2.1.1 Freiheit

Grundrechte im digitalen Zeitalter und wie sie garantiert werden können

Ellen Ueberschär[1]

Zwischen Alarmismus und Ambivalenz

Als die Bundeskanzlerin Angela Merkel vor einigen Jahren bemerkte, dass das Internet für uns alle »Neuland« sei, prasselten höhnische Kommentare auf sie nieder. Eine ganze Reihe von Menschen fühlte sich offenbar schon recht sicher in der neuen digitalen Wirklichkeit. Bis heute lässt sich wohl nicht behaupten, dass das Internet und die Digitalisierung aller Lebensbereiche auch nur annähernd so in das menschliche Leben integriert wäre, dass die Mehrheit das Gefühl hat, hier souverän und selbstbestimmt zu agieren.

Spätestens seit Shoshana Zuboffs Standardwerk über *Das Zeitalter des Überwachungskapitalismus*[2], in dem sie die digitalisierten Verzerrungen der wirtschaftlichen, öffentlichen und menschlichen Beziehungen nachzeichnet, verstärkt sich die Wahrnehmung der Freiheitsgefährdungen durch die digitalkapitalistische Überformung. Shoshana Zuboff sieht die Grundlagen des Zusammenlebens, der Individualität und der Sozialität durch die internetbasierten Plattformökonomien bedroht. Soziales Vertrauen und Demokratie werden ausgehöhlt und machen einer freiwilligen Unterjochung der Mehrheit Platz. Inzwischen reiht sich Zuboffs generationenprägende Theorie in eine ganze Bibliothek kritischer Literatur ein.

Den mahnenden und bisweilen apokalyptisch anmutenden Prognosen zum Trotz zeigt die Mehrheit der digitalen Nutzer*innen ein Verhalten, das

1 Unter Mitarbeit von Nina Locher und Vérane Meyer.

2 Zuboff Shoshana: Das Zeitalter des Überwachungskapitalismus, Frankfurt/New York: Campus Verlag 2018, S. 22.

bestenfalls von Ambiguität geprägt ist, wenn nicht gar von Ignoranz gegenüber diesen Warnungen. Selbst hinreichend sensibilisierte Zeitgenoss*innen machen sich zwar Sorgen, nutzen aber Messengerdienste, Vermittlungsplattformen oder Apps, deren Datengebaren sie nicht gutheißen, und hinterlassen freiwillig und großzügig Datenspuren im Netz – frei nach dem »Nichts-zu-verbergen-Argument«. Im Zeitalter von Homeoffice und Videokonferenzen sind die Anbieter mit dem geringsten Datenschutzniveau diejenigen, bei denen die Technik reibungslos und nutzerfreundlich funktioniert.

Überwiegt nicht der Nutzen (Komfort) den Schaden (Rechtsbruch und Rechtsunsicherheit)? Ist es vielleicht übertrieben, vor Freiheitsberaubung zu warnen? Die Datenschutz-Grundverordnung (DSGVO), von der noch die Rede sein wird, ist bei vielen Nutzer*innen unbeliebt und in ihrem Inhalt, ihrem Ziel und ihrer Funktionsweise unbekannt. Was soll der nervige »Einverstanden«-Klick, wenn es um Cookies und Ad-Tracker geht? Für die Nutzer*innen der Angebote überwiegen die Vorteile – die gesuchte Information ist nur einen Klick weit entfernt, der gesuchte Weg ist rasch gefunden, Meinungen sind mit Freunden schnell ausgetauscht und in Corona-Zeiten ist der digitale Einkauf sogar sicherer.

Oder liegt die Ursache für das ambivalente Verhalten nicht im Abwägen von Vor- und Nachteilen, sondern ganz woanders? Fehlt uns das angemessene Sensorium, fehlen uns das Wissen und die digitale Kompetenz für diese neue Form der Bedrohung? Fehlt uns die Klugheit des Hänsels aus dem Märchen, der – im Wissen um den Ofen, in dem er verschwinden soll – der Hexe immer nur ein dünnes Stöckchen, niemals aber sein dickes Fingerchen hinstreckt? Lassen wir uns von den glänzenden Pfefferkuchen behexen, geben gutherzig unser Leben preis und bemerken den Ofen nicht?

Warum steht dem Alarmismus der wenigen die Ambiguität der vielen gegenüber? Warum ist das Bewusstsein für eine schleichende *Ent-Wertung* und Rechtlosigkeit noch wenig ausgeprägt?

Dieser Beitrag gibt Antworten. Es geht in der Digitalisierung nicht um die reparierfähige Verletzung einzelner Grundrechte, sondern um eine irreparable Beschädigung der menschlichen Würde. Es ist aber keineswegs zwangsläufig, dass die Verletzung der Würde unaufhaltsam voranschreitet. Am Ende gibt es Vorschläge für den produktiven Umgang mit der Digitalisierung.

Wenn wir das Bewusstsein für die Freiheitsgefährdungen schärfen wollen, müssen wir zunächst verstehen, was eigentlich geschieht, wer wann und wie die Würde verletzt. Zugleich brauchen wir Wissen und Klarheit über un-

sere europäische Grundrechtstradition, die zu Themen wie Überwachung, Zwang und Totalitarismus einiges zu sagen hat.

Digitale Möglichkeiten für alle

Zunächst aber soll einem möglichen Missverständnis vorgebeugt werden:

Wenn es um die Gefährdungen im digitalen Raum geht, dann sprechen wir nicht von einer Schmälerung der Chancen und Möglichkeiten für Vernetzung und Austausch. Die Wahrung der Freiheitsrechte muss nicht konzeptionell gegen fast grenzenlose Informationsmöglichkeiten, Wissenserwerb und Lebenserleichterungen, die das Netz und die digitalen Tools für viele darstellen, ausgespielt werden. Der gern propagierte Gegensatz ist keiner, wie wir noch sehen werden. Das, was ein Smartphone heute an Bedienungshilfen bietet, kostete früher mehrere Tausend Euro und musste beispielsweise für Menschen mit Einschränkungen extra angefertigt werden. Digitale Endgeräte sind ein riesiger Gewinn an Freiheit und Inklusion für alle, die auf Assistenzsysteme angewiesen sind. Die Oppositionsbewegung in Belarus wäre ohne das Internet nicht so flächendeckend aktiv, nicht so gut organisiert und vernetzt. Migrant*innen, die über das Meer flüchten, verständigen sich über das Internet, halten Kontakt untereinander und mit ihren Bezugspersonen.

Die Liste positiver Anwendungsmöglichkeiten von digitalen Technologien ließe sich unendlich verlängern, angefangen bei algorithmengestützten Diagnoseverfahren in der Medizin über ressourcenschonende vernetzte Fertigung im Anlagenbau bis zur Präzisionslandwirtschaft. Auch hier ist rechtlich nicht alles geklärt, für vieles müssen Rechtskonzepte neu interpretiert und erweitert werden. Aber solange der Wettbewerb funktioniert, die Kreativität gesteigert und der Beitrag zu einem guten Leben deutlich wird, lässt sich mit den Unsicherheiten einer technologischen Umwälzung umgehen. Wenn wir über die Freiheitsgefährdungen im digitalen Raum reden, dann müssen wir die freiheitliche, lebensförderliche Seite der Digitalisierung ins Zentrum stellen und wirksam vor Gefahren schützen.

Freiheitsgefährdungen, die digitale Möglichkeiten in ihr Gegenteil verkehren

Freiheitsgefährdungen gehen in hohem Maße aus von den Mono- und Oligopolen der unter dem Akronym GAFAM (Google, Amazon, Facebook, Apple, Microsoft) bekannten Unternehmen, die in kürzester Zeit alles Realwirtschaftliche an Börsenwert überflügelt haben. Sie sind dabei, mit ihren Geschäftsmodellen den Marktplatz, den öffentlichen Raum, die digitale Infrastruktur zu nutzen. Sie selbst stellen den digitalen öffentlichen Raum! Und können sich so beinahe des gesamten Lebens der Bürger*innen bemächtigen.

In ihrem Opus magnum über den »Überwachungskapitalismus« hat Shoshana Zuboff die Geschäftspraktiken der digitalen Industriegiganten im Rahmen ihrer Kapitalismusanalyse auseinandergenommen. Die neue Wirtschaftsform »beansprucht einseitig menschliche Erfahrung als Rohstoff zur Umwandlung in Verhaltensdaten. Ein Teil dieser Daten dient der Verbesserung von Produkten und Diensten, den Rest erklärt man zu proprietärem Verhaltensüberschuss, aus dem man mithilfe [… von] Maschinen- oder künstlicher Intelligenz […] Vorhersageprodukte fertigt. […] Und schließlich werden diese Vorhersageprodukte auf einer neuen Art von Marktplatz für Verhaltensvorhersagen gehandelt, […] dem ›Verhaltensterminkontraktmarkt‹.«[3]

Dabei aber bleibt es nicht. Menschliches Verhalten wird von den großen Plattformen nicht nur abgeschöpft, sondern angestoßen und herausgekitzelt, mit anderen Worten: manipuliert. Je mehr Daten über einzelne Individuen bekannt sind und zusammengeführt werden, umso genauer sind die Vorhersagen, umso besser lassen sie sich an andere Unternehmen verkaufen, umso mehr Geld lässt sich mit ihnen verdienen. Vorhersageprodukte sind wertvoll für Versicherungen, Dienstleistungen – und am Ende auch für den Staat, zum Beispiel die Polizei.

Während der ehrbare Kaufmann noch Ware gegen Geld tauschte, funktioniert diese Art von Geschäft über die Köpfe derer hinweg, die die Ressourcen bereitstellen. Sie sind lediglich so eine Art »Minen«, aus denen der Rohstoff gewonnen wird, später veredelt zu Vorhersageprodukten und verkauft an interessierte Unternehmen. Die Nutzer*innen der Dienste von Google, Microsoft, Amazon und Co. sind nicht einmal die Kund*innen, sie sind nur die Rohdatenlieferant*innen, und das mit jedem einzelnen Klick. Auf diese Weise werden Subjekte zu Objekten.

3 Ebd.

Zuboff sieht in diesen Geschäftsmodellen, die die weitgehende Rechtsfreiheit im Internet erst ausnutzten und später zum Programm erklärten, schon heute eine »aus dem Ruder gelaufene, von neuartigen ökonomischen Imperativen getriebene Kraft, […] die nicht nur alle sozialen Normen ignoriert, sondern auch die Naturrechte aufhebt, die wir mit der Souveränität des Einzelnen verbinden und auf denen jede Möglichkeit von Demokratie an sich baut«.[4]

Fassen wir zusammen: Das Geschäftsmodell des Überwachungskapitalismus besteht darin, das Recht auf Selbstbestimmung der Individuen auszuhöhlen, sich selbst aber uneingeschränkte (Verfügungs-)Rechte anzumaßen. Und dort, wo der Staat an dieser Art von Vorhersageprodukten partizipieren kann, fällt es ihm schwer, regulierend einzugreifen. Das führt unmittelbar in den zweiten Bereich der Freiheitsgefährdung:

Diese Gefährdung erwächst aus der klassischen Situation, in der Technikkritik schon immer stand: die Entscheidung zwischen Sicherheit und Freiheit. Das große Sicherheitsbedürfnis des Staates nimmt mit der Digitalisierung neue Fahrt auf und tendiert dazu, die garantierten Grundrechte mithilfe von weitgehenden rechtlichen und technischen Geheimdienstbefugnissen zu unterlaufen – Stichwort Snowden-Enthüllungen – oder mit Technologien zu arbeiten, die potenziell diskriminierend und insofern grundrechtseinschränkend sind. Hier, wohlgemerkt, geht es um freiheitliche Demokratien mit robustem Rechtsstaat. Autoritär-populistisch geführte Demokratien, die sich selbst gern als illiberal bezeichnen, die freie Medien und Rechtsstaatlichkeit abbauen, arbeiten oft wenig verdeckt an der Aushöhlung von Bürger*innenrechten. Autoritäre Regime und Diktaturen wie China wiederum nutzen die Überwachungsdaten zur Zementierung ihrer Machtbasis.

Was folgt daraus? Die Bürger*innen sind gefragt. Wir brauchen Wissen und Klarheit über unsere Grundrechte und über die Geltung universeller und unteilbarer Menschenwürde. Wenn Menschen zu Objekten gemacht werden, steht das in klarem Widerspruch zum deutschen Grundgesetz im Besonderen und zum europäischen Menschenwürdeverständnis im Allgemeinen. Beides ist in Reaktion auf beispiellose Würdeverletzungen entstanden. Schauen wir genauer hin:

4 aaO., S. 26.

Menschenwürde und Freiheitsrechte

Die »Unantastbarkeit der Menschenwürde« bekam im Grundgesetz der Bundesrepublik eine starke Verankerung. Der nicht zu begrenzender Schutzraum menschlicher Würde war eine Antwort auf die Verbrechen des Nationalsozialismus und die Entrechtung und Würdeberaubung von Menschen in der faschistischen Diktatur.

Die ebenfalls aus der Erkenntnis des »Nie wieder!« heraus entstandene Allgemeine Erklärung der Menschenrechte formuliert in Artikel 1: »Alle Menschen sind frei und gleich an Würde und Rechten geboren. Sie sind mit Vernunft und Gewissen begabt […]«.

Anders noch die europäische Menschenrechtskonvention, die in ihrer ursprünglichen Fassung von 1950 Menschenwürde nicht explizit erwähnte. Erst die Rechtsentwicklung – insbesondere im Bereich der Bioethik – ließ der Menschenwürde in der EU eine neue Aufmerksamkeit zukommen, sodass sie – ähnlich wie im Grundgesetz – eine herausgehobene Stellung in der Präambel der Charta der Grundrechte der Europäischen Union von 2009 einnimmt: »In dem Bewusstsein ihres geistig-religiösen und sittlichen Erbes gründet sich die Union auf die unteilbaren und universellen Werte der Würde des Menschen, der Freiheit, der Gleichheit und der Solidarität.«[5]

In der Klarheit und Deutlichkeit, mit der in Europa die Menschenwürde als *norma normans* (normierende Norm), als Maßstab der Auslegung aller weiteren Grund- und Freiheitsrechte zentral gestellt wurde, spiegelt sich die Lernerfahrung aus den totalitären Diktaturen des 20. Jahrhunderts wider. Der *Totalitarismus*, der jede Selbstbestimmung, jede Individualität und millionenfach Leben vernichtete, erscheint in vielen Analysen über die problematischen Entwicklungen der Internetökonomie als Gefahr am Horizont.

Umfassende Kontrolle, Überwachung aller Lebensvorgänge, Manipulation und letztlich die Auflösung des Individuums in einem absolut gemeinschaftlichen Ganzen – die Herrschaftspraktiken des Totalitarismus scheinen ihre Wiedergänger in den Führungsetagen von Digitalkonzernen zu finden, mahnen viele kritische Stimmen. Argumente aus Hannah Arendts Analyse der *Elemente und Ursprünge totalitärer Herrschaft*, Grundgedanken aus George Orwells *1984*, die Dystopie einer totalen Überwachungsgesellschaft durch »Big Brother«, und Theodor W. Adornos *Erziehung nach Auschwitz* verfügen mit dem

5 https://www.europarl.europa.eu/germany/de/europäisches-parlament/grundrechtecharta

Blick auf manches Gebaren der Internetkonzerne über erstaunliche Passgenauigkeit zur heutigen Situation. Adornos Worte können als ein Hinweis auf die Potenziale des Totalitarismus gelesen werden, ohne die Entwicklung heute mit dem Entstehen des Faschismus gleichzusetzen. Adorno schreibt, »dass der Faschismus und das Entsetzen, das er bereitete, damit zusammenhängen, dass die alten, etablierten Autoritäten […] zerfallen, gestürzt waren, nicht aber die Menschen psychologisch schon bereit, sich selbst zu bestimmen. Sie zeigten der Freiheit, die ihnen in den Schoß fiel, nicht sich gewachsen.«[6] Sich der Freiheit gewachsen zu zeigen, ist eine Lektion, die Europäer*innen nach der Befreiung vom Faschismus gelernt haben und weiter lernen müssen.

Menschenwürde und Freiheit sind nicht an sich vorrätig, sondern müssen geschützt, verteidigt und gepflegt werden. Zusätzlich bedarf es der Anstrengung jedes einzelnen Individuums, ein Bewusstsein für die Freiheit, ein Gespür für ihre Verletzung zu entwickeln. Bisweilen scheint es, als hätte Adorno hier nachträglich und mit Blick auf die Enteignung des menschlichen Verhaltens Recht behalten: Es besteht die Gefahr, dass Menschen sich der Freiheit nicht gewachsen zeigen, sondern sie verspielen.

Der Schutzraum der Menschenwürde ist nicht begrenzt. Aber es gibt ein Kriterium, das feststellt, wann sie verletzt ist: die sogenannte Objekt-Formel: »Die Menschenwürde ist getroffen, wenn der konkrete Mensch zum Objekt, zu einem bloßen Mittel, zur vertretbaren Größe herabgewürdigt wird.«[7] Genau das geschieht im Geschäftsmodell der großen Internetplattformen. Die Methode des Data-Mining, die Gewinnung von Verhaltensdaten ohne echte Transparenz und Nachvollziehbarkeit, ohne Information an diejenigen, deren Daten aus der »Mine« extrahiert werden, ist eindeutig eine Verletzung menschlicher Würde, dessen also, was die Basis der Menschen- und Bürger*innenrechte ausmacht.

Das Primat des Rechtes durchsetzen

Das Menschenbild des Silicon Valley, das die heutige Digitalisierung prägt, steht dem Menschenwürdekonzept diametral entgegen. Was in der Frühzeit

6 Adorno, Theodor W.: »Erziehung nach Auschwitz«, in: Kulturkritik und Gesellschaft, Teil 2 (Gesammelte Schiften, Bd. 10.2), Frankfurt: Suhrkamp 2003, 677f.

7 Dürig, Günter: »Der Grundrechtssatz von der Menschenwürde«, in: Archiv des öffentlichen Rechts, 81 (1956), Tübingen: Mohr Siebeck, S. 117-157, hier S. 127.

des Internets vielversprechend schien, die Freiheit und Gleichheit aller, die sich im Netz bewegen, erweist sich, wie alle Freiheit, die nicht durch die Freiheit des Anderen begrenzt wird und keinen Ausgleich für Benachteiligung schafft, lediglich als die ultralibertäre Freiheit einer kleinen, auserwählten Gruppe. Für alle anderen ist sie außer Kraft gesetzt.

Einige Manager der großen Tech-Unternehmen fühlen sich in der Rolle der Herrscher, die besser wissen, was für alle Menschen gut ist als diese selbst. Stichworte sind hier Solutionism und Singularität. Eine Gruppe von »Weisen« verfügt über eine gefügige Masse, eigene Entscheidungen einzelner Individuen werden ausgehebelt; sehr schön beschrieben in Dave Eggers Roman *The Circle* unter Verwendung vieler, aus totalitären Systemen bekannten Sujets. Auch in der Realität: Die Konzernzentralen von Google und Facebook gleichen undurchdringlichen Festungen. Totale Transparenz und Aufgabe von Privatsphäre, von den Nutzer*innen gefordert, gilt für das eigene Geschäftsgebaren gerade nicht. Rechtsstaatlichkeit und Marktwirtschaft werden als veraltet betrachtet, den Nutzer*innen der immer umfassenderen Dienste wird weisgemacht, ihre Daten und damit ihr Verhalten seien gut aufgehoben – in undurchdringlichen Rechenzentren. Die digitalen Dienste versprechen Sicherheit und Rundum-Betreuung, Bequemlichkeit und Entlastung von der Qual der Wahl. Menschenwürde und Grundrechte sind in dieser Welt keine Kategorien. Oder sogar andersherum: Erst die digitalen Dienste würden Freiheit ermöglichen.

Auch in staatlichen Institutionen kommen – wie wir spätestens seit Edward Snowden wissen – hoch problematische Praktiken zur Anwendung. Gleichzeitig aber gibt es Gegengewichte, es gibt Parlamente und Menschen im administrativen Bereich, die gegensteuern, Alarm schlagen, problematische Entwicklungen ans Licht bringen und Korrekturen einfordern – auf rechtsstaatlichem Wege.

Die Bindung des liberalen Verfassungsstaates an das Grundgesetz und seine korrigierende Wirkung zeigen sich in richtungsweisenden Gerichtsurteilen. Exemplarisch zu nennen sind Urteile des Karlsruher Verfassungsgerichtes, etwa das »BND-Urteil«[8] zur Geltung der Grundrechte auch im Ausland, das Urteil zur »Antiterrordatei«[9], das mit Verweis auf die Grundrechte

8 https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2020/bvg20-037.html

9 https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2020/bvg20-104.html vom 11.12.2020; https://netzpolitik.org/2020/urteil-des-bundesverfass

eben jenes Data-Mining – die Verknüpfung von Daten aus unterschiedlichen Quellen – für teilweise verfassungswidrig erklärt, und das Urteil zur »Vorratsdatenspeicherung«[10], die in ihrer bisherigen Form ebenfalls mehrfach als verfassungswidrig bezeichnet wurde.

Diese Urteile des Bundesverfassungsgerichtes, aber auch weitere des Europäischen Gerichtshofes für Menschenrechte, belegen den kategorialen Unterschied, der zwischen problematischen Praktiken staatlicher Behörden in Rechtsstaaten und solchen in globalen, privatwirtschaftlichen Bereichen besteht. Eine derartige Praxisprüfung entlang demokratischer Normen steckt für die Konzerne, die Markt und Staat unterminieren, noch in den Kinderschuhen. Dennoch: Das Primat des Rechtes verschafft sich zunehmend Geltung in zahlreichen Regulierungsvorschlägen auf europäischer Ebene. Zudem besteht jetzt die Chance, diese auch transatlantisch abzustimmen. Und nicht zuletzt weist der regulatorische Prozess auch einige Ergebnisse auf, beispielsweise das Netzwerkdurchsetzungsgesetz und das Gesetz gegen Wettbewerbsbeschränkungen.

Digitales Rechtsbewusstsein entwickeln

Freiheit und Grundrechte, die sie schützen, sind fest verankert in einem grundlegenden Würde-Verständnis. Die Verletzung eines einzelnen Grundrechtes durch digitale Praktiken hat grundsätzlich die Tendenz zur Würdeverletzung. Nie geht es nur um den Bruch eines einzelnen Rechtes, zum Beispiel die Unverletzlichkeit des Eigentums oder den Schutz der räumlichen Privatsphäre, nie nur um die Beschädigung einzelner aktiver Rechte wie Versammlungs- und Meinungsfreiheit. Immer besteht eine enge Verknüpfung mit menschlicher Würde. Stets geht es um die Kombination von Freiheitseinschränkung und Würdeverletzung.

Das erklärt die starke Beunruhigung all jener, die sensibel für Grundrechtsverletzungen sind, wie Nichtregierungsorganisationen, die Gesellschaft für Freiheitsrechte, aber auch Parlamentarier*innen im Bundestag oder im Europäischen Parlament.

---

ungsgerichts-datamining-in-antiterrordatei-fuer-strafverfolgung-war-verfassungswidrig/

10 https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2020/bvg20-061.html;jsessionid=235A2A54704ABEE876859E3B9DEDB765.1_cid386

Solange aber nicht eine kritische Masse von Menschen die Verletzungen ihrer eigenen Würde wahrnimmt, ein Rechtsbewusstsein entwickelt, Klagen anstrengt und Druck erzeugt, wird das Geschäftsmodell der Rechte-Enteignung und der Würdeverletzung weiter funktionieren und perfektioniert werden.

Die Anstrengung, ein solches Bewusstsein für die eigenen Freiheitsrechte im digitalen Raum zu schaffen, ist vergleichbar mit der Herausbildung eines Umweltbewusstseins, das in den 1970er Jahren zu wachsen begann, getrieben von der Sorge um einen für kommende Generationen bewohnbaren Planeten. Zunächst lächerlich gemacht als fortschrittsfeindlich und technikskeptisch, hat sich das Umweltbewusstsein inzwischen bis in die Mitte der Gesellschaft verbreitet.

Ähnliches ist für das Rechtsbewusstsein im digitalen Raum nötig. Für die Einhegung der digitalen Praktiken und ihren Einsatz für das Gemeinwohl reicht es nicht, auf die positiven Rechte, die existierende Rechtsprechung, zu verweisen. Es braucht ein neues Rechtsbewusstsein aller demokratischen Akteur*innen und eine breite gesellschaftliche Debatte. Welches Menschenbild in einer Gesellschaft gelten und welche Werte es verkörpern soll – Würde, Freiheit, Solidarität – das bildet sich im öffentlichen Diskurs heraus. Würde, Freiheit und Solidarität spiegeln die emanzipatorischen und antitotalitären Lernerfahrungen der Vergangenheit. Für die digitale Zukunft werden Werte wie Privatheit, Selbstbestimmung, Sicherheit und Gerechtigkeit weichenstellend sein. Viel mehr Menschen müssen in diesen Diskurs involviert werden. Unter Expert*innen ist die Debatte in vollem Gange, aber sie braucht Belebung und Förderung und vor allem Verbreiterung.

Wir haben beschrieben, dass die Abschöpfung menschlichen Verhaltens und die intransparente Verknüpfung von Daten Menschen zu Objekten macht, also das grundlegende Menschenrecht auf Würde verletzt.

Wie genau sind Grundrechtseinschränkung und Würdeverletzung verbunden? Wir sehen uns drei Spannungsfelder konkret an, die unmittelbaren Grundrechtsbezug haben: das Recht auf informationelle Selbstbestimmung, den Gleichheitsgrundsatz und die Meinungsfreiheit.

Beispiel 1: Überwachung und Kontrolle versus informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung kam zunächst in den Grundrechtskatalogen nicht vor. Darf der Staat alle möglichen Daten sam-

meln, aufheben, verarbeiten und nutzen? Diese Frage ließen Bürger*innen 1983 durch das Bundesverfassungsgericht klären. Dieses antwortete mit der Anerkennung eines Rechtes, das Bürger*innen in der Tradition der Abwehrrechte gegen den Staat davor schützte, »nicht mehr wissen [zu] können, wer was wann und bei welcher Gelegenheit über sie weiß«.[11] Gemeint war hier die Volkszählung. Auch der heute sogenannte *chilling effect* fand schon Berücksichtigung, also die Einschränkung der Entscheidungsfreiheit durch Furcht vor Benachteiligung in der Zukunft.

Wie das Recht auf informationelle Selbstbestimmung aus dem Grundgesetz Artikel 2 in Verbindung mit Artikel 1 erwuchs, so basiert der europäische Datenschutz und die sehr tiefe Ausprägung der DSGVO auf dem in Artikel 8 der Europäischen Grundrechtecharta festgehaltenen Schutz personenbezogener Daten. Es gibt also ein rechtliches Fundament zur Wahrung dieser Freiheitsrechte in der digitalen Welt.

Das Persönlichkeitsrecht garantiert Privatheit und Entscheidungshoheit über die eigenen Daten. Zugleich aber ist die Digitalisierung, in der Regel mit Einwilligung der Nutzer*innen, tief in das Privatleben eingedrungen. Das zeigen Online-Dienste, die wir auf Deutsch Partnervermittlung nennen würden, wie Tinder oder OkCupid der Match Group. Intimste Informationen werden für perfekt zugeschnittene Werbung genutzt. Die Mathematikerin Cathy O'Neill beschreibt in ihrem Buch *Weapons of Math Destruction*[12] das Geschäftsinteresse dabei: Nutzer*innen sollen sich so lange wie möglich auf den Plattformen aufhalten und deren Apps nutzen, um möglichst viele Daten preiszugeben, mehr Einblicke in die persönlichen Gedanken und Vorlieben zu gewähren. Wie nebenher bestimmen algorithmische Entscheidungssysteme, welche Menschen den Nutzer*innen vorgestellt werden und welche nicht. Bei Nichtgefallen: einfach wegwischen. Eine algorithmisch eingebaute Verletzung von Menschenwürde.

Ging es vor 40 Jahren noch um die Erhebung einzelner Daten durch den Staat, haben wir es heute mit der Zusammenführung von Daten für die Privatwirtschaft zu tun. Auf diese Veredlung würden auch staatliche Stellen gerne zugreifen. Das Verbot, ein einzelnes Datum zu erheben, würde wenig nutzen, auch eine Verpflichtung zur Anonymisierung der Daten würde nicht den erwünschten Zweck erfüllen. Denn das wirtschaftliche Potenzial liegt

11 https://www.bfdi.bund.de/DE/Datenschutz/Ueberblick/Was_ist_Datenschutz/Artikel/InformationelleSelbstbestimmung.html

12 https://weaponsofmathdestructionbook.com/

in der Verknüpfung von öffentlich zugänglichen und privat bereitgestellten Daten, aus denen sich Muster erkennen lassen. Erst diese Muster, nicht das Datum an sich, lassen präzise Rückschlüsse auf Gruppen oder Einzelne zu. Der bekannte Fall der Cambridge-Analytica-Methode hat mit diesem Microtargeting-Prinzip großflächig funktioniert. Große Sammlungen demografischer Daten, Likes, Aktivitäten auf Facebook wurden ausgebeutet und das Verhalten von Nutzer*innen analysiert, um psychologische Profile zu erstellen und so persönlich zugeschnittene Wahlwerbung an spezifische Zielgruppen zu richten, ohne dass dies den Betroffenen bekannt oder bewusst gewesen wäre.[13] Microtargeting wurde unter anderem während der US-Präsidentschaftswahl 2016 für Donald Trumps Wahlkampf und beim Brexit-Referendum im selben Jahr von der »Vote Leave«-Kampagne genutzt.

Inzwischen laufen Forschungsprojekte, die allein aufgrund der Auswertung von Bilddaten aus Google Street View präzise das Wahlverhalten bis hinunter auf Wahlkreisebene vorhersagen.[14] Weder geht es um personenbezogene Daten, noch müssen die Betroffenen eingewilligt haben, dass dieses Forschungsprojekt stattfindet. Mannigfaltige Möglichkeiten des Gebrauchs, aber auch des Missbrauchs öffnen sich damit. Nun ließe sich mit einem Opt-out aus Google Street View argumentieren. Schließlich könne man die Aufnahme ablehnen. Aber auch das schützt nicht vor einem Scoring auf Basis individueller Parameter. Dieses Scoring kann eine gruppenspezifische Diskriminierung zur Folge haben, wenn es um höhere Versicherungstarife aufgrund des Wohnortes, um einen guten Job, um Wahlbeeinflussung und gezieltes Nudging für dieses oder jenes Verhalten geht. Das Recht auf informationelle Selbstbestimmung ist hier, trotz der Möglichkeit des Opt-out, weitgehend infrage gestellt.

Besonders sensibel sind Gesundheitsdaten. Der Markt ist attraktiv und die Verlockungen der fitnessorientierten Gesellschaft, hier Daten preiszugeben, sind immens: Fitness-Tracker, wie Fitnessarmbänder oder Smart Watches, bieten jede nur denkbare Gelegenheit, den Gesundheitszustand einer unbekannten Überwachung und Kontrolle zu übergeben. Trotz zahlreicher Warnungen von Datenschützer*innen und Menschenrechtler*innen genehmigte die EU-Kommission die Übernahme der Firma Fitbit, spezialisiert auf Wearables und Fitnesstracker, durch Google. Einmal mehr zeigt sich, dass das

13 Vgl. https://netzpolitik.org/2018/cambridge-analytica-was-wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen/

14 Vgl. https://www.nytimes.com/2017/12/31/technology/google-images-voters.html

Geschäftsmodell von Google durch das Raster der üblichen Kriterien zur Bewertung von Marktverzerrungen fällt. Es ging nicht allein um Markterschließung, es geht um die Potenziale der Überwachung und Steuerung von Millionen Menschen und um ihren Missbrauch als Datenminen für Geschäfte mit Dritten. Grundrechtsschutz ist trotz gestiegener Sensibilität auf EU-Ebene kein Prüfkriterium im Wettbewerbsrecht. Das heißt, hier kann ein Grundrecht nicht umgesetzt werden, weil die Potenzialität der Grundrechtsverletzung in einem scheinbar weit entfernten Regulierungsfeld noch nicht ausreichend bewertet werden kann.[15]

Beispiel 2: Diskriminierung versus Gleichheitsgrundsatz

Ein weiteres Grundrechtsversprechen der Demokratie ist die Gleichheit. Im Grundgesetz in Artikel 3 niedergelegt, geht es um Gleichheit vor dem Gesetz, um Geschlechtergerechtigkeit und um Gleichbehandlung aller Menschen. In der vielfältigen Gesellschaft muss gerade die Gleichbehandlung immer wieder und für jedes Merkmal der möglichen Diskriminierung oder gegen Privilegierung erkämpft werden, angefangen bei der Bildung bis hin zum Arbeitsmarkt oder der Wohnungssuche. Gleichheit bedeutet gleichberechtigte, angstfreie Teilhabe und Zugang zu öffentlichen Gütern, Räumen und Netzen.

Das Geschäftsmodell der algorithmenbasierten Auswahlprozesse impliziert aber nicht den Grundsatz der Gleichheit, sondern die Weltsicht der Coder und die Daten der Vergangenheit. Zudem werden algorithmenbasierten Entscheidungssysteme nach subjektiven Kriterien trainiert, die in der Regel intransparent sind. Das birgt erhebliche Potenziale für die Diskriminierung ganzer Bevölkerungsgruppen aufgrund individueller Merkmale, sei es bei Bewerbungsprozessen, der Vergabe von Schulplätzen,[16] der Beurteilung der Kreditwürdigkeit oder bei juristischen Entscheidungen (wie etwa im US-

15 Eine Möglichkeit, zu erwartende Marktmachtkonzentration einzuhegen, könnte mit der Ex-ante-Regulierung, die durch den Digital Market Act der EU-Kommission im Gespräch ist, eingeführt werden. Mit einer solchen Vorab-Regulierung soll verhindert werden, dass die Marktmacht in dem einen Segment dazu genutzt wird, sich in einem anderen Segment einen uneinholbaren Startvorteil zu verschaffen. Allerdings reicht auch das nicht bis zum Recht auf informationelle Selbstbestimmung.

16 Vgl. https://netzpolitik.org/2018/wenn-sie-ethisch-umgesetzt-werden-kosten-sie-mehr-danah-boyd-ueber-algorithmische-entscheidungssysteme/ Dazu auch: https://algorithmwatch.org/en/busted-internet-myth-algorithms-are-always-neutral/

Justizsystem).[17] Ein weiteres Beispiel sind Gesichtserkennungssysteme, die in einigen Ländern eingesetzt werden. Diese können die Gesichter von Schwarzen, Indigenen und anderen Menschen of Colour oder Frauen häufig nicht korrekt identifizieren, werden aber zum Teil im Strafvollzug, in der Strafverfolgung oder der Prävention verwendet.[18]

Viele Beispiele der Diskriminierung durch Entscheidungsalgorithmen stammen aus den USA. Für Deutschland hat die NGO AlgorithmWatch in einem *Atlas der Automatisierung* aufgezeigt, in welchen Bereichen auch hierzulande Entscheidungen automatisiert getroffen werden, vom Personalmanagement über die Verwaltung von Arbeitslosigkeit bis hin zur Spracherkennung von Asylsuchenden und Predictive Policing. AlgorithmWatch hat daraus Handlungsempfehlungen entwickelt, die vom Grundsatz »do no harm« über die Forderung nach Nachvollziehbarkeit der Entscheidungen und einer wirkungsvollen Aufsicht über privatwirtschaftliche und staatliche Anwendungen reichen.[19] Dieser Katalog ist ein wichtiger Beitrag zur Schärfung und Stärkung des Rechtsbewusstseins im digitalen Raum.

Beispiel 3: Hate Speech und digitale Gewalt versus Meinungsfreiheit und demokratische Öffentlichkeit

Ein drittes Feld der Grundrechtsverletzungen umfasst Hassrede und Gewalt im Netz, die dem Grundrecht auf Meinungsfreiheit in Artikel 5 des Grundgesetzes entgegenstehen. Hate Speech (Hassrede) ist nicht nur zu einem Problem individueller Bedrohung, sondern zu einer Gefährdung medialer Öffentlichkeit überhaupt geworden. Während der Bundestag 2013 noch keinerlei gesetzgeberischen Handlungsbedarf sah, gegen Hate Speech vorzugehen,[20] hat sich die Lage innerhalb weniger Jahre dramatisch verändert. Wo Hassrede zu kriminellen Handlungen anstachelt, gepaart mit Falschinformationen und verstärkt durch Shitstorms, Hetzjagden im Netz, ist rechtliche Eindämmung gefragt.

17 Vgl. https://www.nytimes.com/2017/06/13/opinion/how-computers-are-harming-criminal-justice.html

18 Vgl. https://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Hintergrundpapier-hp024.pdf

19 Vgl. https ://atlas.algorithmwatch.org

20 Dreizehnter Zwischenbericht der Enquete-Kommission »Internet und digitale Gesellschaft«, Bundestag Drucksache 17/12542, S. 82.

Die Algorithmen der Intermediären wie Facebook und Twitter vervielfältigen Hassrede und sorgen für die schnelle Verbreitung von Desinformationen. Die Verächtlichmachung von seriösen Medien und Wissenschaft, die Entstehung von undurchdringlichen Informationsblasen verfälschen den offenen Meinungsbildungsprozess, beschädigen die demokratische Öffentlichkeit und stacheln nachweislich auch zu physischer Gewalt an.[21] Während der Corona-Pandemie erscheint die von der WHO beklagte »Infodemie« – aus Desinformationen, Verschwörungstheorien und Wissenschaftsfeindlichkeit – lebensbedrohlich, weil wichtige Informationen zum Schutz der Gesundheit bestimmte Teile der Bevölkerung nicht mehr erreichen. Je nach Stärke der öffentlich-rechtlichen Medien sind das in unterschiedlichen Ländern verschieden große Gruppen von Menschen. In Sachen Hate Speech stehen auf der einen Seite Täter, die Meinungsfreiheit für sich reklamieren, auf der anderen Seite Opfer, die unter Einschüchterung und Mobbing leiden, deren Persönlichkeitsschutz nicht mehr gewahrt ist, was sie an der freien Entfaltung ihrer Persönlichkeit hindert.

Eine ganze Reihe wissenschaftlicher Studien belegt die gefährdenden Auswirkungen, darunter Selbstzensur und psychische Folgeschäden für die Betroffenen, Veränderung impliziter Haltungen und Meinungen der un- oder beteiligten Nutzer*innen.[22] Insbesondere Frauen sind überdurchschnittlich häufig Opfer von Hate Speech und digitaler Gewalt. Der Fall von Renate Künast, in dem unerhörte Beleidigungen gerichtlich teilweise gebilligt wurden, warf ein grelles Licht auf die Notwendigkeit, Meinungsfreiheit für Hassrede zugunsten des Persönlichkeitsschutzes einzuschränken und zugleich Meinungsfreiheit als Freiheit für Meinung zu schützen, denn: Hass ist keine Meinung.

Für die Gerichte gilt es, eine Rechtsprechung zu entwickeln, die dem Risiko angemessen ist, das durch die pure Reichweite der neuen Medien massiv

21 Vgl. https://hatebase.org/news/2019/11/18/does-online-hate-speech-cause-violence

22 z.B. Aslan, Alev: »Online hate discourse: A study on hatred speech directed against Syrian refugees on YouTube«, in: Journal of Media Critiques 3(12) (2017), S. 227-256; Geschke, D., Klaßen, A., Quent, M., & Richter, C.: »#Hass im Netz: Der schleichende Angriff auf unsere Demokratie: Eine bundesweite repräsentative Untersuchung« in: Forschungsbericht (2019); Weber, M., Koehler, C., Ziegele, M., & Schemer, C.: »Online Hate Does Not Stay Online–How Implicit and Explicit Attitudes Mediate the Effect of Civil Negativity and Hate in User Comments on Prosocial Behavior«, in: Computers in Human Behavior (2019), S. 106-192.

erhöht ist. Beleidigungen im öffentlichen Raum sind nicht zu vergleichen mit Beleidigungen im digitalen Raum, die in einem weltweiten Kommunikationsnetzwerk tausendfach vervielfältigt werden können. Die bestehenden Standards, nach denen Hassrede strafrechtlich nur im Falle einer expliziten Beleidigung und physischer, direkter Gewaltandrohung verfolgt werden kann, reichen für die im Netz begangenen Taten nicht aus.

Darüber hinaus besteht inzwischen Konsens über die Dringlichkeit einer Regulierung der Intermediären mit Blick auf die demokratische Öffentlichkeit und ihren Einfluss auf Meinungsbildungsprozesse in der Gesellschaft. Offen debattiert wird über einen Regulierungsrahmen, der vergleichbar ist mit einer Mediengesetzgebung. Ein solcher Rahmen hätte automatisch Rückwirkung auf die Grundrechte der Nutzer*innen.

Nach diesen Tiefenbohrungen an drei grundlegenden Freiheitsrechten, die einen gemischten Befund ergaben, drängt sich eine Frage auf, die häufig gestellt wird:

Brauchen wir neue Grundrechte für das digitale Zeitalter?

Reichen die bisherigen Freiheitsrechte denn überhaupt aus, um den Gefahren für die demokratische Öffentlichkeit, der Manipulation von Einstellungen und Verhalten, der Beeinflussung des Wahlverhaltens, der Lenkung der öffentlichen Meinung und der Lähmung freiheitlicher Entscheidung durch allgegenwärtige Überwachungstechnologien etwas entgegenzusetzen?

Die Stichproben bei den Grundrechten des Persönlichkeitsrechtes, des Rechtes auf informationelle Selbstbestimmung, dem Gleichheitsgrundsatz und der Meinungsfreiheit haben gezeigt: Es mangelt nicht an Freiheitsrechten, sondern an ihrer Durchsetzung. Versuche neuer Definitionen, wie die Charta der digitalen Grundrechte von 2016, bleiben hinter dem hohen Rechtsschutz zurück, den das Grundgesetz und die Europäische Grundrechtecharta bereits bieten.

Die einschneidenden Erfahrungen aus den Diktaturen des 20. Jahrhunderts haben die in der Menschenwürde gegründeten Grundrechte und ihre Rechtsdurchsetzung fest in Europa verankert. Sie sind keine Papiertiger, sondern rechtlich einklagbar und durchsetzungsfähig – genau das ist die Stärke der Rechtsstaatlichkeit, die Europa zu einem Kontinent mit hohen menschenrechtlichen und demokratischen Standards hat werden lassen.

Gleichwohl, Grundrechtsschutz fällt uns als Unionsbürger*innen nicht in den Schoß. Im Digitalen muss die Durchsetzung der Freiheitsrechte genauso erkämpft werden wie im Analogen. Worauf es jetzt ankommt, ist die Europäisierung ihrer Durchsetzung und in letzter Konsequenz die Globalisierung der Rechtsdurchsetzung. Da dies aber eher zu den visionären Zielen gehört, die rasch als Ausflucht für Nichtstun auf nationaler Ebene herhalten könnte, kommt es jetzt darauf an, Grundrechte auf eine Weise durchzusetzen, dass sie erstens auf international agierende, digitale Konzerne anwendbar sind und dass diese Durchsetzung europäisiert wird. In der Regel sind europäische Normen im nationalen Recht umgesetzt und der Rechtsweg steht in erster Linie im Inland offen. Das muss geöffnet werden: Wenn Google in Irland seinen Sitz hat, aber Hate Speech aus den USA sich gegen eine Person in Deutschland richtet, die sich gerichtlich dagegen wehren will dann müssen die Möglichkeiten der grenzüberschreitenden Rechtsdurchsetzung erweitert werden.[23]

Es ist beschämend und für den Rechtsstaat kein guter Zustand, wenn sich in den AGBs von Facebook & Co Paragrafen befinden, die schlicht rechtswidrig sind, das geltende Recht aber wegen der enormen Marktmacht und einem unverhältnismäßigen Aufwand, den eine Rechtsdurchsetzung von Deutschland aus nach sich ziehen würde, nicht durchgesetzt werden kann.

Das muss sich ändern. Bis dahin muss aber ein anderer Bereich geschärft werden, von dem wir bereits sprachen: das Rechtsbewusstsein für die Verletzungen der eigenen Grundrechte. Um der Freiheit willen muss eine Atmosphäre entstehen, in der das digitale Rechtsempfinden unter Nutzer*innen, Mitbewerber*innen und im öffentlichen Bewusstsein aktiviert wird. Dafür ist es wichtig, das offensichtliche Unrecht anhaltend und öffentlich sichtbar anzuprangern.

Die Anpassung des Rechtes an die globale Herausforderung ist auch eine Frage der Zeit. Ein erster Schritt war die Europäische Datenschutz-Grundverordnung, die 2018 in Kraft trat und gegen enorme Widerstände durchgesetzt werden musste. Nach ihrer Verabschiedung existiert nun aber eine Grundverordnung, die sich zum Ziel setzt, »die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten« zu schützen (Art. 1, Abs. 2 DSGVO). Dieser Schutz gilt sowohl für die Erhebung als auch für die Verarbeitung

23 Vgl. hierzu im Detail: https://irights.info/artikel/die-digitalcharta-und-was-wir-statt-dessen-brauchen/28273

der Daten. Einen zweiten Schritt geht die EU nun mit ihrem Gesetzespaket zum Digital Services Act und Digital Marktes Act, das einen europäischen Rechtsrahmen für digitale Dienste und Märkte schaffen will. Dieser soll Marktmachtmissbrauch und unfaire Praktiken von Anbietern in der EU nach dem Marktortprinzip wirksam einschränken, Datenzugang und Interoperabilität der Messengerdienste ermöglichen und mehr Transparenz für Empfehlungsalgorithmen und Online-Werbung schaffen.

Der digitale Kompass – Privatheit schützen, Selbstbestimmung und Sicherheit gewährleisten und Teilhabe ermöglichen

Die Werte, die einer Gesellschaft zugrunde liegen, sind in ihrem Rechtssystem verankert. Wenn Würde, Freiheit und Solidarität die emanzipatorischen und antitotalitären Lernerfahrungen spiegeln, dann rücken im digitalen Zeitalter die Werte Privatheit, Selbstbestimmung, Sicherheit und Teilhabe in den Fokus. Nur wenn diese Werte und die damit verbundenen Rechte garantiert und durchgesetzt werden, ist ein Umgang mit digitalen Technologien möglich, der souverän genannt werden kann. Das schließt ein individuelles Rechtsbewusstsein genauso ein wie äußere Rahmenbedingungen, die die Wahrnehmung individueller Rechte ermöglichen und erleichtern.

Privatheit schützen, Selbstbestimmung und Sicherheit gewährleisten und Teilhabe ermöglichen – so könnte die Zielvorstellung für das digitale Gemeinwohl lauten. Dabei geht es nicht um Soft Law in Form von Selbstverpflichtungen oder Vertrauen in die Rechtstreue der Anbieter. »Das Recht kennt keinen hybriden Zustand eines nicht verbindlichen Rechts.«[24] Es geht um individuelle Grundrechte und Rechtsdurchsetzung als Basis einer freien und offenen Gesellschaft. Die Herausforderung ist komplex, ihre Konkretionen sind unablässig im Fluss.

Privatheit zu schützen, heißt, die Grundrechte auf freie Meinungsäußerung (GG 5), auf Glaubens- und Gewissensfreiheit (GG 4), auf Versammlungsfreiheit (GG 8), auf Schutz der Familie (GG 6), auf die freie Berufswahl (GG 12) und das Eigentumsrecht (GG 14) zu garantieren und ihre einfachgesetzliche Umsetzung zu gewährleisten.

Selbstbestimmung und Sicherheit im Netz zu gewährleisten, bedeutet, persönlich Hoheit zu erlangen über die Erhebung und Verarbeitung von perso-

24 Grimm, Petra; Keber, Tobias; Zöllner, Oliver: Digitale Ethik. Leben in vernetzten Welten, Ditzingen: Reclam 2019, S. 24.

nenbezogenen, persönlichen Daten. Das setzt klare, faire und vertrauenswürdige Regelungen für Datenerhebung, Datenzugang und Datennutzung voraus. Zudem muss die Nachvollziehbarkeit von algorithmischen Entscheidungen gegeben sein. Das setzt wiederum die Integrität informationstechnischer Systeme voraus, Verschlüsselung spielt dabei die größte Rolle.[25]

Teilhabe zu ermöglichen, bedeutet, digitaler Gewalt und Diskriminierungen etwa durch fehlgeleitete Entscheidungsalgorithmen, vorzubeugen und möglichst im Vorhinein zu unterbinden. Zudem geht es um gleichberechtigten Zugang zu öffentlichen Gütern, Räumen und zum Netz.

Was jetzt zu tun ist: Infrastruktur, Bildung, Partizipation und Ordnungspolitik

Mit diesem digitalen Werte-Kompass ist ein Teil der Antwort auf die Ausgangsfrage gegeben: Wie lassen sich Grund- und Freiheitsrechte im digitalen Zeitalter umsetzen? Wir hatten gesehen: Grundrechte setzen sich nicht von allein durch. Das gesellschaftliche Bewusstsein für ihre Verletzung im digitalen Raum muss die nötige Kraft entwickeln. Um den digitalen Kompass auch tatsächlich auszurichten, sind verschiedene Ansätze nötig.

Digitalisierung ist auch eine Frage der Infrastruktur: Ja, der Zugang zum stabilen, sicheren und leistungsfähigen Netz ist ein wichtiger Schritt zur digitalen Teilhabe aller Bürger*innen – kein Luxus, sondern Teil der Daseinsvorsorge. Dass es dazu eines stabilen, schnellen Internetzuganges bedarf, ist eine Binsenweisheit, aber in Deutschland noch lange nicht Realität. Technische Voraussetzungen fehlen vielerorts, auch die rechtliche Verpflichtung der Anbieter, alle Flächen des Landes abzudecken. Die Netzneutralität hingegen ist durch ein Urteil des EuGH gestärkt worden.[26]

Gemeinwohl und digitale Infrastruktur gehören zusammen.

Ein weiteres, wichtiges und großes Thema ist *digitale Bildung*. Wenn wir das Internet als »Neuland« unter den Pflug nehmen wollen, dann braucht es starke Angebote der digitalpolitischen Bildungsarbeit. Der Satz »Ich habe nichts zu verbergen« gehört ins Museum. Niemand käme auf die Idee zu sagen: »Ich habe nichts Wertvolles in meiner Wohnung, also lasse ich die Haustür offen.« Mit Bildungsangeboten muss in Schulen, in Vereinen, durch poli-

25 Vgl. https://www.bundestag.de/dokumente/textarchiv/2020/kw05-pa-inneres-669564

26 Vgl. https ://netzpolitik.org/2020/eugh-zur-netzneutralitaet-provider-duerfen-angebote-nicht-selektiv-drosseln

tische Stiftungen und die Zivilgesellschaft ein neues Bewusstsein für die Abwehrrechte nicht nur gegenüber dem Staat, sondern auch gegenüber privaten Datensammlern und -verwertern entwickelt werden. Zu politischer Bildung gehört, Menschen das Handwerkzeug für die Nutzung des Internets in beide Richtungen zu geben: Zum einen muss das Wissen um die eigenen Rechte im digitalen Raum gestärkt werden, denn das Bewusstsein für Rechtsverletzungen und das Wissen um Gefahren schützen die Freiheitsrechte. Zum anderen aber umfasst politische Bildung auch das Know-how, das Internet zum eigenen Vorteil mehr und besser zu nutzen. Denn erst mit diesen Fähigkeiten wird aus digitaler Bildung ein Instrument zu digitaler Teilhabe. Diese schließt selbstverständlich viel mehr Aspekte ein, denn die Barrieren der Teilhabe verschärfen oder potenzieren sich in der digitalen Welt. Gut erforscht ist das im Blick auf die Fähigkeit von Schüler*innen, mit digitalen Anwendungen umzugehen.[27] In der Corona-Pandemie wirkt sich ein fehlender oder unzureichender Internetzugang sehr konkret auf die Bildungschancen von Kindern aus, wenn Möglichkeiten des digitalen Lernens schlicht aus Mangel an stabilem Zugang zum Internet nicht genutzt werden können. Das Grundrecht auf die freie Entfaltung der Persönlichkeit ist hier von vornherein verletzt.

Ein weiterer, wesentlicher Faktor ist die *Partizipation von Bürger*innen* an politischen Entscheidungen. Dazu gehört eine *breite öffentliche Debatte* über Sicherheit und Freiheit im Netz, über Persönlichkeitsschutz, Meinungsfreiheit und vieles andere mehr. Diese Debatten, so konfliktreich sie sein mögen, schärfen das Bewusstsein individueller Grundrechte in der digitalisierten Welt.

Nachweislich stärkt nachhaltige und sinnvolle politische Beteiligung die Demokratie.

Je transparenter und beteiligungsorientierter Politik und Verwaltung mit den von ihnen erhobenen Daten, mit politischen Antworten zur Wahrung der Grundrechte im Netz, mit dem Zugewinn an Kommunikation und Vernetzung, mit den vielfältigen Informationsmöglichkeiten umgehen, umso mehr stärken sie die Souveränität ihrer Bürger*innen.

Ordnungspolitisch – das hatten wir gesehen – stehen große Entscheidungen an. Diese müssen öffentlich debattiert werden. Eine wertegeleitete, digitale Ordnungspolitik stärkt auch die Robustheit des Rechtsstaates. Es ist höchste Zeit für eine ordnungspolitische Antwort, die die individuellen Rech-

27 Vgl. https ://www.boell.de/BildungDigitaleWelt

te zentral stellt und einen klaren Rahmen für die Regulierung der algorithmenbasierten Wirtschaft gibt.

Die Grundrechte werden sich nicht von allein und nicht durch freiwillige Selbstverpflichtungen der Konzerne durchsetzen. Deshalb braucht es die breite Unterstützung und das gemeinsame Engagement der (Zivil-)Gesellschaft, Politik, Wissenschaft und Wirtschaft, um Bürgerrechte auch im digitalen Zeitalter zu garantieren und zu schützen, um den digitalen Raum im Sinne des Gemeinwohls nutzbar zu machen.