwort geben. Aber es gibt Aspekte, die für Kinder besonders relevant sind.

Das Internet ist voll von allem, was man sich nur vorstellen kann – im Guten und im Schlechten. Positiv ist zum Beispiel, dass Informationen schnell verfügbar sind und beim Lernen helfen; der Austausch mit Menschen, die an anderen Orten leben als man selbst; oder Kaufangebote, die es nur im Netz gibt oder die jedenfalls am Wohnort schwer zu bekommen sind.

Es gibt aber auch negative Aspekte. Informationen, die man im Internet findet, können falsch sein und manipulierend wirken. Aktuell sehen wir das etwa mit Blick auf den Ukraine-Krieg. Einige werden sich an die vielen Fehlinformationen rund um die Corona-Pandemie erinnern. Fake News sind oft schwer zu erkennen, da mithilfe von künstlicher Intelligenz Fotos, Videos oder Tonaufnahmen gefälscht werden können, die erstaunlich echt wirken. Hinzu kommen die Algorithmen, die die Anzeige von Informationen steuern. Welche Nachrichten wir wann angezeigt bekommen, entscheiden wir nicht selbst, sondern die Filter, die hinter den Suchmaschinen und Angeboten liegen.

Die Möglichkeiten zum Austausch werden nicht nur für freundliche Dinge genutzt: Mobbing im Klassenchat etwa oder Grooming in sozialen Netzwerken, wenn Menschen versuchen, Informationen, Videos und Fotos von Kindern zu bekommen, die sie nichts angehen. Denn ein falsches Profil in sozialen Netzwerken zu erstellen, ist nicht sonderlich schwer. Da wird aus Friedrich, 43 Jahre alt, vielleicht die vierzehnjährige Fine, die zunächst ganz nett wirkt.

Auch die Kaufangebote sind oft verlockend. Im Online-Spiel braucht man unbedingt ein Item, um den nächsten Gegner zu besiegen. Und das kostet Geld. Je nachdem, wie offen oder begrenzt die Zugänge sind, kaufen vor allem Jugendliche Dinge, die sie sich vielleicht nicht leisten können. Und dann kommen sie in Schwierigkeiten, wenn sie die Rechnungen oder Abos nicht begleichen können.

Was können Eltern, Schulen und Politik konkret tun, um Kinderrechte auch online zu sichern?

Erwachsene tragen im Sinne der Kinderrechtskonvention Verantwortung. Sie müssen den Kindern ermöglichen, ihre Rechte wahrzunehmen, einen schützenden Rahmen geben und helfen, dass die Kinder verstehen, was im digitalen Raum passiert.

Erziehungsberechtigte müssen mit ihren Kindern überlegen, wann welche Endgeräte (Handy, Tablet, Laptop) und welche Apps sinnvoll sind. Die Altersangaben der Apps und die Schutzeinstellungen sind nicht nur ein Ärgernis („Alle in meiner Klasse haben Whatsapp, nur ich nicht!“), sondern erfüllen wichtige Schutzfunktionen.

Das gemeinsame Sprechen über die Erfahrungen im Internet ist wichtig. Nur so verstehen Erziehungsberechtigte, was Kinder interessiert und bewegt. So können sie helfen, dass sich die Kinder gut zurechtfinden.

In der Schule sind die Möglichkeiten mannigfaltig. Lehrpersonen müssen den Schüler*innen helfen, Informationsrecherchen gut zu organisieren. Das fängt bei der Nutzung von Suchmaschinen an und geht beim Prompting von künstlicher Intelligenz weiter. Um die Hintergründe zu verstehen, braucht es Fachwissen: Was sind Algorithmen? Wie funktioniert ein Large-Language-Modell? Ist künstliche Intelligenz wirklich intelligent? Das ist Wissen, das auch schon in der Grundschule aufgebaut werden kann. Die Schule ist der Ort, um in abgesteckten Bereichen sicher Erfahrungen zu machen.

Die Rahmenbedingungen müssen klar geregelt sein. Das ist die Aufgabe der Politik. Sie werden innerhalb der Gesellschaft ausgehandelt, wie etwa bei der Frage, ob Mobiltelefone in der Schule erlaubt sein dürfen. Die Antworten sind komplex. Auch hier können Kinderrechte einen Orientierungsrahmen geben: Kinder brauchen Schutz, etwa durch effektive Beschränkungen von pornografischen Inhalten. Kinder brauchen Förderung – und hierfür müssen Mittel bereitstehen,

um Angebote aufzubauen. Kinder müssen sich beteiligen können und dürfen aus dem digitalen Raum nicht ausgeschlossen werden. Vielmehr ist zu klären, wie Beteiligungsmöglichkeiten sichergestellt werden können, etwa durch kindgerechte Apps, die auch politisch gefördert werden können.

Es ist wichtig, dass Erwachsene Kinder als Subjekte im digitalen Raum ernst- und wahrnehmen. Vorschriften zu machen, erscheint zwar leicht, ist aber nur begrenzt sinnvoll. Denn Kinder sollen aktive, selbstbestimmte Nutzende werden. Das gelingt nur, wenn sie Verantwortung übernehmen müssen und Gelegenheit haben, sich auszuprobieren.

Wie können Kinder selbst dabei unterstützt werden, ihre Rechte in digitalen Räumen zu verstehen und zu nutzen?

Kinder müssen in das Netz – wie auch in andere Bereiche – hineinsozialisiert werden. Dies soll eng begleitet werden (durch Erziehungsberechtigte oder Lehrpersonen). Oftmals erfolgen das Kennenlernen und Ausprobieren aber mit Gleichaltrigen. Für beide Bereiche – die Erziehung und Bildung, aber auch die Sozialisation – müssen die Kinder Handwerkszeug bekommen, um sich zurechtzufinden.

Ein wichtiger Aspekt ist das kritische Denken: Ist dieses Video wirklich echt? Soll ich auf diese Kontaktanfrage antworten? Hierfür können in der Schule und zu Hause Kompetenzen aufgebaut werden. Hierfür ist wichtig, dass Kinder (und Erwachsene) die Möglichkeiten im Netz nicht einfach blind nutzen, sondern die Hintergründe verstehen. Wenn ich das für mich selbst mache, dann stellen sich etwa die Fragen, warum mir gerade vor allem Informationen zu London angezeigt werden

(Antwort: Ich war da auf einer Tagung und musste dort arbeiten.) und warum Nachrichten zu Preußen Münster in meinem Feed sehr präsent sind (Antwort: Ich bin Fan und suche oft nach aktuellen Informationen.)

Ein weiterer Punkt ist die ernst gemeinte Begleitung: Erwachsene sollten nicht bevormunden, sondern gemeinsam diese Wege im digitalen Raum gehen. Hierzu ein Beispiel aus meiner eigenen Jugend. Als Wikipedia erfunden wurde, haben meine Lehrpersonen das verteufelt. Es war verboten, dieses freie Lexikon zu nutzen. Heute ist Wikipedia weitestgehend akzeptiert, auch in Bildungskontexten. Und viele Lehrpersonen nutzen Wikipedia selbst, um sich zu orientieren. Bei künstlicher Intelligenz wird es ähnlich laufen. Klug von Erwachsenen wäre es, die Chancen auszuloten und die Grenzen zu kennen – und ihre Ideen und Gedanken mit den Kindern zu teilen.

Dr. David Rott ist Studienrat im Hochschuldienst an der Universität Münster (Institut für Erziehungswissenschaft). Seine Promotion verfasste er über die Handlungskompetenzen von Lehramtsstudierenden in der individuellen Förderung. Seine Forschungsschwerpunkte sind diversitätssensibler Unterricht, kritisches Denken und Kinderrechte. In der Lehre ist er in der Lehrer*innenbildung eingebunden. Unter www.researchgate.net/profile/David-Rott sind alle aktuellen Veröffentlichungen zu finden.

4

Gerechtigkeit, Schutz und Nachhaltigkeit

Sebastian Felix Zappe

Hat die Digitalisierung die Gesellschaft wirklich inklusiver gemacht?

Ein Schwimmbad, das nur noch Onlinetickets zulässt? In der Metropole Berlin ist das ganz normal: Seit 2024 sind dort fünf öffentliche Freibäder nur noch mit Onlineticket besuchbar. Wer weder Smartphone noch PC besitzt oder technische Abläufe nicht beherrscht, ist von diesen öffentlichen Orten fürs Erste ausgeschlossen. Diese Verletzung des Grundrechts auf Teilhabe ist keine Seltenheit. Manche Ticket- und Behördensysteme setzen mittlerweile voraus, dass die Zielgruppe digital fit ist. Doch was passiert, wenn ältere Menschen, Personen mit Behinderungen oder wohnungslose Menschen auf Offlinealternativen angewiesen sind?

Man sollte meinen, dass wir über Digitalisierung eigentlich gar nicht mehr so viel reden müssen. Wir erledigen unsere Bankgeschäfte per App, buchen Urlaubsreisen online und kommunizieren täglich über Chats oder Videokonferenzen. Viele von uns sehen das als selbstverständliche Erleichterung.

Aber wie ermöglichen wir Menschen Teilhabe, die nicht auf dem neuesten technologischen Stand sind? Vertieft die Digitalisierung gesellschaftliche Gräben? Wird sie sogar neue Gräben schaffen? Wir werden immer älter – werden wir uns irgendwann selbst auf der anderen Seite des Grabens befinden?

Teilhabe ist ein Menschenrecht, das bereits vor der Digitalisierung bestand. Unsere Gesellschaft hat sich diesem Ziel verschrieben – zumindest auf dem Papier. Worauf müssen wir achten, damit wir in der Praxis das Grundrecht auf Teilhabe nicht wegdigitalisieren?

Inklusion als Grundrecht vor der Digitalisierung

Inklusion bedeutet, dass alle Menschen, unabhängig von Merkmalen wie Alter, Behinderung, Herkunft oder Geschlecht, gleichberechtigt am gesellschaftlichen Leben teilnehmen können. Dieses Recht ist in zahlreichen nationalen und internationalen Verträgen und Gesetzen festgeschrieben – nicht zuletzt im Grundgesetz, der fundamentalen Rechtsbasis der Bundesrepublik und unserer Gesellschaft. Soziale Gerechtigkeit kann

nicht existieren, wenn nicht die Rechte aller Menschen gleichermaßen gewahrt werden. Durch die digitale Revolution entstehen nun ständig neue Werkzeuge und Möglichkeiten, Barrieren zu senken – leider aber auch neue Formen der Ausgrenzung.

Einerseits können Onlinedienste Barrieren abbauen, etwa wenn Menschen, die schlecht sehen können, die Lupenfunktion ihres Telefons, vergrößerte Schriften oder Screenreader nutzen. Andererseits schließt die zunehmende Fokussierung auf digitale Lösungen Menschen aus, etwa wenn sie keinen schnellen Internetanschluss haben, wenig technische Erfahrung mitbringen oder aufgrund einer Behinderung spezifische Anforderungen an Geräte und Software stellen. Zudem verstärkt die Annahme, dass alle Menschen über entsprechende Mittel und Zugänge verfügen, bestehende klassistische Muster in unserer Gesellschaft.

Ist ein Grundrecht auf Inklusion (zu) teuer?

Egal ob beim Staat oder in Unternehmen: Digitalisierung wird primär von einem anderen Gedanken als dem an die Grundrechte getrieben. Die Ziele sind eher zum Beispiel Personalausgaben zu senken, Prozesse effektiver zu gestalten, schneller auf Nachfrage zu reagieren oder neue Produkte zu entwickeln – kurz, Kosten zu sparen. Inklusion wird im Politik- und Wirtschaftskontext genau wie andere Nachhaltigkeitsthemen nicht selten als Hemmnis betrachtet. Inklusionsaspekte haben dann eher die Priorität eines nachgeordneten Nebeneffekts, den man für die PR nutzen kann. Aber ist diese Ansicht wirtschaftlich und gesellschaftspolitisch sinnvoll?

Barrierefreiheit als Fundament für Innovationssprünge

Gerade im Hightech-Bereich gibt es Barrierefreiheitsideen, die ganze Branchen umgekrempelt haben. So machte ein einziges Produkt – das iPhone – die Firma *Apple* zu einem der profitabelsten Unternehmen der Welt. Das Buch „Mismatch“ des *Massachusetts Institute of Technology* (MIT) erzählt die Entwicklung des iPhones aus einer Inklusionsperspektive. Die wichtigste Innovation des Geräts stammte danach nicht von Apple, sondern von der Firma *TouchStream*. *TouchStream* stellte Tastaturen her, die mit weniger Druckkraft bedient werden konnten. Statt auf physischen Tasten tippte man dort auf ein Multi-Touch-Display. Die Tastaturen wurden für mobilitätseingeschränkte Menschen vermarktet, bis Apple im Jahr 2005 die Firma aufkaufte – und die Touch-Tastatur zum neuen Standard für Mobiltelefone und Tablets wurde.

Zum Verkaufsstart wurde die Neuerung zunächst von der Presse verhöhnt – Telefone ohne physische Tasten galten als Spielzeug. Der Touch-Bildschirm, gestartet als Teilhabe-Technologie, gilt heute als essenziell für den Aufstieg Apples zu einer der größten Firmen der Welt.

Im selben Buch des MIT findet sich eine weitere Anekdote: Der amerikanische Techpionier Vinton Gray Cerf legte bei der Forschungsagentur des US-Verteidigungsministeriums DARPA Ende der 1970er-Jahre den technischen Grundstein für das heutige Internet. Um Informationen mit seiner gehörlosen Frau austauschen zu können, nutzte Vint Cerf das Netzwerk für eine frühe Form von Textmessaging – und entwickelte, geformt von dieser Erfahrung, einen der ersten kommerziellen E-Mail-Dienste.

Inklusives digitales Design per Gesetz

Beide Beispiele zeigen, dass inklusives digitales Design als Grundsatz eine erfolgreiche Basis für neue Technologien bildet. Inklusives Design bedeutet, dass Prozesse, Webseiten, Software und Apps von vornherein so gestaltet sein müssen, dass möglichst viele Menschen sie problemlos nutzen können. Dieses Prinzip führt nicht nur zu mehr sozialer Gerechtigkeit, sondern zahlt sich auch bereits bei kleineren Erfindungen als der E-Mail oder dem iPhone aus. Wer Produkte und Dienstleistungen für verschiedene Zielgruppen zugänglich macht, verbessert die Usability für alle – und erreicht nebenbei mehr Kundschaft.

In den Vereinigten Staaten gilt der ADA, der *Americans with Disabilities Act*. Er erlaubt Amerikaner*innen schon seit den 1970er-Jahren, gegen nicht barrierefreie Produkte und Dienstleistungen Klage zu erheben. Der viel jüngere *Europäische Rechtsakt zur Barrierefreiheit* (EAA) stellt auf EU-Ebene umfangreiche Anforderungen an die Barrierefreiheit von Gebäuden, Produkten und Services.

Auch wenn solche Regulierungen von vielen Unternehmen als zu bürokratisch wahrgenommen werden: Sie verbessern die Lebensqualität der Menschen in Europa und den USA. Und sie setzen einen Rahmen, in dem die Entwicklung innovativer Produkte, die für alle Menschen funktionieren, statistisch wahrscheinlicher wird.

Gerade Menschen ab 50, die statistisch häufiger von Behinderungen betroffen sind, verfügen über eine beachtliche Kaufkraft – zum Beispiel im Tourismus. Der Anteil von Menschen mit Behinderung in der Gesellschaft deutet darauf hin, dass durch barrierefreie Angebote bis zu zehn Prozent mehr Gäste erreicht werden, etwa Menschen mit Behinderung, Senior*innen und Familien. Da ältere Reisende zudem häufig mehr finanzielle Ressourcen mitbringen und längere Aufenthalte buchen, dürfte der potenzielle Umsatzanstieg sogar darüber liegen.

Verstärkt wird dies durch den demografischen Wandel. Die Gesellschaft der Industriestaaten wird immer älter. Wer das in der Planung berücksichtigt, sorgt für die Zukunft vor.

Förderungen müssen inklusiv entworfen werden

Barrierefreie Angebote erfordern häufig zunächst Investitionen – sei es für Personal, Qualifizierungen oder barrierefreie Technik. Solche Ausgaben sind in der Regel sinnvoll angelegtes Kapital. Dafür braucht es allerdings Unterstützung, etwa durch staatliche Fonds oder Förderprogramme, damit sich kleine und mittlere Unternehmen den Mehraufwand leisten können. Das Gleiche gilt für zivilgesellschaftliche und öffentliche Einrichtungen: Staat und Zivilgesellschaft müssen gemeinsam sicherstellen, dass Digitalförderung nie zulasten von Teilhabe geht – etwa bei Schulen, Kitas, Kulturzentren, Theatern, Beratungsstellen, Schwimmbädern oder Sporteinrichtungen. Im Zweifel müssen bei Vorhaben nicht-digitale Wege finanziell eingeplant sein.

Beispiele für inklusives Digitaldesign

Um Teilhabe-Aspekte einer Digitalisierungs-maßnahme zu beurteilen, könnte man an digitale Vorhaben folgende Fragen stellen:

- Sind neue Webseiten oder Apps barrierefrei nutzbar – auch für blinde, gehörlose, sehbehinderte und lernbehinderte Menschen? Hierfür gibt es die Web Content Accessibility Guidelines (WCAG). Es ist ein international anerkannter Standard, der Anforderungen und Best-Practice-Beispiele für barrierefreie Websites zusammenfasst und der ständig an aktuelle Entwicklungen angepasst wird.
- Welche Sinne werden vor der Digitalisierung und danach benötigt, um den Service oder das Produkt nutzen zu können? Die digitalisierte Neuerung sollte im Bestfall ermöglichen, den Service mit mehr Sinnen (Hören, Sehen, Tasten) benutzen zu können – und weniger Sinne haben zu müssen.

- Gibt es Videos in Gebärdensprache und in Leichter Sprache? Menschen mit Hörbehinderung oder kognitiven Einschränkungen profitieren von zusätzlichen Sprachoptionen. Gleichzeitig erleichtert ein solches Angebot auch anderen das Verständnis, zum Beispiel beim Erlernen einer Fremdsprache. Digitale Angebote können die Barrierefreiheit hier im Vergleich zum analogen Pendant verbessern. Inklusives Design führt dabei oft auch zu mehr Klarheit über das eigene Produkt: Wer seine Inhalte in Leichte Sprache überträgt, hinterfragt zugleich, ob das Angebot wirklich verständlich konzipiert ist.
- Gibt es ein telefonisch erreichbares Alternativangebot?
- Reduziert das neue Angebot „Crip Time“? Als Crip Time bezeichnet die Behindertenbewegung versteckte Zeitaufwände, die im Alltag nur bei Menschen mit Behinderung anfallen. Wer nicht für jede Kleinigkeit – etwa einen Banktermin – große Wege auf sich nehmen muss, sondern alles online erledigen kann, spart mit einer Behinderung eventuell mehr Zeit und Aufwand als eine Person ohne Behinderung.
- Wurden diverse Zielgruppen schon beim Design eines Produkts oder Services beteiligt?
- Wurde bei Orten oder Veranstaltungen bedacht, dass jeder Mensch den Ort auch finden können muss? Hier helfen Personalschulungen und ein Hinweis auf einen festgelegten Abholort – eine Erleichterung für blinde Menschen.
- Wurden Print-Produkte durch neue Prozesse ersetzt? Viele Menschen sind auf Flyer, Broschüren etc. angewiesen. Reicht statt einer Abschaffung vielleicht einfach eine kleinere, vereinfachte Publikation?
- Wird ein Offline-Konzept durch Video-Calls ersetzt? Wie wichtig ist das Offline-Konzept für benachteiligte Menschen in der Zielgruppe? Als Beispiel seien hier Beratungsstellen genannt, bei denen direkter Kontakt vielen Menschen ein Gefühl von Zugehörigkeit und Sicherheit gibt.
- Benötigt ein digitaler Ersatz eine Neuanschaffung von Hardware? Dies ist ein häufiger Grund für den Ausschluss von Menschen, die unter dem Existenzminimum leben und daher auf ältere PC- und Telefon-Modelle angewiesen sind.

- Gibt es ein Back-up, falls eine Person das neue Angebot nutzen möchte, aber nicht über die notwendige Hardware verfügt? Kann man Personalkosten durch wirtschaftliche Vorteile beheben, die gleichzeitig durch die Digitalisierung entstehen? Gibt es eine Möglichkeit, benachteiligte Menschen durch direkte Ansprache oder Schulungen weiter teilhaben zu lassen?

Kurzum: Wer Digitalisierung richtig einsetzt, ermöglicht Teilhabe, statt sie zu begrenzen. Wenn Produkte und Dienstleistungen barrierefrei gestaltet und soziale wie finanzielle Aspekte berücksichtigt werden, entsteht eine Win-win-Situation: Menschen werden in ihren Grundrechten gestärkt und Unternehmen erreichen mehr Kund*innen.

Exkurs: Was Deutschland von Japan lernen kann

Durch seine Hardware-Industrie hat Japan in der Digitalisierung bereits frühzeitig größere Fortschritte gemacht als andere Länder – und mit Digitaltechnik experimentiert. Überall finden sich digitale Anzeigen für Werbung, Abfahrten und Hinweise (und genauso häufig wie in Deutschland sind sie defekt). Scheinbar ist der Alltag in Japan von digitalen Lösungen durchzogen. Da die Systeme schon länger existieren, wirken sie aus heutiger Perspektive aber oft unüberlegt und altbacken in ihrer User Experience (UX). Japan hat technologisch anscheinend ein *Legacy*-Problem.

Zum Beispiel ist das japanische Verkehrswesen komplexer als das in Deutschland. Deutlich häufiger als bei uns ist der Kauf mehrerer Tickets für eine Reisekette erforderlich, die auch digital angepriesen werden. Aber egal, durch wie viele QR-Codes und Apps man sich langwierig klickt, in den meisten Fällen endet der „digitale“ Prozess genau wie in Deutschlands Nuller Jahren mit mehreren Tickets und Reservierungen – und zwar aus Papier.

Aber ist das schlecht? Denn immerhin existiert so in den meisten Fällen parallel ein nicht digitaler Zugang. Wer mit Japans verbreiteten Bahnhofsdrehsperren und ihren automatischen Ticket-Einzügen,

den komplizierten Ticketsystemen oder einfach nur mit der Orientierung am Bahnhof nicht zurechtkommt, findet an jedem Bahnsteig oder im Bus Angestellte, die technische Probleme jeder Art durch gesunden Menschenverstand zu überbrücken wissen. Ältere Menschen oder ausländische Gäste, die sich mit technischen Neuerungen schwertun, können damit selbstständig und mobil am öffentlichen Leben teilhaben.

Andere technische Neuerungen sind einfach zu verstehen, zum Beispiel Wegweiser, die anfangen zu sprechen, wenn sich ihnen eine sehbehinderte Person nähert. Die Vielzahl solcher baulichen Barrierefreiheitselemente in Japan würde mehrere Essays füllen. Ein Besuch offenbart, dass die Bedürfnisse älterer und behinderter Menschen in der Städte- und Verkehrsplanung stark berücksichtigt werden.

Einzelne ältere und behinderte Menschen ohne Begleitung sind im Stadtbild stark präsent. Kein Wunder, denn ihre Bedürfnisse wurden berücksichtigt! Wenn über Japan die Rede ist, stellen deutsche Medien dieses Phänomen nicht selten als sichtbare Vereinsamung dar. Dabei lässt es sich auch positiv interpretieren: Wer wegen vorhandener Barrierefreiheit bis ins hohe Alter allein reisen kann, genießt einfach sehr viel Unabhängigkeit. Sollte das nicht auch in Deutschland ein Ziel sein?

Während Japan trotz hoher Digitalisierung immer noch analoge oder leicht zugängliche Alternativen bietet, verengt sich in Deutschland der Weg durch rein digitale Lösungen mitunter zu stark.

Wer Reisen für ältere Familienmitglieder plant, wird rasch feststellen, dass Japan auch aus Digitalisierungsaspekten in puncto Barrierefreiheit viel komfortabler ist als Deutschland. Das wirft provokante Fragen auf: Würde man seinen Großeltern eher Japan oder Deutschland als Urlaubsziel empfehlen? Waren die Deutschen in ihrem effizienten Stellenabbau bei Hotline, ÖPNV und Postwesen eventuell zu voreilig?

Digitalisierung und Inklusion dürfen kein Widerspruch sein

Digitalisierung soll das Leben erleichtern – für alle. Wenn wir zulassen, dass die Digitalisierung Menschen ausschließt, verspielen wir unnötig ein wichtiges Grundrecht und nehmen noch dazu wirtschaftliche Einbußen in Kauf. Beispiele aus dem In- und Ausland zeigen, dass Inklusion und Wirtschaftlichkeit Hand in Hand gehen können. Die Frage „In was für einer Gesellschaft wollen wir leben?“ ist eng damit verbunden, wie wir die digitalen Technologien der Zukunft gestalten.

Indem wir uns auf inklusive Lösungen im Digitalen konzentrieren, gewinnen alle: Menschen mit unterschiedlichen Bedarfen, Unternehmen, Staat und letztlich auch die Gesellschaft als Ganzes. Dieses Transformationspotenzial sollten wir nutzen. Nicht nur für den Fortschritt, sondern um die Vision zu verwirklichen, dass jede*r von uns gleichberechtigt am gesellschaftlichen Leben teilnehmen kann – online wie offline.

Sebastian Felix Zappe arbeitet beim Berliner Verein Sozialhelden e. V. als CTO. Das Team setzt sich aktiv für gesellschaftliche Teilhabe ein und arbeitet dafür an innovativen Lösungen – zum Beispiel Wheelmap.org, einer weltweiten Karten-App für barrierefreie Orte, und broken-lifts.org, mit dem Fahrgäste im ÖPNV früher Bescheid wissen, ob ein Aufzug nicht funktioniert.

Felix Sühlmann-Faul

Grundrechte im Spannungsfeld zwischen Digitalisierung und Nachhaltigkeit – eine globale Heraus-forderung

In einer zunehmend digitalisierten Welt stehen wir vor der doppelten Herausforderung, die Chancen der Digitalisierung zu nutzen und gleichzeitig ihre negativen Auswirkungen auf Mensch und Umwelt zu minimieren. Die Digitalisierung verspricht Effizienz, Arbeitserleichterung und Produktionssteigerung, doch diese Potenziale verdecken oft tiefgreifende Nachhaltigkeitsprobleme. Diese reichen von ökologischen Belastungen bis hin zu ethischen Fragen der Ausbeutung im Globalen Süden, die durch die Klimakrise noch verschärft werden. Dieser Text analysiert diese kritische Wechselbeziehung zwischen Digitalisierung und Nachhaltigkeit. Er zeigt auf, dass eine verantwortungsvolle Gestaltung der digitalen Transformation unerlässlich ist, um soziale Gerechtigkeit, Klimaschutz und die Stärkung von Grundrechten in Einklang zu bringen und eine Fortsetzung kolonialer Ausbeutung im digitalen Zeitalter zu verhindern. Es bedarf eines globalen Umdenkens, bei dem die Kosten der Digitalisierung nicht länger ignoriert, sondern aktiv angegangen werden, um eine wirklich nachhaltige und gerechte Zukunft zu gestalten.

Nachhaltigkeit

Nachhaltigkeit bedeutet, dass wir Ressourcen so nutzen, dass sie nicht aufgebraucht werden. Das Ziel ist, dass die Natur oder andere Systeme, aus denen wir Ressourcen entnehmen, sich erholen und langfristig bestehen können. Im Kontext globaler Entwicklung umfasst Nachhaltigkeit ökologische, ökonomische und soziale Aspekte, die in einem ausgewogenen Verhältnis zueinander stehen sollten.

Zu den bekanntesten Definitionen von Nachhaltigkeit gehört die Fassung aus dem Bericht von Gro Harlem Brundtland an die Vereinten Nationen „Our Common Future“ von 1987. Sie schreibt darin: „Nachhaltige Entwicklung ist eine Entwicklung, die gewährt, dass künftige Generationen nicht schlechter gestellt sind, ihre Bedürfnisse zu befriedigen als gegenwärtig lebende.“

Diese Definition beschreibt einen Generationenvertrag und verweist dadurch auf die soziale Ebene. Trotzdem wird Nachhaltigkeit häufig auf die ökologische Ebene reduziert, wodurch die Verletzung von Menschen-, Gleichheits- und Freiheitsrechten, die durch

Nachhaltigkeitsdefizite entstehen, vergessen werden. Das verkennt auch den Umstand, dass ökologische Probleme früher oder später immer zu sozialen Problemen werden: Wenn zum Beispiel der Abbau von Rohstoff die umgebende Lebenswelt bedroht, ist eine würdige Existenz für viele dort ansässige Menschen nicht mehr gewährleistet.

Digitalisierung und Nachhaltigkeit

Diese beiden für sich allein genommen schon komplexen Themen stehen in einer ebenso komplexen Wechselbeziehung zueinander. Einerseits bietet die digitale Transformation durchaus enorme Chancen für eine nachhaltige Entwicklung, etwa durch effizientere Ressourcennutzung, verbesserte Umweltüberwachung oder die Abkehr von der Nutzung fossiler Energieträger. Andererseits bringt die rasante Verbreitung digitaler Technologien auch erhebliche Risiken mit sich. Von der Rohstoffgewinnung bis zur Entsorgung elektronischer Geräte ziehen sich diese wie ein roter Faden durch den gesamten Lebenszyklus unserer digitalen Begleiter. Diese Probleme manifestieren sich besonders deutlich in Entwicklungsländern, in denen Ausbeutung und Umweltzerstörung auf der Makroebene und gesundheitliche Risiken für die einzelnen Menschen Hand in Hand gehen.

Der Fluch der Konfliktmineralien

Beginnen wir am Anfang der Wertschöpfungskette: der Rohstoffgewinnung. Die Demokratische Republik Kongo (DRK) steht hier exemplarisch für viele Länder, die zwar einen Reichtum an wertvollen Rohstoffen besitzen, aber davon keineswegs profitieren. In der DRK erzeugt der Rohstoffreichtum eine Abwärtsspirale von zusätzlicher Armut und Chaos.

Die Produktion digitaler Endgeräte wie Smartphones setzt den Abbau zahlreicher chemischer Elemente voraus. Je nachdem, welche Quelle herangezogen wird, werden für ein Smartphone 55 bis 75 verschiedene Rohstoffe benötigt. Fünf der wichtigsten werden aus der DRK exportiert. Es handelt sich um die Mineralien Tantal, Zinn, Wolfram, Gold und Kobalt.

Kobalt wird unter anderem für die Herstellung von Lithium-Ionen-Akkumulatoren benötigt – dem Standard der aktuellen Akku-Technologie. Und der Bedarf ist groß: Laut Veröffentlichungen des United States Geological Survey (USGS) belief sich allein die Nachfrage aus dem Automobilsektor 2022 auf ungefähr 104.000 Tonnen des Rohstoffs. 148.000 Tonnen werden aktuell aus der DRK exportiert – das sind 70 Prozent der weltweiten Produktion.

Der Abbau und die Produktion der Elemente befinden sich in der DRK allerdings nicht in öffentlicher Hand oder staatlichen Betrieben. Sie werden Konfliktmineralien genannt, weil der Abbau vor Ort größtenteils von Rebellentruppen kontrolliert wird. Diese Gruppen, die sich seit etwa 35 Jahren einen immer wieder aufflammenden Bürgerkrieg liefern, haben den Bergbau und Teile des Handels mit den Mineralien an sich gerissen. Mit dem Gewinn von mehreren Hundert Millionen US-Dollar pro Jahr finanzieren sie Waffen, sichern ihre Macht und destabilisieren so die gesamte Region.

Diese Zustände haben verheerende Folgen für die Zivilbevölkerung: Die Todesopfer des Bürgerkriegs gehen in die Millionen. Allein 2021 zählte das UN-Flüchtlingshilfswerk 1.200 Todesopfer und 1.100 Fälle sexueller Gewalt. Durch die Konflikte wurden laut dem Flüchtlingshilfswerk der UN (UNHCR) 11 Prozent der zivilen Bevölkerung aus ihren ursprünglichen Heimatorten vertrieben und viele Millionen sind

vom Hunger bedroht. Die Zahl der vom UNHCR registrierten Flüchtlinge aus der DRK beläuft sich aktuell auf mehr als eine Dreiviertelmillion Menschen, die entweder in umliegenden Staaten eine neue Heimat suchen müssen oder sich dem Flüchtlingsstrom Richtung Europa anschließen. Das bedeutet, dass diese Konflikte, die durch Rohstoffe für die Digitalisierung des Globalen Nordens finanziert werden, keineswegs vor Ort bleiben.

Das größte Leid erleben wie so oft Frauen und Kinder: Unter dem Zwang der Rebellengruppen werden Kinder teilweise zu Arbeit gezwungen oder als Kindersoldaten missbraucht. Im Umfeld der Bergbauanlagen gibt es Zwangsprostitution von Frauen und Kindern, was auch zur Verbreitung von Infektionen wie mit dem HIV-Virus beiträgt. All diese Zustände entsprechen den Merkmalen moderner Sklaverei: Zwangsarbeit und sexuelle Ausbeutung, deren Opfer die Situation aufgrund von Drohungen, Gewalt, Machtmissbrauch oder extremer Armut nicht verlassen können.

Ökologische Folgen

Der Abbau von Rohstoffen für Digitalisierung und E-Mobilität ist nicht nur für Menschen in den Förderregionen problematisch. Die Folgen des Abbaus zeigen sich in der DRK in Abholzung, Erosion, Zerstörung von Lebensräumen und Vergiftung von Boden und Wasser. Auch der Lebensraum der vom Aussterben bedrohten Gorillas und Bonobos wird durch die planlose Landnahme von Rebellengruppen dezimiert.

Ökologische Probleme verlagern sich auf die soziale Ebene. Der Abbau von Lithium, ein Element, das für Akkumulatoren für Smartphones, Laptops, E-Autos und so weiter essenziell ist, verbraucht enorm viel Wasser – je nach Extraktionsmethode bis zu 2.000 Liter für ein Kilogramm. Eines der größten Vorkommen befindet sich in der Atacama-Wüste im Norden Chiles. Das Land erzeugte 2022 knapp 30 Prozent des weltweiten Bedarfs, hat aber angekündigt, die Produktion bis 2025 zu verdoppeln. Diese Entscheidung wurde getroffen, obwohl sich die Gewinnung dort direkt auf die Wasserreserven der gesamten Region auswirkt. Die Wüste zählt zu den trockensten Gebieten der Erde

und der Wasserverbrauch lässt den Grundwasserspiegel dramatisch sinken. Dadurch trocknen die Flussläufe aus, Wiesen verdorren und gehen unwiederbringlich verloren. Das gefährdet die Trinkwasserversorgung und landwirtschaftliche Bewässerung. Indigene Gemeinschaften, die traditionell von diesen Wasserressourcen abhängig sind, sehen sich gezwungen, ihre Lebensweise aufzugeben. Viele Menschen fühlen sich von den Unternehmen übergangen und berichten von unzureichenden Entschädigungen für den Verlust ihrer Ressourcen. Die indigenen Gemeinden befürchten, dass der Lithiumboom zwar kurzfristige Gewinne bringt, aber langfristig ihre Lebensgrundlagen zerstört.

Die Ausbeutung in der Produktionskette

Die Nachhaltigkeitsprobleme enden nicht bei der Rohstoffgewinnung. Auch die Herstellung unserer Smartphones, Tablets und Computer erfolgt oft unter unmenschlichen Bedingungen. Das taiwanesische Unternehmen Foxconn, eines der größten Zulieferer für Technologiegiganten wie Apple, beschäftigt über eine Million Arbeiter*innen, vorwiegend in chinesischen Niederlassungen. In riesigen Fabrikanlagen wie dem Longhua Science and Technology Park, auch „Foxconn-City“ genannt, der sich in der südchinesischen Technologiemetropole Shenzhen über drei Quadratkilometer erstreckt, leben und arbeiten Menschen unter Bedingungen, die mit westlichen Standards nicht vergleichbar sind. Untersuchungen von China Labor Watch im Jahr 2023 ergaben anhaltende Arbeitsrechtsverletzungen wie erzwungene Überstunden, Diskriminierung bei der Einstellung, Mobbing und sexuelle Belästigung am Arbeitsplatz. Überlange Arbeitszeiten, mangelnder Arbeitsschutz und psychische Belastungen führten in der Vergangenheit zu einer Serie von Selbstmorden unter den Mitarbeitenden.

Das Problem des E-Waste

Am Ende des Lebenszyklus unserer digitalen Begleiter stoßen wir auf die am stärksten wachsende Müllart – den Elektroschrott. 2023 fielen weltweit etwa 65 Millionen Tonnen Elektroschrott an, bis 2030 sollen es laut UN-Prognose 82 Millionen Tonnen werden. Ein Großteil landet in Entwicklungsländern wie Ghana, wo er unter gefährlichen Bedingungen verwertet wird. Selbst Kinder zerlegen dort Geräte und setzen sich giftigen Substanzen wie Blei, Quecksilber und Kadmium aus. Hohe Konsumraten und kurze Produktlebenszyklen erzeugen diese Müllberge. Trotz Exportverboten wird viel Elektroschrott illegal, oft als Spenden deklariert, in ärmere Länder gebracht. Dort wird die Verwertung aufgrund mangelnder Alternativen als Einkommensquelle akzeptiert, obwohl sie Gesundheit und Umwelt stark gefährdet.

Der Weg zu Grundrechten im digitalen Zeitalter

Um Grundrechte im digitalen Zeitalter durchzusetzen, ist ein Blick über den Tellerrand nötig. Es bedarf einer ganzheitlichen Strategie, die Bildung, Infrastrukturentwicklung und Wirtschaftsförderung umfasst. Nur so können eine Fortsetzung der Kolonialgeschichte verhindert und das Potenzial der Digitalisierung für nachhaltige Entwicklung und Wohlstand für alle erschlossen werden.

Die Verantwortung liegt zum größeren Teil bei den Unternehmen und der Politik. Transparente und faire Lieferketten, menschenwürdige Arbeitsbedingungen und eine echte Verantwortung für den gesamten Lebenszyklus der Produkte – von der Rohstoffgewinnung bis zur Entsorgung – muss gewährleistet sein. Dafür braucht es bessere Sammel- und Recyclinginfrastruktur, strengere Regulierung und Durchsetzung von Exportverboten, Designrichtlinien für längere Lebensdauer und Reparierbarkeit sowie Aufklärung und Bewusstseinsbildung bei den Verbraucher*innen. Und die höchste Forderung ist die Internalisierung

der Rohstoffkosten: Unternehmen begleichen in aller Regel nur die Kosten für Abbau, Transport und Material. Internalisierung würde bedeuten, auch für Umweltkosten (Umweltschutzmaßnahmen, Renaturierung …), soziale Kosten (Arbeitsschutz, Bildungsprojekte …) und langfristige Folgekosten (Gesundheitskosten, Kosten für Klimaschutz …) aufzukommen. Die resultierenden Preissteigerungen wären ein klares Argument für beschleunigte Maßnahmen hin zur Kreislaufwirtschaft.

Fazit: Digitalisierung als Werkzeug für eine bessere Zukunft

Die Herausforderungen sind komplex und erfordern ein Umdenken auf vielen Ebenen. Wir müssen verstehen, dass digitale Geräte kein Selbstzweck sind, sondern ein Werkzeug, das wir bewusst und verantwortungsvoll einsetzen müssen. Es geht darum, eine Balance zu finden zwischen technologischem Fortschritt, sozialer Gerechtigkeit und ökologischer Nachhaltigkeit. Der Globale Süden muss aus seinen Abhängigkeiten befreit werden. Die für das digitale Zeitalter typische exponentielle Steigerung von Innovationsraten, Produktion von Geräten und Konsumchancen reduzieren die ärmsten Länder dieser Welt auf eine Existenz als Lieferant von Rohstoffen und billiger Arbeitskraft. Ein Schlüssel, um den Abhängigkeiten zu entkommen liegt im Aufbau eigener digitaler Infrastrukturen und Technologien, in Investitionen in Bildung und Forschung im IT-Bereich und in der Entwicklung lokaler Alternativen zu dominanten westlichen Plattformen. Das kann nur durch einen Technologietransfer von Nord nach Süd, offene Zugänge zu Forschungsergebnissen und Technologien und der Förderung von Open-Source-Lösungen fernab der proprietären Soft- und Hardware der großen Technologiekonzerne gelingen.

Die Klimakrise verdeutlicht die Notwendigkeit eines globalen Umdenkens. Sie erfordert eine nie da gewesene internationale Kooperation, die auch als Modell für die Überwindung digitaler Abhängigkeiten

dienen kann. Der Mangel an politischem Willen und echtem Engagement für Veränderung bleibt jedoch eine zentrale Herausforderung in beiden Bereichen. Dazu gehört es, anzuerkennen, dass die Klimakrise das meiste Leid in den Ländern des Globalen Südens erzeugt, obwohl diese am wenigsten dazu beigetragen haben. Europa muss aus ethischen Gründen eine Vorreiterrolle in der Förderung des Globalen Südens und der Bewältigung der Klimakrise übernehmen, insbesondere, da von den USA und China in dieser Hinsicht wenig Unterstützung zu erwarten ist. Diese Verantwortung ergibt sich zunächst aus Europas kolonialer Vergangenheit und der daraus resultierenden historischen Schuld gegenüber vielen Ländern des Globalen Südens. Als Wertegemeinschaft, die für Demokratie, Menschenrechte und Gerechtigkeit eintritt, hat Europa zudem die moralische Verpflichtung, globale Herausforderungen anzugehen und Solidarität zu zeigen. Durch eine Vorreiterrolle in diesen Bereichen kann Europa nicht nur zur globalen Stabilität und Konfliktvermeidung beitragen, sondern auch als Vorbild für andere Akteur*innen dienen. Letztlich liegt ein solches Engagement auch im Eigeninteresse Europas, da globale Herausforderungen wie Klimawandel und Armut direkte Auswirkungen auf Migration, Sicherheit und Wirtschaft in Europa haben. Indem die EU diese Verantwortung wahrnimmt, stärkt sie ihre Glaubwürdigkeit als globaler Akteur und trägt aktiv zu einer gerechteren und nachhaltigeren Welt bei. Diese Vision einer zweiten Moderne bietet die Chance, die Fehler der Vergangenheit zu korrigieren und gleichzeitig die Möglichkeiten der Digitalisierung für den Klimaschutz zu nutzen. Technologie hat uns an den Rand des Kollaps geführt – aber so bizarr das ist: Um uns vom Kollaps zu befreien, brauchen wir nicht weniger, sondern mehr Technologie. Denn digitale Technologien können einen erheblichen Beitrag zur Reduzierung von CO2-Emissionen leisten und somit helfen, die Klimaziele zu erreichen. Die Nutzung erneuerbarer Energien steht und fällt sogar mit der Digitalisierung: Intelligente Stromnetze (Smart Grids) ermöglichen eine effiziente Steuerung und Verteilung von erneuerbaren Energien, während KI-basierte Prognosemodelle die Energieproduktion aus Wind und Sonne optimieren. Digitale Energiemanagement-Systeme steuern den Verbrauch in Gebäuden und Industrien, und virtuelle Kraftwerke vernetzen dezentrale Energiequellen. Diese Beispiele digitaler Innovationen sind entscheidend für die effiziente Integration und Nutzung erneuerbarer Energien im modernen Energiesystem.

Trotzdem gleicht die Digitalisierung einem Werkzeugkasten. Auch dieser löst nichts von selbst. Es liegt an uns, die Werkzeuge gezielt zu nutzen, an den notwendigen Stellen einzusetzen und dadurch eine gerechtere, nachhaltigere Welt zu gestalten. Zentral für diese Vision ist die Anerkennung und Stärkung von Grundrechten als unabdingbare Basis einer gerechten und nachhaltigen Gesellschaft. Der Schutz der Umwelt und des Klimas muss als fundamentales Menschenrecht verstanden und in Verfassungen und internationalen Abkommen integriert werden. Gleichzeitig müssen wir sicherstellen, dass Maßnahmen zum Klimaschutz die bestehenden Grundrechte respektieren und stärken, insbesondere für marginalisierte Gruppen und Gemeinschaften im Globalen Süden.

Die Zeit drängt, aber mit Entschlossenheit, sozialer Innovation und Solidarität können wir den Wandel gestalten. Jede*r kann dazu beitragen: Organisationen wie *urgewald e. V.* setzen sich für Umweltrechte und gegen die Finanzierung klimaschädlicher Projekte ein, während *Germanwatch* konkrete politische Veränderungen für globale Gerechtigkeit anstößt. Durch Unterstützung von Initiativen wie *Fairphone* oder *Shift*, die auf faire Elektronikproduktion setzen, oder durch die Teilnahme an Kampagnen von *Greenpeace* und *Fridays for Future* kann jede*r Einzelne aktiv werden. Durch bewusstes Konsumverhalten, Unterstützung von Petitionen und Teilnahme an Demonstrationen können wir gemeinsam eine nachhaltige, gerechte Welt für kommende Generationen schaffen, in der Grundrechte und Klimaschutz Hand in Hand gehen.

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

Zum Weiterlesen, -schauen, und -hören

- Sühlmann-Faul, Felix und Stephan Rammler. Der blinde Fleck der Digitalisierung: Wie sich Nachhaltigkeit und digitale Transformation in Einklang bringen lassen. München: Oekom, 2018.
- Podcast „Quarks Daily Spezial Folge 43 – Alles Elektroschrott? – Was wird aus TV, Handy & Co?“, 23. April 2022. https://www.quarks.de/podcast/quarks-daily-spezial-folge-43-alles-elektroschrott-was-wird-aus-tv-handy-co/
- Video Inside Apple's iPhone Factory In China, 2021. https://www.youtube.com/watch?v=9XkX6EGk_CA
- Ghielmini, Sabrina, Christine Kaufmann, Charlotte Post, Tina Büchler, Mara Wehrli, und Michèle Amacker. „Grund- und Menschenrechte in einer digitalen Welt“, 2021, 144. https://boris.unibe.ch/163080/1/Grund-und-Menschenrechte-in-einer-digitalen-Welt-V1_00-20210414-digital.pdf

Francesca Schmidt

Digitale Grundrechte und Geschlechter-gerechtigkeit

173

Die Digitalisierung verändert tiefgreifend gesellschaftliche Strukturen und Aushandlungsprozesse. Dabei sind Diskriminierung, Ausschlüsse und Gewalt oft untrennbar mit digitalen Technologien verwoben, sei es durch algorithmische Entscheidungsprozesse, automatisierte Überwachung oder in digitalen Öffentlichkeiten. Diese Mechanismen sind nicht neu, sondern setzen sich aus analogen Machtverhältnissen fort und verstärken bestehende Ungleichheiten.

Digitale Grundrechte wie Meinungsfreiheit, Datenschutz und das Recht auf digitale Teilhabe stehen im Zentrum zunehmend polarisierter gesellschaftlicher und politischer Debatten. Besonders relevant ist dabei die Frage der Geschlechtergerechtigkeit, die jedoch nur im Rahmen einer intersektionalen Analyse adäquat erfasst werden kann. Denn digitale Technologien müssen nicht nur diskriminierungsfrei gestaltet werden, sondern auch als Werkzeuge für gerechtere gesellschaftliche Strukturen nutzbar sein.

Der Begriff der Intersektionalität wurde von Kimberlé Crenshaw (1989) geprägt und beschreibt die Überschneidung verschiedener Diskriminierungsformen wie Rassismus, Sexismus, Klassismus und Ableismus. Diesen Ansatz kann man als rassismuskritisch bezeichnen, da er insbesondere die historische und systemische Verankerung von Rassismus in sozialen, politischen und technologischen Strukturen analysiert. Auch für digitale Räume ist dies relevant, denn sie sind nicht neutral, sondern durchzogen von kolonialen Kontinuitäten, Geschlechternormen und sozioökonomischen Ungleichheiten.

Digitale Kluft und strukturelle Barrieren

Der sogenannte „Digital Gender Gap“ verdeutlicht die ungleiche Verteilung von Zugängen und Kompetenzen im digitalen Raum. Laut dem D21-Digital-Index von 2024/2025 liegt der Digitalisierungsgrad für Frauen bei 56 Punkten, während Männer 62 Punkte erreichen. Frauen schätzen ihre digitalen Fähigkeiten weiterhin geringer ein und nutzen digitale Technologien weniger vielfältig. Gleichzeitig bleiben sie insbesondere in technologischen

und datengetriebenen Berufsfeldern unterrepräsentiert. Frauen äußern zudem häufiger Sicherheitsbedenken und zeigen eine skeptischere Haltung gegenüber der digitalen Transformation. Bildung erweist sich als ein Schlüsselfaktor: Während Menschen mit niedriger Bildung nur eine digitale Resilienz von 43 Prozent aufweisen, liegt dieser Wert bei hochgebildeten Personen bei 78 Prozent. Digitale Resilienz beschreibt die Fähigkeit, sich souverän und gestaltend im digitalen Wandel zu bewegen. Wer diese Kompetenz nicht entwickelt, läuft Gefahr, von zentralen gesellschaftlichen Entwicklungen abgehängt zu werden. Mit dem Resilienzindikator kann, laut dem D21-Digital-Index, eine Aussage darüber getroffen werden, wie (digital) zukunftsfähig die betrachtete Gruppe ist.

Neben strukturellen Unterschieden existieren finanzielle Barrieren. Frauen verdienen weiterhin durchschnittlich 16 Prozent weniger als Männer (Gender-Pay-Gap), was ihre Möglichkeiten zur Anschaffung von Hardware oder zur Nutzung digitaler Dienstleistungen einschränkt. Der Migration-Pay-Gap, also Einkommensunterschiede aufgrund von Migrationserfahrungen, verstärkt diese Problematik, ebenso wie rassistische Diskriminierungen, die den Zugang zu hochwertigen digitalen Ressourcen erschweren. Technologien selbst sind zudem oft nicht barrierefrei gestaltet.

Der dritte Gleichstellungsbericht der Bundesregierung beschreibt, dass während des Lockdowns deutlich wurde, wie stark ungleiche Zugänge zu digitalen Endgeräten und stabilem Internet Bildungslücken vertiefen – insbesondere bei einkommensschwachen Haushalten und Familien mit Migrationsgeschichte. Diese digitale Kluft hat direkte Auswirkungen auf Bildungsbiografien: Kinder und Jugendliche aus finanzstärkeren Haushalten können leichter auf digitale Lernangebote zugreifen, während benachteiligte Gruppen aufgrund fehlender Infrastruktur, mangelnder digitaler Kompetenz oder begrenztem Zugang zu technischen Geräten zurückfallen.

Dadurch werden bestehende soziale Ungleichheiten vertieft, und es zeigt sich, dass digitale Teilhabe nicht nur eine Frage des technischen Zugangs ist, sondern auch von sozioökonomischen Faktoren, politischen Rahmenbedingungen und geschlechtergerechten Strukturen abhängt. Langfristige Investitionen in digitale Bildung, Infrastruktur und inklusive Konzepte sind daher unerlässlich, um solche Bildungsungerechtigkeiten zu minimieren und digitale Grundrechte für alle zu gewährleisten.

Global betrachtet verstärken neokoloniale Abhängigkeiten diese Dynamiken: Während digitale Technologien überwiegend aus westlicher Perspektive entwickelt werden, bleibt der Zugang zu schneller Internetinfrastruktur in vielen Ländern des sogenannten Globalen Südens beschränkt. Dies führt zu fortschreitender digitaler Marginalisierung und einer Fortsetzung kolonialer Machtverhältnisse im digitalen Raum. Besonders in den Bereichen Sprachtechnologien und algorithmische Entscheidungsprozesse zeigt sich, dass nicht-dominante Sprachen und Wissenssysteme oft ignoriert oder unterrepräsentiert sind. So versteht etwa die automatische Übersetzung von KI-Systemen viele afrikanische Sprachen kaum oder gar nicht – mit gravierenden Folgen für Teilhabe und Sichtbarkeit. Auch große Plattformen wie Meta oder X (ehemals Twitter) investieren kaum in Content-Moderation in nicht westlichen Sprachen, was Falschinformationen und digitaler Gewalt Tür und Tor öffnet. Hinzu kommt, dass viele Länder im Globalen Süden gezwungen sind, Cloud-Infrastrukturen westlicher Tech-Konzerne zu nutzen – was zu neuen Abhängigkeiten und Kontrollverlusten führt. Diese neokolonialen Strukturen sind nicht losgelöst von historischen Kontinuitäten zu betrachten, da koloniale Herrschaftssysteme die ungleichen Machtverhältnisse geschaffen haben, die sich bis heute in technologischen Abhängigkeiten und Ressourcenkontrollen fortsetzen. Dieser Sachverhalt wird oft mit dem Begriff Digitaler Kolonialismus umschrieben.

Forderungen nach inklusiver Infrastruktur

Eine feministische und rassismuskritische Digital- und Netzpolitik muss diese Ungleichheiten adressieren. Ein geschlechtergerechter digitaler Raum erfordert nicht nur den Zugang zu Technologien, sondern auch deren bewusste Gestaltung. Der geringe Anteil von BIPoC- und FLINTA*-Personen (also Schwarze, Indigene und Menschen of Colour und Frauen, Lesben, Inter-, Nicht-binäre, Trans- und Agender-Personen) in der Technologiebranche führt dazu, dass digitale Systeme oft aus einer cis-männlichen und dominanten Perspektive entwickelt werden. Feministische

Netzpolitiken setzen sich daher unter anderem für diversere Teams und bewusstere Entscheidungsprozesse ein.

Kapitalismus, Risikokapital und strukturelle Ausschlüsse in der Technologiebranche

Die kapitalismuskritische Perspektive, die feministische und rassismuskritische Netzpolitik auch einnehmen kann, zeigt, wie stark strukturelle Ungleichheiten durch die Logik des Marktes fortgeschrieben werden. Venture-Capital-Finanzierung, ein zentraler Mechanismus zur Förderung von Innovationen, bevorzugt systematisch cis-männlich dominierte Teams, während FLINTA*-geführte oder divers aufgestellte Teams nur etwa zwei Prozent des gesamten Risikokapitals erhalten. Diese Diskriminierung ist nicht nur Ausdruck patriarchaler Strukturen, sondern auch eine Folge kapitalistischer Prioritäten, die kurzfristige Profite über langfristige soziale und wirtschaftliche Nachhaltigkeit stellen. Ironischerweise zeigen Studien, dass divers geführte Unternehmen im Durchschnitt eine um 25 Prozent höhere Rendite erzielen. Dennoch wird Diversität oft als „unrentabel“ oder „risikoreich“ eingestuft, da sie nicht in das vorherrschende Bild von Erfolg innerhalb des kapitalistischen Systems passt.

Das heißt, dass marginalisierte Gruppen als aktive Akteur*innen technologischer Innovation anerkannt werden müssen. Statt sie lediglich als passive Nutzende oder Betroffene zu betrachten, müssen ihre Perspektiven aktiv in die Entwicklung digitaler Technologien einfließen. Denn ihr Wissen um Transformationsprozesse innerhalb unterschiedlicher Communitys kann zentral sein. Gerade marginalisierte Gruppen entwickeln bereits innovative Lösungen für gesellschaftliche Herausforderungen, etwa durch feministische Tech-Kollektive wie *TechHer* in Nigeria, die gezielt digitale Kompetenzen von Frauen stärken und Räume für selbstbestimmte Teilhabe schaffen. Die Organisation *TEDIC* in Paraguay setzt sich für Datenschutz, digitale Rechte und freie Netzwerke ein – aus einer dezidierten gender- und menschenrechtlichen Perspektive.

Und das Projekt *Masakhane* zeigt, wie afrikanische Forscher*innen gemeinsam KI-Sprachtechnologien entwickeln, die afrikanische Sprachen und Wissenssysteme sichtbar machen. Daher ist es essenziell, dass technologische Entwicklung nicht über diese Communitys hinweg geschieht, sondern aktiv durch ihr Wissen, ihre Perspektiven und ihre Bedürfnisse gestaltet und gesteuert wird.

Netzneutralität und Open Source als Bausteine einer gerechten digitalen Infrastruktur

Internationale Initiativen wie die *Feminist Principles of the Internet* fordern darüber hinaus eine grundsätzliche Netzneutralität, also das Prinzip, dass alle Daten im Internet gleich behandelt werden müssen, unabhängig von Sender, Empfänger oder Inhalt. Netzneutralität ist deshalb so zentral, weil sie verhindert, dass große Internetanbieter bestimmten Plattformen oder zahlungskräftigen Akteur*innen Vorrang geben, während andere ausgebremst oder blockiert werden. Ohne Netzneutralität könnten etwa feministische, queere oder unabhängige Medienangebote schlechter auffindbar oder langsamer zugänglich sein als kommerzielle Inhalte, was digitale Sichtbarkeit, Teilhabe und Meinungsfreiheit massiv einschränken würde. Netzneutralität sichert also den gleichberechtigten Zugang zu Informationen und digitalen Räumen, gerade für marginalisierte Gruppen.

Gleichzeitig betonen diese Initiativen die Bedeutung von Open-Source-Lösungen, die nicht nur kostengünstigere Alternativen darstellen, sondern auch Möglichkeiten für größere Partizipation und Kontrolle durch diverse und marginalisierte Gemeinschaften bieten. Der Quellcode ist öffentlich zugänglich, sodass Technologien nicht nur genutzt, sondern auch verstanden, hinterfragt und weiterentwickelt werden können, ohne Abhängigkeit von großen Konzernen. Aus einer

rassismuskritischen Perspektive können Open-Source-Technologien helfen, Macht zu dezentralisieren, Transparenz herzustellen und marginalisierten Gruppen mehr Selbstbestimmung über digitale Werkzeuge zu geben. So können Communitys etwa eigene Tools an ihre Bedürfnisse anpassen, statt sich an intransparente Systeme anpassen zu müssen, die ihre Realität oft nicht abbilden.

Technologien dürfen also nicht nur bestehende Machtverhältnisse reproduzieren, sondern müssen gezielt für inklusivere und gerechtere digitale Gesellschaften genutzt werden, dies auch jenseits kapitalbezogener Profitstrukturen.

Repräsentation und Sichtbarkeit im digitalen Raum: Fake News, geschlechtergerechte Grundrechte und Meinungsfreiheit

Laut einer Studie von *Plan International*, die 2021 erschienen ist („The Truth Gap"), fühlen sich über 90 Prozent der befragten Mädchen und jungen Frauen durch Fake News und Hass im Netz verunsichert. Etwa ein Viertel der Befragten zögert daher, ihre Meinung online zu äußern, und 18 Prozent haben sich aufgrund von Falschinformationen aus politischen Diskussionen zurückgezogen. Die zunehmende Verbreitung von Desinformation und Hassrede schränkt somit digitale Grundrechte ein, indem sie marginalisierte Gruppen aus dem öffentlichen und politischen Diskurs verdrängt.

Beispielhaft sei hier das neue Community-Notes-System von Meta, das die bisherigen unabhängigen Faktenprüfungsprogramme ersetzt, angeführt.

Die Community Notes basieren auf einem nutzergetriebenen Ansatz, bei dem registrierte Teilnehmer kurze Notizen mit maximal 500 Zeichen zu Beiträgen verfassen und bewerten können. Diese

Notizen werden nur veröffentlicht, wenn Nutzende mit unterschiedlichen Perspektiven ihre Genauigkeit bestätigen. Meta argumentiert, dass dieser Ansatz weniger voreingenommen ist und zudem skalierbarer sei als professionelle Faktenprüfung. Kritiker*innen weisen jedoch darauf hin, dass dieses System anfällig für Verzögerungen bei der Kennzeichnung von Fehlinformationen ist und es bei komplexen Themen oft an Expertise mangelt.

Die Auswirkungen unzureichender Moderation treffen Frauen oft besonders stark. Fehlinformationen zu Themen wie reproduktiver Gesundheit, Feminismus oder Gleichstellung verbreiten sich schnell und bleiben häufig unwidersprochen. Das kann konkrete Folgen haben, etwa wenn falsche Gesundheitsinformationen Entscheidungen beeinflussen oder frauenfeindliche Narrative die Sichtbarkeit und Sicherheit von Aktivist*innen im Netz einschränken. Community Notes, also nutzergenerierte Faktenkorrekturen auf Plattformen wie X (ehemals Twitter), können das Vertrauen in die Faktenprüfung stärken. Ihre Wirksamkeit hängt jedoch stark vom gesellschaftlichen Konsens über ein Thema ab. Bei politisch weniger umstrittenen Inhalten funktionieren sie gut. Bei kontroversen oder systemkritischen Themen wie Feminismus oder Rassismus hingegen werden Falschinformationen seltener mit Community Notes versehen, unter anderem, weil die Beiträge nur veröffentlicht werden, wenn Nutzende mit unterschiedlichen Perspektiven ihrer Richtigkeit zustimmen. Fehlt dieser Konsens, bleibt vieles unkorrigiert, selbst dann, wenn es nachweislich falsch oder gefährlich ist.

Digitale Grundrechte sind stets in ihrer wechselseitigen Beziehung zu betrachten. Das Recht auf Meinungsfreiheit darf nicht losgelöst von anderen fundamentalen Rechten wie dem Schutz vor Diskriminierung, geschlechtsspezifischer Gewalt und strukturellen Ausschlüssen verstanden werden. Ein diskriminierungsfreier Zugang zur digitalen Öffentlichkeit erfordert daher Maßnahmen, die gezielt Desinformation und Hassbotschaften entgegenwirken und marginalisierten Stimmen Raum verschaffen.

Digitale Transformation geschlechtergerecht, intersektional und dekolonial gestalten

Die digitale Transformation birgt trotz aller Herausforderungen ein großes Potenzial für gesellschaftlichen Wandel. Doch sie ist nicht losgelöst von bestehenden Machtstrukturen. Digitale Technologien und Infrastrukturen sind oft von den gleichen kolonialen Kontinuitäten geprägt, die auch andere gesellschaftliche Bereiche durchziehen. Ungleichheiten manifestieren sich dabei entlang mehrerer Achsen: Geschlecht, Herkunft, Klasse und andere soziale Faktoren bestimmen maßgeblich, wer Zugang zu Wissen, Ressourcen und Mitgestaltung hat. Eine intersektional-feministische Netz- und Digitalpolitik bedeutet daher konkret, Machtverhältnisse bewusst zu hinterfragen und neu zu verteilen – sowohl in der technologischen Entwicklung als auch in der Wissensproduktion. Geschlechtergerechtigkeit ist in diesem Kontext kein nachrangiges Ziel, sondern ein grundlegendes Recht, das in digitalen Räumen ebenso verteidigt werden muss wie in anderen gesellschaftlichen Bereichen.

Gleichzeitig eröffnet die Digitalisierung neue Möglichkeiten für Vernetzung, Sichtbarkeit und kollektives Handeln über soziale und geografische Grenzen hinweg. Marginalisierte Communitys schaffen eigene Räume, entwickeln alternative Infrastrukturen, schreiben ihre Geschichten neu und bringen Technologien hervor, die auf Fürsorge, Solidarität und Gerechtigkeit ausgerichtet sind. Digitale Werkzeuge können genutzt werden, um diskriminierende Strukturen sichtbar zu machen und marginalisiertes sowie konterhegemoniales Wissen zugänglich zu machen. Wenn diese Ansätze gestärkt und politisch unterstützt werden, kann digitale Transformation nicht nur Probleme reproduzieren, sondern aktiv zur Schaffung gerechterer Zukünfte beitragen.

Ein zentraler Ansatz, um diese Ungleichheiten zu überwinden, ist die Dekolonisierung digitaler Räume. Sie umfasst die aktive Einbindung diverser bisher marginalisierter Perspektiven und Gruppen, die in digitalen und gesellschaftlichen Diskursen unterrepräsentiert sind. Das

Projekt *Whose Knowledge?* etwa schließt gezielt Wissenslücken in der Wikipedia, indem es marginalisierte Stimmen sichtbar macht. Die feministische Initiative *Coding Rights* aus Brasilien bietet ein weiteres gutes Beispiel, dort werden kritisch digitale Technologien und Datenschutz aus intersektionalen und dekolonialen Perspektiven hinterfragt, insbesondere im Hinblick auf die Rechte von Frauen, queeren Menschen und Communitys im sogenannten Globalen Süden.

Zur Dekolonisierung von Wissen gehört ebenso die Anerkennung und Förderung vielfältiger Wissenssysteme. Das südafrikanische Projekt *Deep Learning Indaba* zeigt, wie afrikanische Perspektiven und Sprachen gezielt in die Entwicklung von künstlicher Intelligenz integriert werden können. Aus einer rassismuskritischen Perspektive setzt sich die *Algorithmic Justice League* von Joy Buolamwini erfolgreich dafür ein, rassistische und diskriminierende Verzerrungen in Algorithmen zu identifizieren und zu bekämpfen, Verzerrungen, die oft Frauen und nicht-binäre Personen betreffen.

Diese Beispiele zeigen, wie eine intersektionale, feministische und rassismuskritische Netz- und Digitalpolitik aussehen kann. Sie sind essenziell, um langfristig strukturelle Ausschlüsse zu überwinden, Macht neu zu verteilen und vielfältige Wissensformen sowie geschlechtergerechte digitale Räume gleichberechtigt anzuerkennen.

Francesca Schmidt arbeitet zu digitaler Gerechtigkeit, KI und feministischer Netzpolitik. Ihre Schwerpunkte liegen auf rassismuskritischer, dekolonialer und queer-feministischer politischer Bildung. Sie konzipiert Veranstaltungen, schreibt, berät und forscht praxisnah – u. a. als Vorsitzende von netzforma* e. V. und Referentin bei der Bundeszentrale für politische Bildung.

Zum Weiterlesen

- Algorithmic Justice League https://www.ajl.org/
- Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) (2021). Dritter Gleichstellungsbericht der Bundesregierung: Digitalisierung geschlechtergerecht gestalten. Berlin https://www.dritter-gleichstellungsbericht.de/
- Coding Rights – Intersektionale und dekoloniale Perspektiven auf digitale Technologien. https://codingrights.org/en/
- Deep Learning Indaba https://deeplearningindaba.com/2025/
- D21 Initiative (Hrsg.). (2025). D21-Digital-Index 2024/2025 – Jährliches Lagebild zur Digitalen Gesellschaft in Deutschland. https://initiatived21.de/d21-digital-index/
- Plan International. (2021). The Truth Gap – How misinformation and disinformation online affect the lives, learning and leadership of girls and young women. Abgerufen von: https://plan-international.org/publications/truth-gap
- Whose Knowledge? – Decolonizing the Internet. Abgerufen von: https://whoseknowledge.org/

Anne Roth

Digitale Gewalt – Formen, Folgen, fehlender Schutz

Was genau ist digitale Gewalt?

Menschen, die digitale Gewalt erleben, wissen oft nicht, was die Ursache der Situation ist, unter der sie leiden. Wenn eine Frau mit ihren Kindern ihren gewalttätigen Partner verlässt und er kurze Zeit später wieder vor der Tür steht, obwohl er die Adresse nicht hat, hat er den Kindern beim vorgeschriebenen Besuch vielleicht ein winziges Ortungsgerät ins Spielzeug montiert, um herauszufinden, wo die neue Wohnung ist.

Wenn Kolleg*innen merkwürdige Bemerkungen machen, hat ihnen vielleicht ein zurückgewiesener Liebhaber intime Bilder geschickt, die entweder heimlich oder ursprünglich einvernehmlich aufgenommen wurden. Manchmal droht der Täter auch nur damit, Nacktbilder zu veröffentlichen. Das Motiv: Demütigung, verletzte Eitelkeit, Kontrollverlust. Woher sie stammen, ist den Opfern oft unklar. Wurden sie mit einer unsichtbaren Kamera oder mit einer Drohne durchs Fenster aufgenommen? Hat jemand das Smartphone gehackt? Oder ist das alles gar nicht wahr?

Die meisten Menschen haben eine Vorstellung davon, was mit dem Begriff digitale Gewalt gemeint ist. Manche denken an Hass im Netz, andere an Stalking und wieder andere erinnern sich an mit Mini-Kameras heimlich in Festivalduschen aufgenommene Nacktbilder. Tatsächlich gibt es aber keine feste Definition. Die Bilder, die wir dazu im Kopf haben, können sich ganz erheblich voneinander unterscheiden. Allerdings wird Technik noch immer stark geschlechterstereotyp verschieden genutzt – oft sind die Täter Männer, aber natürlich nicht immer.

Der Bundesverband Frauenberatungsstellen und Frauennotrufe (bff) definiert digitale Gewalt folgendermaßen:

„Digitale Gewalt ist ein Sammelbegriff für verschiedene Formen geschlechtsspezifischer Gewalt. Gemeint sind Gewalthandlungen, die sich technischer Hilfsmittel und digitaler Medien

(Handy, Apps, Internetanwendungen, Mails etc.) bedienen und Gewalt, die im digitalen Raum, z. B. auf Online-Portalen oder sozialen Plattformen stattfindet. Wir gehen davon aus, dass digitale Gewalt nicht getrennt von ‚analoger Gewalt' funktioniert, sondern meist eine Fortsetzung oder Ergänzung von Gewaltverhältnissen und -dynamiken darstellt."

Für *Hateaid*, eine gemeinnützige Organisation, die Beratung und rechtliche Unterstützung bei digitaler Gewalt bieten, meint der Begriff „verschiedene Formen von Belästigung, Herabwürdigung, Diskriminierung oder sozialer Isolation im Internet oder mithilfe elektronischer Kommunikationsmittel. Die Orte digitaler Gewalt sind vielseitig: Soziale Netzwerke, Messenger Apps, Chaträume, Gaming-Plattformen oder das E-Mail-Postfach sind nur einige davon."

Klar ist, dass digitale Gewalt viel mehr ist als nur Hass im Netz. Auch die Begrifflichkeiten unterscheiden sich, mit denen häufig die gleichen oder sehr ähnliche Handlungen gemeint sind. Neben digitaler wird von Cyber- oder Online-Gewalt gesprochen, und im englischsprachigen Raum ist häufig von tech-based, also technikbasierter Gewalt die Rede.

Hassrede im Netz – wer ist betroffen?

Auf Social-Media-Plattformen, via Messenger oder E-Mail sind vielen Menschen schon Beleidigungen, Abwertungen oder Verleumdungen begegnet. Auch wenn dies auf den ersten Blick harmlos zu sein scheint, kann diese Hassrede (oft auch mit dem englischen Begriff *Hatespeech* bezeichnet) ernste Auswirkungen haben. Wenn etwa viele Accounts zur gleichen Zeit öffentlich oder nicht öffentlich diffamierende Posts über eine Person oder Gruppe verbreiten, ist eine solche Kampagne für die Betroffenen schwer zu ertragen. Ihre eigenen Online-Aktivitäten können dadurch stark beeinträchtigt sein, weil zwischen dem Shitstorm andere Reaktionen, positive Nachrichten oder Unterstützung nur mühsam gefunden werden. Wenn Social-Media-Accounts beruflich genutzt werden, können die Auswirkungen gravierender sein, etwa wenn nach Verleumdungen oder Falschbehauptungen finanzielle Nachteile entstehen. Menschen, die in der Öffentlichkeit stehen, zum Beispiel Politiker*innen, Journalist*innen, Aktivist*innen oder anders ehrenamtlich Aktive, sind sehr viel stärker von Hatespeech betroffen.

Das US-amerikanische *Pew Research Center*, das regelmäßig Studien zu Online-Belästigung herausgibt, stellte wiederholt fest, dass massivere und sexualisierte Angriffe häufiger Frauen treffen, während Männer von weniger schwerwiegenden Formen häufiger betroffen sind.

Wenn andere Identitäten dazu kommen, wie die Zugehörigkeit zu einer ethnischen oder sexuellen Minderheit, verstärkt das die Schwere der Angriffe. Die Studie „Lauter Hass – leiser Rückzug“ des Kompetenznetzwerks *Hass im Netz* befragte 2023 3.000 Nutzende in Deutschland ab 16 Jahren und kam zu dem Ergebnis, dass Personen mit sichtbarem Migrationshintergrund, junge Frauen und Menschen homosexueller oder bisexueller Orientierung besonders häufig von Hass im Netz betroffen sind. Fast jede zweite Person wurde online schon beleidigt, ein Viertel mit körperlicher und 13 Prozent mit sexualisierter Gewalt konfrontiert. In der Folge äußern mehr als die Hälfte der Befragten seltener ihre politische Meinung und formulieren Beiträge bewusst vorsichtiger.

Digitales Stalking hat viele Formen

Der Übergang von Hass im Netz zum digitalen Stalking ist manchmal fließend. Mit Stalking ist das systematische Überwachen, Verfolgen oder Kontrollieren einer Person mit technischen Mitteln gemeint – oft im sozialen Nahraum und meist ohne Wissen oder Einverständnis der Betroffenen. Stalking findet nicht nur auf Plattformen statt. Genutzt wird alles, was sich dazu eignet, andere aus der Nähe oder Ferne zu beobachten: Kameras, Mikrofone oder Überwachungsapps auf Smartphones, auch bekannt als „Stalkerware".

Stalking ist strafbar – auch digital. Der entsprechende Paragraf 238 des Strafgesetzbuches wurde 2021 so verändert, dass darunter auch explizit das Ausspähen und Abfangen von Daten fällt. Als besonders schwerer Fall gilt, wenn dazu Software oder Apps eingesetzt werden, deren „Zweck das digitale Ausspähen anderer Personen ist". Dies kann eine Freiheitsstrafe von drei Monaten bis zu fünf Jahren nach sich ziehen.

Für den Einsatz von Stalkerware ist der Zugriff auf das Mobilgerät notwendig, um die erforderliche App installieren zu können. Es ist also eine Methode, die vor allem in Partnerschaften oder Ex-Partnerschaften eingesetzt wird.

Die Apps werden relativ offen im Netz als Möglichkeit beworben, die Partnerin (seltener den Partner) vollständig überwachen zu können. Der Verkauf ist legal, aber die Nutzung ist strafbar, wenn die überwachte Person nicht aktiv zugestimmt hat. Einmal installiert, kann fast alles aus der Ferne verfolgt werden: Chats und E-Mails mitlesen, Telefonate mithören und Telefon- und Standortverläufe oder Kalendereinträge nachverfolgen. Es sind dieselben Apps, die auch für Eltern vermarktet werden, um die Aktivitäten ihrer Kinder im Netz beobachten zu können. Auch dies ist problematisch, wenn die Kinder oder Jugendlichen nicht wissen, dass sie überwacht werden. In manchen Fällen wissen die Überwachten zwar vom Einsatz der Software, können sich aber aus Furcht vor Konflikten oder Gewalt der Überwachung nicht entziehen.

Spezielle Software ist aber oft nicht nötig, denn für die Überwachung reicht es aus, wenn der Standort, Passwörter zu Mail-Accounts oder der Cloud geteilt werden. Wenn etwa eine Person der

anderen das Smartphone eingerichtet hat, kennt sie die nötigen Passwörter und PINs. So können selbst technisch nicht versierte Personen ohne zusätzliche Apps verfolgen, wo sich andere befinden. Sie können etwa über gekoppelte Messenger-Apps Nachrichten auf dem Desktop mitlesen oder sich in den Mail-Account einloggen.

Digitale Geräte für die Überwachung im physischen Raum

Weitere Werkzeuge der digitalen Gewalt können Mini-Kameras und -Mikrofone und zunehmend auch verschiedene vernetzte oder „smarte“ Geräte sein, die per App aus der Ferne gesteuert werden können. So kann die ursprünglich zur Sicherheit installierte Videokamera über der Haustür vom inzwischen ausgezogenen Ex-Partner dazu genutzt werden, um weiterhin zu beobachten, wer wann das Haus betritt oder verlässt. Über per App ferngesteuerte Beleuchtung, Heizungen oder Musikanlagen kann Psychoterror ausgeübt werden, wenn immer wieder mitten in der Nacht in voller Lautstärke ein Song abgespielt wird, der Erinnerungen weckt. Kleine mobile Bluetooth-Tracker, bekannt als „Air Tags“ oder „Smart Tags“ kosten mittlerweile nicht viel und können an Fahrzeugen befestigt oder heimlich in Taschen gesteckt werden. Sie verraten dann ständig den Aufenthalt der überwachten Person.

Nicht nur in privaten Wohnräumen gibt es unsichtbare Mini-Kameras. Auf Porno-Plattformen wurden Videoaufnahmen aus Duschen und Toiletten der deutschen Festivals „Monis Rache“ und „Fusion“ aus den Jahren 2016 bis 2019 gefunden, die mithilfe solcher fast unsichtbaren winzigen Kameras gemacht wurden. Die Rapperin und Wissenschaftlerin Lady Bitch Ray kommentierte dazu bei Twitter, dass auch auf Toiletten des Backstage-Bereichs eines Clubs, in dem sie einen Auftritt hatte, solche Mini-Kameras gefunden worden seien.

Für die Betroffenen ist nicht nur belastend, zu erfahren, dass heimlich Nacktaufnahmen von ihnen gemacht wurden, die von

unzähligen fremden Menschen gesehen werden; dazu kommt, dass sie sich selbst – und zwar immer wieder – darum kümmern müssen, solche Aufnahmen von den Plattformen zu löschen.

Zahlen, Lücken, blinde Flecken

Wie groß das Problem ist, also wie häufig Fälle digitaler Gewalt insgesamt vorkommen, lässt sich nicht zuverlässig beantworten. Es fehlen bis heute aussagekräftige empirische Studien. Erhebungen zu Teilbereichen digitaler Gewalt, zu verschiedenen Alters- oder anderen Bevölkerungsgruppen gibt es hingegen immer wieder. Sie verdeutlichen, dass das Problem eklatant ist und weiter zunimmt. So stellte die *UN Broadband Commission* bereits 2015 in einer Studie zu digitaler Gewalt gegen Frauen und Mädchen fest, dass 73 Prozent aller Frauen eine Form digitaler Gewalt erlebt oder beobachtet haben. *Women's Aid UK* befragte 2013 307 Frauen, die häusliche Gewalt erlebt hatten. 45 Prozent gaben an, dass die von ihnen erlebte Gewalt digitale Anteile hatte und 75 Prozent berichteten, dass sie bei der Polizei keine angemessene Unterstützung bekommen hätten.

Die Zahlen der deutschen Polizeilichen Kriminalstatistik wie auch des Hilfetelefons *Gewalt gegen Frauen* des Familienministeriums sind bis heute hingegen vergleichsweise niedrig. Die Ursache dafür liegt vermutlich einerseits darin, dass viele Fälle nicht bei der Polizei angezeigt werden – was bei Gewalt gegen Frauen oft der Fall ist – oder nicht als Fälle digitaler Gewalt erfasst werden. Das Hilfetelefon dokumentierte für das Jahr 2024 26.682 Fälle häuslicher Gewalt, aber nur 540 Fälle digitaler Gewalt, und schreibt selbst dazu: „Digitale Gewalt tritt oft in Verbindung mit analogen Gewaltdynamiken auf." Die niedrige Zahl könnte also ihre Ursache darin haben, dass Fälle je einer Kategorie zugeordnet werden und die große Mehrzahl in erster Linie als häusliche Gewalt erfasst werden. Der wissenschaftliche Dienst des Europäischen Parlaments EPRS kam 2021 zu dem Ergebnis, dass die Gesamtkosten allein von Online-Belästigung und

Online-Stalking zwischen 49 und 89 Milliarden Euro liegen, basierend auf der Annahme, dass vier bis sieben Prozent der Frauen in den EU-Mitgliedsstaaten Online-Belästigung und ein bis drei Prozent Online-Stalking erlebt haben.

Verbände wie der Deutsche Juristinnenbund oder der bff fordern daher seit Jahren verpflichtende Weiterbildungen für die geschlechtsspezifische Dimension digitaler Gewalt für Justiz, Staatsanwaltschaft und Polizei. Anwält*innen wie Beratungsstellen berichten, dass es bei den Anzeigen wie in den folgenden Gerichtsverfahren häufig grundlegend an Verständnis für Dynamiken geschlechtsspezifischer digitaler Übergriffe fehlt. Betroffene sehen sich oft Vorwürfen ausgesetzt, etwa weil sie sich in eine Situation begeben haben, die später vom Täter ausgenutzt wurde. Ein weiteres Problem ist, dass es bei der Polizei in vielen Fällen einerseits an der technischen Ausstattung für eine gerichtsfeste Beweiserhebung fehlt und andererseits am Wissen, wie sie anzuwenden ist. Nur ein Beispiel: Wenn mit Smartphones gemachte Bilder kopiert und neu gespeichert werden, ohne dass der ursprüngliche Zeitstempel erfasst wird, ist später nicht mehr mit Sicherheit feststellbar, wann die Aufnahme gemacht wurde.

Politische Regelungsversuche sind noch nicht ausreichend

So vielfältig die Formen digitaler Gewalt sind, so zahlreich sind die Gesetze, unter die sie fallen können. Das beginnt beim Kunsturhebergesetz, wenn Bilder ohne Einverständnis verbreitet werden, und geht bis zum Strafgesetzbuch mit dem jeweiligen Paragrafen, die Nötigung, Bedrohung, Erpressung, Beleidigung und Verleumdung, das gefährdende Verbreiten personenbezogener Informationen, das Ausspähen und Abfangen von Daten, die Verbreitung pornografischer Inhalte, die Verletzung von Persönlichkeitsrechten oder natürlich Stalking unter Strafe stellt. Dann gibt es noch den Datenschutz und das Telekommunikationsrecht mit dem

sehr spezifischen Paragrafen 8 des „Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten“, der Geräte verbietet, die vortäuschen, ein Haushaltsgegenstand zu sein und dabei aber in der Lage sind, heimlich Bild- oder Tonaufnahmen zu machen. Diese Aufzählung ist nicht vollständig.

Es gibt zwar auch die Möglichkeit, sich zivilrechtlich mit Abmahnungen, Unterlassungsklagen oder einstweiligen Verfügungen zu wehren. Das ist aber mit Kosten verbunden, die die Betroffenen zunächst selbst tragen müssen, ohne zu wissen, ob Aussicht auf Erfolg und damit auf Erstattung der Kosten besteht. Problematisch ist in vielen Fällen, dass es sich um Antragsdelikte handelt. Das bedeutet, dass die betroffene Person einen Strafantrag stellen muss, damit die Ermittlungsbehörden die Tat verfolgen – und zwar innerhalb von drei Monaten nach Kenntnis der Tat.

Die Rechtsanwältin Christina Clemm, die zahlreiche Betroffene von digitaler Gewalt vertritt, schrieb dazu: „In der bisherigen Praxis (Stand 2020) werden die Verfahren wegen digitaler Gewalt meist eingestellt. Dabei wäre Voraussetzung für einen effektiven Schutz insbesondere, dass digitale Gewalt als Gewaltform anerkannt wird und nicht weiter unbeachtet oder bagatellisiert bleibt. Bisher werden Verfahren, Möglichkeiten und Grenzen strafrechtlicher Intervention bei digitaler Gewalt häufig eingestellt, weil die Ermittlungsbehörden und Strafjustiz die Dimension der Verletzung nicht verstehen.“

Zwischen Grundrecht und Grauzone

Durch digitale Gewalt wird eine Reihe von Rechten verletzt, ohne dass den Betroffenen angemessene Unterstützung zuteilwird. Auch wenn wir Grundrechte als Abwehrrechte dem Staat gegenüber begreifen und die digitale Gewalt im sozialen Nahraum oder auf Plattformen in der Regel nicht von staatlichen Institutionen ausgeht, können sie als Orientierung dafür dienen, wie weitreichend die Einschränkungen sind, die von dieser Form der Gewalt ausgehen.

Hass im Netz greift die Meinungsfreiheit an (Art. 5, Absatz 1 des Grundgesetzes) – umso mehr, wenn er in Form von gesteuerten und sich verstärkenden Kampagnen einer großen Zahl von Accounts ausgeht. Der Effekt, dass sich die Angegriffenen zurückziehen und sich öffentlich weniger oder gar nicht mehr äußern, ist vielfach beschrieben worden. Das kann mit erheblichen finanziellen Einbußen einhergehen, wenn sie sich gezwungen sehen, aufgrund von Bedrohungen umzuziehen, die Arbeitsstelle zu wechseln oder als freiberuflich Tätige Aufträge verlieren. Das betrifft insbesondere, aber nicht nur Menschen, die in besonderer Weise in der Öffentlichkeit stehen: Politiker*innen, Journalist*innen, Menschenrechtsverteidiger*innen oder Aktivist*innen.

Für sie, wie für alle Menschen, die digital kommunizieren und im Netz Bedrohungen und Verleumdungen ausgesetzt sind, ist damit auch die freie Entfaltung der Persönlichkeit eingeschränkt (Art. 2, Absatz 1 des Grundgesetzes). Je mehr sich die öffentlichen Diskussionsräume ins Netz verlagern, die wesentlicher Teil der demokratischen Gesellschaft sind, desto gravierender sind die Auswirkungen, wenn sich Menschen aufgrund von Aggressionen aus der Debatte teilweise oder vollständig zurückziehen. Hass im Netz betrifft vorrangig Angehörige von bereits diskriminierten Bevölkerungsgruppen. Wenn ihre Perspektive in öffentlichen Debatten unterrepräsentiert ist, geraten diese Diskurse in gefährliche Schieflagen.

Auch das Grundrecht auf Gleichberechtigung in Artikel 3 des Grundgesetzes kann durch digitale Gewalt angegriffen werden. Er besagt explizit, dass der Staat auf die Beseitigung bestehender Nachteile hinwirkt. Absatz 2 betrifft die Benachteiligung von Frauen, Absatz 3 weitere Formen von Diskriminierung. Genau diese spielen bei Hass im Netz und bei Gewalt im sozialen Nahraum eine Rolle. Von beidem sind Frauen stärker betroffen – und LGBTIQ-Personen müssen im Fall von Hass im Netz mit wesentlich heftigeren Angriffen rechnen.

Zu guter Letzt ist das Post- und Fernmeldegeheimnis durch Artikel 10 des Grundgesetzes geschützt. Jede Form der heimlichen oder erzwungenen Überwachung der digitalen Kommunikation verletzt dieses Grundrecht. Wir verändern unser Verhalten, wenn wir uns beobachtet fühlen. Deshalb ist es für die Entfaltung der Persönlichkeit zentral, frei von jeglicher unerwünschter digitaler Überwachung und Beobachtung zu sein.

Was jetzt nötig wäre – gesetzlich, institutionell, gesellschaftlich

Die Vorschläge, wie Betroffene durch digitale Gewalt besser geschützt werden können, liegen seit Langem auf dem Tisch. 2014, vor über 10 Jahren, forderte die GFMK (Konferenz der Gleichstellungs- und Frauenministerien der Bundesländer) Maßnahmen wie bessere Beratung, Fortbildung für Polizei und Justiz oder konkrete Veränderung wie die Novellierung der Impressumspflicht, die bis heute Soloselbstständige und Blogger*innen verpflichtet, ihre Wohnadresse auf ihrer Website anzugeben, wenn sie keine separate Büroadresse haben. Im Juni 2025 forderte die GFMK die Bundesregierung zum wiederholten Mal auf, Betroffene und Berater*innen zu digitaler Gewalt im sozialen Nahraum nachhaltig zu unterstützen, um dieser Gewaltform adäquat zu begegnen.

Die Ampel-Koalition hatte 2021 im Koalitionsvertrag vereinbart, Hürden für Betroffene mit einem „Gesetz gegen digitale Gewalt" abzubauen. Endlich bewegt sich etwas, dachten viele, die seit Jahren mit dem Thema befasst waren, und hofften, dass das Thema endlich die nötige politische Aufmerksamkeit bekommen würde. Diese Hoffnung zerschlug sich bald.

Als die Bundesregierung Ende 2023 in einer Kleinen Anfrage der Linksfraktion gefragt wurde, ob sie eine Definition habe, lautete die Antwort: „[B]ei dem Begriff ‚digitale Gewalt' handelt es sich um einen rechtlich bisher nicht definierten Fachbegriff, unter dem verschiedene Formen von Angriffen auf Personen und Personengruppen, insbesondere durch Herabsetzungen, Rufschädigung, Nötigung, Erpressung, Bedrohung und soziale Ausgrenzung verstanden werden, die im digitalen Raum, also insbesondere auf Online-Portalen und sozialen Plattformen, über Messenger-Dienste oder auch über E-Mail-Dienste, begangen werden." Es sollte also ein Gesetz geben, ohne dass den Verantwortlichen klar war, welches Problem eigentlich gelöst werden sollte.

Es kam dann auch gar nicht zustande. Bis zum Ende der Ampel gab es lediglich Entwürfe des Justizministeriums, denen zu entnehmen war, dass gar nicht beabsichtigt war, sich umfassend mit den

Auswirkungen digitaler Gewalt zu befassen. Das Vorhaben wurde von Verbänden und auch der GFMK heftig kritisiert. Das geplante Gesetz sollte Betroffenen nur helfen, Auskunft über die Identität von Verfassern rechtswidriger Inhalte zu erlangen, um bei Klagen größere Aussichten auf Erfolg zu haben. Die noch im Koalitionsvertrag angekündigten umfassenden Beratungsangebote wurden nicht mehr erwähnt. Weitere Auswirkungen digitaler Gewalt, die letztlich bis zum Femizid führen kann, wurden nicht betrachtet. Auch die neue Koalition aus SPD und CDU/CSU hat sich ein solches Gesetz vorgenommen. Ob und wie sie dabei auf die bereits geäußerte Kritik eingehen will, ist derzeit noch nicht erkennbar.

Gleichzeitig wird die neue Bundesregierung die 2024 beschlossene EU-Richtlinie zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt bis Mitte 2027 umsetzen müssen. Die Richtlinie enthält sehr konkrete und umfassende Vorgaben zur Bekämpfung digitaler Gewalt über die reine Festlegung der Strafbarkeit einzelner Delikte hinaus. Thematisiert werden bildbasierte Gewalt, digitale Formen des Stalkings sowie Hass im Netz. Polizei und Justiz sollen über Fachwissen und wirksame Ermittlungsinstrumente verfügen, um elektronische Beweise erheben zu können; Weiterbildungen sollen verpflichtend, Beratungsstellen besser ausgestattet und Opfer unterstützt werden. Außerdem werden regelmäßige Datenerhebungen vorgeschrieben. Dazu wäre Deutschland durch die Ratifizierung der Istanbul-Konvention zwar schon seit Jahren verpflichtet, ist dem allerdings bisher nicht nachgekommen.

Verbände wie der *Bundesverband Frauenberatungsstellen und Frauennotrufe* und die *Frauenhauskoordinierung* weisen immer wieder darauf hin, dass angemessene Ressourcen für die Beratung von Betroffenen von geschlechtsspezifischer Gewalt erforderlich sind. Hier sind die Budgets immer schon knapp, sodass die zusätzliche Expertise, die benötigt wird, um Betroffene bei digitalen Formen von Gewalt zu unterstützen, oft nicht geleistet werden kann. Zudem erfordert sie ständige eigene Weiterbildung, weil sich das Feld stetig verändert. Für komplexe technische Hilfestellungen wie forensische Untersuchungen der Geräte von Betroffenen sollte es eigene IT-Kompetenzzentren geben, die die Beratungsstellen bei Bedarf konsultieren können.

Viele gesetzliche Regelungen stammen aus einer Zeit vor dem Internet. Allein für die bildbasierte digitale Gewalt – also etwa heimliche

Aufnahmen durch Mini-Kameras oder Drohnen, das Filmen von Vergewaltigungen, das Veröffentlichen oder Verschicken ehemals konsensuell erstellter intimer Aufnahmen (Revenge Porn), Deepfakes (mit künstlicher Intelligenz erzeugte Videos) – ist der juristische Rahmen so zerfasert, dass der Juristinnenbund in einem Policy Paper fordert, dass „ein einheitlicher Regelungskomplex von Straftatbeständen innerhalb des Sexualstrafrechts und außerhalb des Pornografiestrafrechts geschaffen wird, der das unbefugte Herstellen, Gebrauchen, Zugänglichmachen und Manipulieren von Bildaufnahmen unter Strafe stellt, die eine andere erwachsene Person nackt oder sexualbezogen wiedergeben."

Genauso notwendig ist eine gesellschaftliche Diskussion, die die Formen und Folgen digitaler Gewalt ernst nimmt und nicht als individuelles Problem betrachtet. In einer sich immer weiter digitalisierenden Gesellschaft muss Aufklärung über die und Beschäftigung mit den daraus resultierenden Gefahren, Umgehensweisen und nötige Hilfestellung selbstverständlich sein, und zwar für alle Altersgruppen, beginnend mit dem Moment, in dem digitale Geräte benutzt werden. Eine Politik, die Bereitschaft zum Umgang mit digitalen Methoden erwartet, muss die nötigen Mittel für die Bewältigung der Probleme bereitstellen.

Anne Roth ist Diplom-Politologin und lebt in Berlin. Bis zur Auflösung im Dezember 2023 war sie Referentin der Linksfraktion im Bundestag für digitalpolitische Themen, zuerst als Referentin für den NSA-Untersuchungsausschuss 2014 – 2017, dann als Referentin für den Digitalausschuss. Seitdem beschäftigt sie sich freiberuflich mit digitalen Grundrechten. Ihre Themen sind digitale Gewalt, digitale Teilhabe, Ein- und Ausschlüsse, Diskriminierung, digitale Überwachung und sichere Kommunikation sowie die Entzauberung aktueller Buzzwords im Kontext der Digitalisierung.

Zum Weiterlesen

- bff: Bundesverband Frauenberatungsstellen und Frauennotrufe, Nivedita Prasad (Hg.): Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung. Formen und Interventionsstrategien, transcript Verlag, 2021.
- Bundesverband Frauenberatungsstellen und Frauennotrufe (bff): Digitale Medien, Digitale Welten, Digitale Gewalt (Broschüre), überarbeitete Neuauflage 2024.
- Frauenhauskoordinierung e. V.: Infosheet Digitale (Ex-)Partnerschaftsgewalt in Frauenhäusern, 2025.
- Habringer, Magdalena; Hoyer-Neuhold, Andrea; Messner, Sandra: (K)ein Raum. Cyber-Gewalt gegen Frauen in (Ex-)Beziehungen: Forschungsbericht, FH Campus Wien, 2023.
- Roth, Anne: Digitale Gewalt: überall und nirgends: Polizei und Justiz sind für Frauen nur selten eine Hilfe, In: Bürgerrechte & Polizei/CILIP 126, 2021.

Zugang zu Wissen und digitalen Inhalten

Saskia Ostendorff

Gemeinfreiheit – Anspruch auf Zugang zu digitalen Kulturgütern als Grundrecht

In einer globalisierten Welt, in der kulturelle Vielfalt und der Schutz von Kulturerbe eine immer größere Rolle spielen, muss der Zugang zu Kulturgütern ein Grund- und Menschenrecht sein. Kulturgüter – sei es in Form von Kunstwerken, Denkmälern oder immateriellem Erbe wie Sprache und Traditionen – spiegeln die Identität und Geschichte von Gemeinschaften wider und tragen entscheidend zur individuellen und gesellschaftlichen Entwicklung bei. Community-Plattformen wie *Wikipedia*, *Wikidata* und *Wikimedia Commons* tragen dazu bei, dass die Schwelle zum Zugang zu Kulturgütern gesenkt wird. Jedoch stehen gerade diese durch freiwillige Arbeit existierenden Projekte immer wieder vor der Herausforderung, diesen Zugang zu verteidigen. Am Beispiel der Himmelsscheibe von Nebra, einem UNESCO-Weltdokumentenerbe, wird deutlich, wie sehr noch heute das Grund- und Menschenrecht zur Teilhabe und der Zugang zu digitalen Kulturgütern erschwert wird.

Zugang und Teilhabe zu Kulturgütern als Menschenrecht

Nach Artikel 27 der Allgemeinen Erklärung der Menschenrechte hat jeder das Recht, am kulturellen Leben der Gemeinschaft frei teilzunehmen, sich der Künste zu erfreuen und am wissenschaftlichen Fortschritt und dessen Wohltaten teilzuhaben. Nach wie vor findet sich dieser ausdrückliche Schutz nicht im Grundgesetz, obwohl er eigentlich grundgesetzlich verankert sein sollte. Im ersten Satz des Artikels 5 des Grundgesetzes findet sich lediglich die Informationsfreiheit, die sich auf allgemein zugängliche Quellen bezieht („Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten“), und in Absatz 3 die Freiheit der Kunst und Wissenschaft („Kunst und Wissenschaft, Forschung und Lehre sind frei“).

Das bedeutet: Der Staat hat nicht nur die Pflicht, kulturelle Angebote zu ermöglichen, sondern auch dafür zu sorgen, dass alle

Menschen sie tatsächlich nutzen können – unabhängig von Einkommen, Herkunft oder Bildung. Dieser Anspruch auf kulturelle Teilhabe wird jedoch oft durch urheberrechtliche Schranken begrenzt. Denn selbst wenn ein Kulturgut theoretisch öffentlich zugänglich ist, heißt das nicht automatisch, dass es auch weiterverwendet oder verbreitet werden darf. Hier klaffen Anspruch und Realität häufig auseinander.

Wikimedia Commons

Wikimedia Commons hilft dabei, die Lücke zum Zugang zu kulturellen Gütern durch digitalisierte Werke zu schließen. Die Plattform dient als zentrale Quelle für frei verwendbare Bilder, Videos, Audiodateien und andere Medieninhalte, die von der Öffentlichkeit hochgeladen werden. Das Projekt wird durch Freiwillige getragen, die Bilder und andere Werke von Kulturgütern auf Wikimedia Commons hochladen und somit für jeden nachnutzbar machen. Hierbei ergeben sich regelmäßig urheberrechtliche Fragestellungen dazu, unter welchen Bedingungen Bilder kultureller Güter auf der Plattform zulässig sind oder nicht.

Die Himmelsscheibe von Nebra

Ein Beispiel für eine solche Herausforderung ist ein auf Wikimedia Commons hochgeladenes Foto der Himmelsscheibe von Nebra**.** Sie gilt als die älteste bekannte Darstellung des Himmels und ist eine archäologische Sensation. Sie zeigt eine präzise Darstellung von Sonne, Mond und Sternen, die auf das Jahr 1600 v. Chr. datiert wird. Seit ihrer Entdeckung fasziniert sie Menschen weltweit, nicht nur wegen ihres Alters, sondern auch wegen ihres kulturellen und historischen Werts. Tatsächlich wurde die Himmelsscheibe von der UNESCO als Weltdokumentenerbe anerkannt und gehört damit zum kulturellen Erbe der gesamten Menschheit. Die

Himmelsscheibe von Nebra ist schon lange gemeinfrei – Werke werden laut Paragraf 64 des Urheberrechtsgesetzes 70 Jahre nach dem Tod des Urhebers gemeinfrei. Das ist bei der Himmelsscheibe von Nebra unstreitig der Fall.

Das Foto der Himmelsscheibe von Nebra, das auf der Website von Wikimedia Commons zu sehen ist, wurde in einer Ausstellung vom Originalfoto der Himmelsscheibe von Nebra abfotografiert – es ist also das Foto eines Fotos. Hierbei stellen sich auf mehreren Ebenen rechtliche Fragen. Zum einen ist es fraglich, ob das ursprüngliche Foto der Himmelsscheibe von Nebra durch den Fotografen Juraj Liptak urheberrechtlichen Schutz genießt. Zum anderen beruft sich das Land Sachsen-Anhalt als Rechteinhaberin auf den Paragrafen 71 des Urheberrechtsgesetzes. Danach erhält derjenige, der erstmals ein bisher nicht veröffentlichtes Werk veröffentlicht, ein sogenanntes Leistungsschutzrecht. Es gilt für eine Dauer von 25 Jahren ab dem Zeitpunkt der Veröffentlichung. Die Regelung soll Anreize schaffen, historische Werke zu erschließen und zu veröffentlichen. Allerdings wird damit die weitere Nachnutzung erschwert, weil hierzu Lizenzen erworben werden müssen.

Bei der Himmelsscheibe von Nebra ist fraglich, ob es überhaupt das Land Sachsen-Anhalt war, das sie erstmals im Jahr 2002 öffentlich zugänglich gemacht hat. Sie wird aller Wahrscheinlichkeit nach bereits vor 2002 der Öffentlichkeit bekannt gewesen sein. Problematisch an der Regelung ist in jedem Fall, dass dadurch eine Institution über ein gemeinfreies Werk ein Ausschließlichkeitsrecht erhält.

Diese Gesetzeslage hat zur Folge, dass das Urheberrecht beziehungsweise Leistungsschutzrecht mit dem Zugang und der Nachnutzung des Fotos der Himmelsscheibe von Nebra kollidiert.

Vervielfältigungen von gemeinfreien Werken sollten gemeinfrei bleiben

Durch die Beanspruchung des urheberrechtlichen Schutzes auf das Foto der Himmelsscheibe von Nebra wird die eigentliche Gemeinfreiheit der Himmelsscheibe ausgehöhlt. Dadurch, dass das Land Sachsen-Anhalt hier ein Leistungsschutzrecht geltend macht, wird der freie Zugang zu dem digitalisierten Kulturgut beschnitten.

Der Gesetzgeber hat 2021 mit der Einführung des Paragrafen 68 des Urheberrechtsgesetzes (die deutsche Umsetzung des Artikels 14 der *Digital Single Market Directive* der EU) erkannt, dass der Widerspruch zwischen der Vervielfältigung von gemeinfreien Werken und einem Leistungsschutzrecht aufgehoben werden muss. Das hat dazu geführt, dass ein Leistungsschutz bei der Vervielfältigung gemeinfreier visueller Werke nicht geltend gemacht werden kann. Daraus folgt, dass sich das Land Sachsen-Anhalt bei der Himmelsscheibe gerade nicht auf ihr behauptetes Leistungsschutzrecht berufen könnte.

Nach der gegenwärtigen Rechtsprechung könnte das Foto der Himmelsscheibe von Nebra (durch den Fotografen Juraj Liptak) zusätzlich urheberrechtlichen Schutz als Lichtbildwerk genießen. Dem ließe sich allerdings entgegenhalten, dass das Foto unter anderem zur Dokumentation eines UNESCO-Weltdokumentenerbes erstellt wurde. Es wurde ein öffentlicher Auftrag zur Erhaltung, Sicherstellung und Archivierung von Kulturgut wahrgenommen. Auf dieser Basis könnte man argumentieren, dass es sich bei dem Foto der Himmelsscheibe von Nebra um ein amtliches Werk im Sinne des Paragrafen 5 des Urheberrechtsgesetzes handelt, das keinen Urheberrechtsschutz genießt. Erst wenn anerkannt wird, dass Vervielfältigungen von Kulturgütern wie der Himmelsscheibe von Nebra durch eine Fotografie keinen Urheberrechtsschutz genießen, wäre die kulturelle Teilhabe vollständig gewährleistet. Bei einer anderen Auffassung würde dies dem Menschenrecht nach Art. 27 der Allgemeinen Erklärung der Menschenrechte widersprechen.

Aufgrund dessen, dass das Grundgesetz keine ausdrückliche Verankerung dieses Rechts kennt, ist es umso wichtiger, dass Fotos

von Kulturgütern in allgemein zugänglichen Quellen zur Verfügung gestellt werden. Dies kann entweder durch die Wahrnehmung der Aufgabe durch Kultureinrichtungen wie Museen selbst erfolgen, oder aber durch freiwillige Projekte wie *Wikimedia Commons*. Insbesondere der digitale Zugang zu kulturellen Gütern senkt die Barrieren, die durch Eintrittsgelder für Museen oder fehlende kulturelle Angebote in ländlichen Regionen existieren. Dadurch wird allen Menschen weltweit der Zugang zu kulturellen Gütern ermöglicht. Es lassen sich dadurch auch geografische Barrieren abbauen. Open-Access-Plattformen wie Europeana oder *Wikimedia Commons* machen kulturelles Erbe weltweit zugänglich.

Fazit: Es braucht ein Grundrecht auf digitale kulturelle Teilhabe

Der Zugang zu Kulturgütern ist ein Menschenrecht, das gemäß Art. 27 der Allgemeinen Erklärung der Menschenrechte jedem Menschen die kulturelle Teilhabe garantieren sollte. Allerdings zeigt sich in der Praxis, dass rechtliche und institutionelle Hürden diesen Zugang häufig erschweren, insbesondere im Spannungsfeld zwischen Urheberrechten und der Gemeinfreiheit von kulturellen Gütern. Digitale Plattformen wie Wikimedia Commons tragen entscheidend dazu bei, diese Hürden zu überwinden und kulturelles Erbe weltweit zugänglich zu machen.

Das Beispiel der Himmelsscheibe von Nebra verdeutlicht allerdings die Problematik, wenn rechtliche Ansprüche den freien Zugang zu gemeinfreien Kulturgütern einschränken. Die Einführung des Paragrafen 68 im Urheberrechtsgesetz stellt einen wichtigen Schritt zur Sicherung der Gemeinfreiheit digitalisierter Werke dar. Dennoch bedarf es weiterer rechtlicher und institutioneller Maßnahmen, um eine umfassende kulturelle Teilhabe sicherzustellen. Neben der erforderlichen gesetzlichen Verankerung im Grundgesetz sind insbesondere Open-Access-Initiativen und Freiwilligenprojekte wie *Wikimedia Commons* unerlässlich, um kulturelle Barrieren zu senken und geografische sowie

finanzielle Hürden abzubauen. Damit wird der digitale Zugang zu Kulturgütern nicht nur erleichtert, sondern auch ein wichtiger Beitrag zur Verwirklichung des Menschenrechts auf kulturelle Teilhabe geleistet. Auch im Grundgesetz sollte das Grundrecht auf digitale kulturelle Teilnahme explizit verankern – es könnte wie folgt lauten: *Art. 5 Abs. 4 Jeder Mensch hat einen Anspruch auf kulturelle Teilhabe.*

Dr. Saskia Ostendorff ist Rechtsanwältin und arbeitet als General Counsel bei Wikimedia Deutschland e. V. Sie ist Expertin für Persönlichkeitsrechte im digitalen Raum, Freiheitsrechte sowie für die Bereiche Open Data, Open Access und Open Source. Mit einem klaren Fokus auf strategische Prozessführung und Politikberatung setzt sie sich für die Verteidigung digitaler Rechte und die Förderung des freien Zugangs zu Informationen ein.

Fabian Rack

Zugang zu kulturellen Gütern und Creative Commons

207

Im Kontext eines möglichst ungehinderten Zugangs zu kulturellen Gütern spielt insbesondere die Informationsfreiheit als Bestandteil der Meinungsfreiheit eine Rolle. Sie besagt, dass der Staat nicht willkürlich in das Recht der Allgemeinheit eingreifen darf, sich aus allgemein zugänglichen Quellen zu bedienen und zu unterrichten. Allerdings ergibt sich aus Grundrechten keine generelle Pflicht von Kulturinstitutionen, kulturelle Güter zu digitalisieren und diese Digitalisate der Allgemeinheit zugänglich und nutzbar zu machen.

Gleichzeitig operieren Kulturinstitutionen vielfach in öffentlicher Trägerschaft in gesetzlichem Auftrag, wobei letzterer auch die Zugänglichmachung von Materialien beinhalten kann. Dann stellt sich nicht nur die Frage über das Ob, sondern auch über das Wie – also unter welchen Bedingungen kulturelle Werke der Allgemeinheit zur Verfügung gestellt werden.

Vor allem für Werke, die frei von Urheberrechten sind, wird es interessant. Denn sind auch die digitalen Reproduktionen kultureller Güter frei von Urheberrechten, kann man sie nicht nur betrachten, sondern auch nutzen: Sie können zum Beispiel in offene Bildungsmaterialien (*Open Educational Ressources*, kurz OER) eingebunden, frei geremixed, in einem geschichtlichen Youtube-Kanal verwendet oder in die Wikipedia eingestellt werden. Was auch immer dabei entsteht – es ist Ausdruck von Kommunikationsfreiheiten wie der Meinungs- und Kunstfreiheit, auch fremde Materialien zu nutzen.

Dabei muss man allerdings wissen, was bei der Nutzung kultureller Güter erlaubt ist. Hier spielt *Creative Commons* (CC) eine wichtige Rolle. Ursprünglich vor 25 Jahren aus dem Open-Source-Gedanken als Lizenzmodell für Kreative zur Freigabe von kreativen Inhalten im Netz entwickelt, hat sich CC mit der Zeit auch in den Bereichen Wissenschaft und Kulturerbe als Instrument der „Openness“ fest etabliert.

Wie kam es zu Creative Commons – und was ist CC?

Ende der 1990er-Jahre wurden in den USA Schutzfristen im Urheberrecht verlängert, was insbesondere der Disney-Konzern vorangetrieben hatte (damals spöttisch „Mickey Mouse Protection Act“ genannt). Viele Aktive hatten eigentlich geplant, Werke, die bald gemeinfrei geworden wären, im Netz frei zugänglich zu machen. Doch durch die Verlängerung der Schutzfristen verschob sich die Grenze um mehrere Jahrzehnte.

Um immer strengeren Urheberrechtsgesetzen und ihrer Durchsetzung im Netz eine Alternative entgegenzusetzen, entstand die Idee, ein Werkzeug dafür zu schaffen, Urheberrechte freizugeben – und dies laienverständlich. Vor allem hatten und haben bei Weitem nicht alle dieselben Anliegen wie die Kreativindustrie. Man wollte transformative Nutzungen ermöglichen, was schließlich zur Kulturtechnik im Netz geworden war. Vor diesem Hintergrund entstand CC. Eine Gruppe um den Juraprofessor Lawrence Lessig veröffentlichte 2002 die erste Version der CC-Lizenzen. Mittlerweile sind wir bei Version 4 mit einem weltweiten Netzwerk und dem Anspruch, Inhalte weltweit rechtssicher teilen zu können.

Bei der Ursprungsidee, dass Kreative ihre Inhalte für die Allgemeinheit freigeben können, blieb es. Hinzu kam über die Jahre, dass CC mittlerweile institutionell verankert ist. So auch beim Teilen kultureller Güter: Dort ist die Rechtslage bezüglich der Urheberrechte etwa bei deren digitaler Abbildung oft kompliziert. Der Einsatz der CC-Instrumente kann da Nutzungsfreiheiten schaffen, wo sie ansonsten nicht wären.

Urheberrecht und Gemeinfreiheit – wo beginnt der Nutzungsspielraum?

Allgemein sind Bücher, Fotografien, Skulpturen und sonstige Werke aus der Zeit vor dem 20. Jahrhundert mit starker Tendenz „gemeinfrei“, denn Urheberrechte erlöschen 70 Jahre nach dem Tod der Person, die das Werk geschaffen hat. Gemeinfrei, das heißt: frei von Urheberrechten. Mit der Gemeinfreiheit steht der Nutzung dieser Werke zumindest rechtlich nichts mehr entgegen.

Bedeutet dies also, dass, wenn ich zum Beispiel ein Foto einer antiken Skulptur vorfinde, ich das Foto in Bildungsmaterialien einbinden oder auf meinem Blog nutzen darf, weil diese Skulptur ja schließlich alt genug ist? Leider ist die Situation etwas komplizierter. Gerade in den vergangenen Jahren wurde debattiert, ob bei der Reproduktion eines gemeinfreien Werks ein eigenes Schutzrecht entsteht – sprich, ob die Abbildung von etwas Ungeschütztem dann doch wieder geschützt sein kann.

„Faithful Reproductions“

Einen Höhepunkt fand die Diskussion in einem Urteil des Bundesgerichtshofs zum Fall des Mannheimer Reiss-Engelhorn-Museums im Jahr 2018 um das Reproduktionsfoto eines Gemäldes, das Richard Wagner zeigte. Das Museum konnte Wikimedia die Nutzung einer Reproduktionsfotografie des Gemäldes untersagen. Es trug damals erfolgreich vor, dass durch die Fotografie ein rechtlich geschütztes „Lichtbild“ entstanden war – obwohl das abgebildete Werk gemeinfrei war.

Wenig später wurde im europäischen Urheberrecht eine Regelung geschaffen, wonach Exklusivrechte durch die wirklichkeitsgetreue Reproduktion von gemeinfreien Werken der bildenden Kunst ausgeschlossen wurden (diese Regelung wird auch im Beitrag von Saskia

Ostendorff in diesem Band beschrieben). Dies sollte den Zugang und die Förderung von Kultur unterstützen und den Zugang zum europäischen Kulturerbe sichern. Aus Nutzungssicht war dies eine erfreuliche Entwicklung, denn es bedeutete von nun an: Es ist Verlass darauf, dass gemeinfrei bleibt, was gemeinfrei ist. Es hilft auch der Meinungs- und Kunstfreiheit, wenn die Nutzung solcher Materialien für die Allgemeinheit rechtssicher erlaubt ist. Der Fall des Richard-Wagner-Gemäldes ist heute also klar – auch das Reproduktionsfoto ist gemeinfrei.

Die Rolle von CC in der Praxis – zwischen Recht, Ethik und Alltag

Creative Commons kommt hier nun auf zweierlei Wegen ins Spiel: Zum einen lässt sich mithilfe der sogenannten „Public Domain Mark“ zum Ausdruck bringen, dass das Werk – und seine Reproduktion – gemeinfrei sind. Dabei handelt es sich um eine Kennzeichnung, mit der die teilende Institution den Status als gemeinfrei zumindest unverbindlich kenntlich machen kann. Wer also Materialien nutzen will und das Icon mit der Public Domain Mark (PDM) sieht, kann davon ausgehen, dass das Material gemeinfrei ist.

Zum anderen hat CC in den vergangenen Jahren umfangreich dazu beigetragen, dass Kulturinstitutionen bewusst wurde, wie wichtig gemeinfreie Inhalte für die Kultur sind. Es hat für die komplizierten Fragestellungen sensibilisiert und Bildungsangebote geschaffen oder bei der Initiative *OpenGLAM* mitgewirkt (GLAM steht für Galleries, Libraries, Archives, Museums). So bietet die Organisation CC ein „CC Certificate for Open Culture“ an, bei dem sich Institutionen über den Einsatz der CC-Instrumente schulen lassen können, um Sammlungen so offen wie möglich halten zu können. Auf der Plattform *Europeana* beispielsweise finden sich zahlreiche offen zur Verfügung gestellte Materialien.

Manchmal Schutzrechte

Und wie ist es mit dem vorher geschilderten Fall – dem Foto der antiken Skulptur, die ich für meinen Blog verwenden wollte? Er ist leider auch unter geltender Rechtslage nicht zweifelsfrei zugunsten der Nutzungsfreiheiten gelöst. Denn in Fällen wie diesem kommt weiterhin unter Umständen bei Reproduktionen ein Schutz nach Urheberrecht infrage: Trifft ein*e Fotograf*in kreative Entscheidungen zur Wahl von Perspektive, Lichtsetzung, Bildausschnitt oder der Anordnung von Objekten als Bildmotiv, so kann dadurch eine eigene schöpferische Prägung und damit ein Urheberrecht am Foto entstehen.

Die Abgrenzung von „geschützt“ und „nicht geschützt“ fällt selbst dem juristisch geschulten Blick häufig schwer – und wird sogar mit wachsender rechtlicher Expertise umso schwieriger. Viele Kulturinstitutionen entscheiden sich deshalb, Materialien explizit frei nutzbar zu machen. Hierfür nutzen sie die CC-Lizenzen. Mit ihnen wird gesagt: Diese Materialien dürfen kostenlos genutzt werden. Dabei gibt es ein Set unterschiedlicher Bedingungen (allem voran die Namensnennung und Anbringung des sogenannten Lizenzhinweises, „BY – Attribution“), die vielfach im Netz erläutert werden.

Die Organisation Creative Commons empfiehlt im Bereich Open GLAM generell den Einsatz von „CC0“ (CC Zero). Hierbei handelt es sich um eine bedingungslose Freigabe der Materialien. Diese Empfehlung wird auch deshalb ausgesprochen, weil die Rechtslage gerade in den Fällen der Reproduktion international oft nicht einheitlich ist und CC0 dann für eine weltweite Freigabe steht. Wer also kulturelle Güter unter CC0 vorfindet, kann sie urheberrechtlich gesehen ohne jegliche Einschränkung nutzen.

Die CC-Instrumente helfen, illegitime Schutzrechte zu verhindern

Creative Commons steht seit jeher dafür, dass keine neuen Schutzrechte durch Digitalisierung entstehen sollen. Dies ist nicht zuletzt auch eine Frage der Sensibilität im Umgang mit kulturellen Gütern. Die ethischen Leitlinien der OpenGLAM-Initiative fordern explizit, bei der Digitalisierung gemeinfreier Kulturgüter keine neuen Schutzrechte zu schaffen. Damit soll verhindert werden, dass gemeinfreie kulturelle Güter durch die Digitalisierung „re-privatisiert" werden. Auch in diesem Sinne sind die CC-Instrumente eine Freigabe.

Freilich sollten diese Perspektiven auch aus Nutzungsperspektive geachtet werden. Hierin liegt zugleich die Grenze der CC-Instrumente, denn sie treffen Aussagen zum Urheberrecht, nicht aber zu ethischen Belangen und auch nicht zu Persönlichkeitsrechten etwa von abgebildeten Menschen auf historischen Fotos.

Aktuelle Debatten – KI, Reziprozität und neue Herausforderungen

Derzeit wird vor diversen Gerichten verhandelt, inwieweit vor allem kommerzielle KI-Systeme ihre Modelle mit Texten und Bildern trainieren dürfen. Das Thema KI spielt auch bei Creative Commons eine Rolle. Vor allem stellt sich die Frage, ob das CC-Lizenzset durch ein Verbot von KI-Training ergänzt werden soll. Dies scheint aber in der CC-Community bisher kein Konsens zu sein. Denn statt auf Verbote zu setzen, arbeitet die Organisation CC derzeit an sogenannten „Preference Signals".

Damit können beim Freigeben von Inhalten Institutionen ihre Wünsche für die KI-Nutzung kenntlich machen – etwa neben dem Wunsch nach Namensnennung, einer Kompensation oder einem Verbot für bestimmte Zwecke. Wie CC-Direktorin Catherine Stihler es formuliert, geht es darum, im Zeitalter von KI eine neue Form der Reziprozität zu finden – ein Geben und Nehmen, das die Interessen der Allgemeinheit und der Schaffenden ausbalanciert. Allerdings hat die Diskussion gerade erst begonnen. Auch Kulturinstitutionen fragen sich, ob sie das ungefragte Scraping ihrer Inhalte zulassen oder verhindern sollen.

Fazit: Nutzungsfreiheiten ermöglichen

Wer kulturelle Güter nutzt, muss über den urheberrechtlichen Status der Materialien Bescheid wissen – was häufig schwierig ist. Die Instrumente von CC sind für Kulturinstitutionen eine Möglichkeit, den Kommunikationsgrundrechten und freiem kreativen Schaffen dienend zur Seite zu stehen.

Fabian Rack ist wissenschaftlicher Mitarbeiter bei FIZ Karlsruhe (Leibniz-Institut für Informationsinfrastruktur) und Anwalt bei iRights.Law in Berlin. Er ist aktives Mitglied des deutschen Chapters von Creative Commons. Er produziert Musik unter dem Künstlernamen Inoti.

Viktoria Kraetzig

Drei Fragen zum „Zensur-heberrecht“

Was ist mit „Zensurheberrecht“ gemeint?

Der Begriff beschreibt eine gängige Praxis, in der das Urheberrecht als „Zensurrecht“ instrumentalisiert wird: Privatpersonen oder der Staat machen einen urheberrechtlichen Unterlassungsanspruch wegen einer Verletzung ihrer Verwertungsrechte geltend, um eine unerwünschte Presseveröffentlichung zu unterbinden. Dabei geht es den von der Berichterstattung Betroffenen gar nicht um die Durchsetzung ihres Urheberrechts, sondern nur darum, eine unliebsame Veröffentlichung aus der Welt zu bekommen. Die Motivation dahinter variiert – Privatpersonen sehen sich in ihrem Persönlichkeitsrecht verletzt, der Staat möchte Informationen unter Verschluss halten. Es sind in der Regel Fälle, in denen ein äußerungsrechtlicher Unterlassungsanspruch angebracht wäre. Das Äußerungsrecht sieht nämlich Rechtsbehelfe für Betroffene von rechtswidrigen Äußerungen vor, zum Beispiel, weil diese ehrverletzend sind. Beim Unterlassungsanspruch aus Äußerungsrecht ist jedoch eine grundrechtliche Interessenabwägung vorzunehmen. Insoweit wägen die Gerichte etwa das Persönlichkeitsrecht des Betroffenen mit der Pressefreiheit des veröffentlichenden Mediums und dem öffentlichen Informationsinteresse an der Berichterstattung ab.

Die Kommunikationsgrundrechte wie Meinungsfreiheit und Informations- und Pressefreiheit nehmen einen hohen Rang im demokratischen Verfassungsstaat ein. Sie sind die Lebensluft für den öffentlichen Diskurs und den Meinungsbildungsprozess. An ihnen wird der äußerungsrechtliche Unterlassungsanspruch oft scheitern. Um diese Abwägung zu umgehen, stützten die Betroffenen ihren Anspruch auf das Urheberrecht. Es kennt nur in eng umrissenen Ausnahmefällen eine grundrechtliche Interessenabwägung, nämlich wenn eine der sogenannten „Schranken“ greift. Diese „Schranken“ hat der Gesetzgeber in das Urheberrechtsgesetz aufgenommen, damit zumindest in engen Grenzen eine Nutzung von urheberrechtlichen Schutzgegenständen möglich ist. Die „Schranken“ setzen dem Urheberrecht also Schranken. Das wohl prominenteste Beispiel ist die Schranke für Zitate, die es erlaubt, aus urheberrechtlichen Werken zu zitieren, damit eine geistige Auseinandersetzung mit diesen möglich ist. Wenn das Urheberrecht als

„Zensurrecht“ eingesetzt wird, versagen die Schranken in der Regel, da die urheberrechtlichen Regelungen, die etwa Zitate oder die Berichterstattung über Tagesereignisse erlauben, sehr eng gefasst sind. Die Betroffenen machen sich das zunutze: Ihr urheberrechtlicher Unterlassungsanspruch zur Verfolgung urheberrechtsfremder Ziele geht durch, ohne dass die Gerichte mit dem Urheberrecht kollidierende Kommunikationsgrundrechte berücksichtigen würden.

In welchen Fällen wurde das Urheberrecht als Zensurrecht missbraucht?

Die Fälle zum Zensurheberrecht lassen sich in zwei Kategorien einteilen. Paradefall der ersten Variante ist die Rechtssache „Reformistischer Aufbruch“: Der Politiker Volker Beck wollte die Veröffentlichung eines seiner Manuskripte durch den *Spiegel* einige Tage vor der Bundestagswahl 2013 unterdrücken – was ihm im entscheidenden Zeitpunkt vor der Wahl dank des Urheberrechts auch gelang. Der Politiker hatte sich in einem Sammelband im Jahr 1988 für eine teilweise Entkriminalisierung gewaltfreier sexueller Handlungen zwischen Erwachsenen und Minderjährigen ausgesprochen. Der Herausgeber des Sammelbandes änderte wenige Worte. Als Volker Beck sich von dem Text dann distanzieren wollte, behauptete er, der Herausgeber hätte seinerzeit inhaltliche Änderungen vorgenommen. Die Berichterstattung des *Spiegels* deckte dann auf, dass der Inhalt vom Herausgeber gar nicht geändert worden war, und belegte damit, dass sich der Politiker wahrheitswidrig zu seinem Manuskript eingelassen hatte. Hieran hätte zweifelsohne ein hohes öffentliches Informationsinteresse bestanden – zumal wenige Tage vor der Bundestagswahl. In dieser ersten Variante macht also eine Privatperson einen urheberrechtlichen Unterlassungsanspruch geltend, weil ihr Berichterstattung über die eigene Person unlieb ist und sie diese aus der Welt schaffen möchte.

Zur zweiten Variante: Paradefall ist für sie die Rechtssache „Afghanistan-Papiere“: Die *Westdeutsche Allgemeinen Zeitung* (WAZ)

veröffentlichte 2012 militärische Lageberichte zum Auslandseinsatz der Bundeswehr in Afghanistan. Das Verteidigungsministerium klagte daraufhin wegen der Verletzung seiner Verwertungsrechte. Dabei hätte das Verteidigungsministerium die militärischen Lageberichte offenkundig nicht kommerziell verwertet. Der Staat konnte sein Urheberrecht hier derart einsetzen, weil ein*e Beamt*in die Texte geschrieben hatte, da in einem solchen Fall das Urheberrecht beim Staat als Dienstherren liegt. Dieser kann als Inhaber der ausschließlichen Nutzungsrechte einen urheberrechtlichen Unterlassungsanspruch geltend machen. Eine Berufung auf das Urheberrecht ist in diesen Fällen möglich, weil der urheberrechtliche Schutz für Werke sehr weit verstanden wird. Auch belanglose Texte oder standardisierte Textbausteine, wie sie in Behörden verwendet werden, können deshalb urheberrechtlichen Schutz genießen.

Aufsehen erregte auch der Fall des Glyphosat-Gutachtens: Das Bundesamt für Risikobewertung wollte Dokumente mit Verweis auf das Urheberrecht unterdrücken, die es nach dem Informationsfreiheitsgesetz hätte transparent machen müssen. Öffentliche Stellen haben in der Vergangenheit also wiederholt versucht, mittels des Urheberrechts staatlichen Informationsschutz zu betreiben. In der zweiten Variante nutzt also der Staat das Urheberrecht, um Inhalte unter Verschluss zu halten.

In all den vorgenannten Fällen sind die Anspruchsteller zunächst erfolgreich gewesen: Im entscheidenden Zeitpunkt, als ein öffentliches Informationsinteresse an den Presseberichterstattungen bestand, konnten diese unterbunden werden.

Welche Folgen hat das Aufkommen von künstlicher Intelligenz und warum ist zu erwarten, dass der Einsatz des Urheberrechts als Zensurrecht dadurch wieder zunehmen wird?

Generative KI-Modelle können neue Inhalte wie Texte, Bilder, Musik oder Videos erzeugen. Hierfür werden sie mit schon vorhandenem, digitalisiertem Bild- und Textmaterial gefüttert. Diese Bilder und Videos, aber auch viele der Texte, sind urheberrechtlich geschützt. Sie genießen entweder als Werke oder über verwandte Schutzrechte Urheberrechtsschutz. Das heißt, KI-Modelle lernen überwiegend mit urheberrechtlich geschützten Inhalten, wie sie neue Bilder und Videos generieren. Während des Trainings der KI-Modelle werden die Bilder und Videos nur vorübergehend gespeichert; technisch betrachtet wird aber eine Kopie von ihnen angelegt. Das genügt bereits für einen Eingriff in das Urheberrecht, denn es findet eine Vervielfältigung der Schutzinhalte statt, die nur mit Erlaubnis des Rechtsinhabers zulässig ist. Wenn die KI einen Output generiert, in dem ein urheberrechtlicher Schutzgegenstand wiedererkennbar ist, liegt auch hierin ein Eingriff in das Urheberrecht. Es gibt dazu zwar Schranken, die greifen können, doch diese sind eng gefasst. Aus diesem Grund konnte die Bundesregierung etwa gegen ein KI-generiertes Video von Bundeskanzler Olaf Scholz vorgehen. In dem auf Youtube eingestellten Video der aktivistischen Künstler*innengruppe „Zentrum für Politische Schönheit“ verkündete der vermeintliche Bundeskanzler, die Bundesregierung wolle ein Verbot der AfD beantragen. Die KI war zur Generierung des Videos offensichtlich mit einer Ukraine-Rede des Bundeskanzlers trainiert worden, denn Ausschnitte daraus fanden sich im KI-generierten Video wieder. Rechtlich gesehen hätte

der Bundeskanzler schlechte Karten gehabt, wäre er wegen Persönlichkeitsrechtsverletzung gegen das Video vorgegangen. Denn das KI-generierte Video war wohl als Satire einzuordnen, die in den Schutzbereich der Kunstfreiheit fällt. Die Bundesregierung ging stattdessen den sicheren Weg: Sie berief sich auf ihr Urheberrecht, um die Veröffentlichung zu unterbinden. Um eine Durchsetzung ihrer Verwertungsrechte an der Rede ging es ihr dabei sicherlich nicht.

Der Fall zeigt: Weil KI mit urheberrechtlich geschütztem Material lernt, das im Output häufig wiedererkennbar sein wird, ist zu erwarten, dass das Urheberrecht mit dem Erstarken von KI wieder mehr als Zensurrecht in Stellung gebracht wird.

Dr. Viktoria Kraetzig studierte Rechtswissenschaften an der Humboldt-Universität zu Berlin und absolvierte ihr Referendariat am Kammergericht. Während der anschließenden Promotion zum „Urheberrecht als Zensurrecht“ an der Goethe-Universität war sie zunächst als Justiziarin der Frankfurter Allgemeine Zeitung tätig, später als Rechtsanwältin in Berlin. Seit 2022 ist sie Habilitandin an der Goethe-Universität. Sie schreibt regelmäßig als freie Journalistin für die Frankfurter Allgemeine Zeitung.

Idee Lilli Iliev, Francesca Schmidt
Konzept und Projektmanagement
Valentina Djordjević, Lilli Iliev
Redaktion Valentina Djordjević, Sophia Tawonga Longwe
Inhaltlich verantwortlich
Lilli Iliev
Design und grafische Umsetzung
MOR Design (Rasmus Giesel, Carlotta Krämer, Moritz Voss)
Druck Druckhaus Sportflieger GmbH
ISBN 978-3-00-084023-4

Wikimedia Deutschland – Gesellschaft zur Förderung Freien Wissens e. V.

Adresse Tempelhofer Ufer 23-24, 10963 Berlin
Telefon 030 219 158 26-0
Fax 030 219 158 26-9
E-Mail info@wikimedia.de
Webadresse www.wikimedia.de
Blog blog.wikimedia.de
Mastodon social.wikimedia.de/@wikimediaDE

Diese Publikation wird gefördert durch das Bundesprogramm „Demokratie leben!“ des Bundesministeriums für Bildung, Familie, Senioren, Frauen und Jugend (BMBFSFJ).

Gefördert vom

Bundesministerium für Familie, Senioren, Frauen und Jugend

im Rahmen des Bundesprogramms

Demokratie leben!