Der Schutz der Grundrechte im Digitalen Zeitalter[1]

Anja Mihr und Sabrina Görisch

Grund- und Freiheitsrechte sind Menschenrechte, die im Grundgesetz sowie in dutzenden internationalen Verträgen der Vereinten Nationen und anderer regionaler Organisationen und so auch in der Grundrechtecharta der Europäischen Union von 2000 festgelegt und in die modernen Verfassungen übernommen worden sind.

Im Zeitalter eines scheinbar unkontrollierten Datenflusses ist eine große Debatte um den Schutz der Grund- und Freiheitsrechte im digitalen Raum entstanden.[2] Es sind nicht mehr allein staatliche Stellen, Regierungen und Gerichte, die trotz einer Bindung an Art. 1 Abs. 3 GG und der EU-Grundrechtecharta die Grundrechte beeinträchtigen könnten. Stattdessen lässt sich eine vermehrte Missachtung der Grundrechte seitens privater, global operierender Unternehmen beobachten (Papier 2018, 172f.). Während es in früheren Debatten vorwiegend um die massenhaft anwachsende staatliche Zensur im Internet und das Thema Cybersicherheit ging, kreisen aktuelle Diskussionen vor allem um Themen wie Hetze, Fake News und Künstliche Intelligenz (Lipton, 2015). Tangiert werden insbesondere das Grundrecht auf Schutz der Persönlichkeit (Art. 2 Abs. 1 i.V.m. Art 1 Abs.1 GG) und das darunterfallende Recht auf Schutz der informationellen Selbstbestimmung und der Vertraulichkeit und Integrität informationstechnischer Systeme (BVerfGE 65, 1ff./BVerfGE 120, 274, in: Papier 2018, 174).

In den Sozialwissenschaften und im Völker- und Internationalen Recht verweisen Autoren gern auf die entsprechenden Grundgesetzartikel über die Meinungsfreiheit, die Unantastbarkeit der Würde oder vom Schutz der Privatsphäre und den Datenschutz.

Grundrechte sind primär Freiheits- und Abwehrrechte des Einzelnen und angesichts der Bedrohung durch »Dritte« greift eine staatliche Schutzpflicht als zweite Schutzfunktion. Allerdings sind staatliche Schutzpflichten nicht von gleicher Stringenz und Verbindlichkeit wie die persönlichen Abwehrrechte. Sie müssen vom

1 Der Beitrag basiert auf der Forschungsarbeit von Anja Mihr. Sabrina Görisch hat an der Nachbereitung der vorliegenden Fassung mitgewirkt.

2 Vgl. auch den Beitrag zur Privatheit von Carlos Becker und Sandra Seubert in diesem Band (Becker/Seubert 2019).

Gesetzgeber ausgestaltet werden, der ermisst, was ein angemessenes Schutzniveau ist (Papier 2018, 180ff.). Auf Basis der staatlichen Schutzpflichten wurden bereits Maßnahmen ergriffen. Artikel 38 der EU-Grundrechtecharta soll User vor der Verbreitung und Weiterverarbeitung ihrer Daten schützen. Hinzu kommt die im Mai 2016 in Kraft getretene Datenschutz-Grundverordnung (DSGVO). Auf Basis des in der DSGVO vermerkten Marktortprinzips (Art. 3) können auch Plattformbetreiber und andere Akteure außerhalb des EU-Raumes dazu angehalten werden, sich hinsichtlich der Verarbeitung personenbezogener Daten an das europäische Datenschutzrecht zu halten.

Ein anderes Beispiel ist die UN-Resolution 68/167 zu Sicherheitsfragen und der Privatsphäre im Internet aus dem Jahr 2013, in der die UN-Generalversammlung die Regierungen aufforderte, Maßnahmen zu ergreifen und die Menschenrechte auf der »Datenautobahn« zu schützen. Damals führte man »Verkehrsregeln« für die Nutzung des virtuellen Raums ein. Unter Bezugnahme auf die internationalen Menschenrechtsrechtsverträge sollten das Sammeln und die Weiterverarbeitung von persönlichen Daten unter gleichen und für alle nachvollziehbaren Kriterien offengelegt werden.

Ein umfassender Schutz der Grund- und Freiheitsrechte konnte laut Lipton (2015) bisher allerdings noch nicht gewährleistet werden. Dabei liegt die Herausforderung weniger in der Interpretation davon, welchen Stellenwert diese Rechte im Zeitalter von Big-Data und Sozialen Medien haben; sondern vielmehr darin, dass unsere demokratischen Entscheidungsprozesse und Rechtsstaatlichkeitspraxis kaum mehr Schritt halten können mit der Geschwindigkeit und der Dimension, mit der Daten im digitalen Raum generiert, verschoben und verarbeitet werden. Denn die Geschwindigkeit mit der heute Nachrichten gepostet und gelöscht oder auf andere Server verschoben werden, ist von keinem Parlament und keinem Gericht dieser Welt einholbar (Lipton 2015, 1ff.). Die unkontrollierte Geschwindigkeit und räumliche Entgrenzung der Datenverarbeitung lässt eine richterliche oder parlamentarische Überprüfung, ob und inwiefern Menschenrechte eingehalten oder verletzt werden, somit schwerlich zu.

Die Bilanz ist folgende: Durch die aktuellen Regulierungsversuche konnte keine funktionierende Ordnungsstruktur, geschweige denn Regierungsstruktur, innerhalb des digitalen Raums geschaffen werden. Doch soll es nicht bei einer Problemanalyse bleiben. Das Anliegen des Beitrags ist es, einerseits einen Überblick über die Grund- und Freiheitsrechte im digitalen Zeitalter zu ermöglichen und darüber hinaus auf Basis von theoretischen Überlegungen Kriterien herauszuarbeiten, die es in Hinblick einer zukünftigen Ordnungsstruktur des digitalen Raums zu beachten gilt. Dazu werden zunächst Potentiale der Digitalisierung für Grund- und Freiheitsrechte aufgezeigt (Abschnitt 1) und anschließend konkrete Herausforderungen wie Fake News (Abschnitt 2), künstliche Intelligenz und Big Data (Abschnitt 3) beleuchtet. Im 4. Abschnitt werden mögliche Regulierungsansätze dargestellt

und diskutiert. Der Aufsatz schließt mit einem konkludierenden Fazit (Abschnitt 5).

1. Digitalisierung als Chance für die Grund- und Freiheitsrechte

In Ländern mit wenig oder schwachen demokratischen Strukturen überlässt die Politik derzeit Internetgiganten wie Apple, Google und YouTube oder Microsoft öffentliche Dienstleitungen in Form von Presseinformationen, frei herunterzuladenden Gesundheits- oder Bildungs-Apps und somit auch die Entscheidung darüber, welche Daten weitergeleitet, welche Menschenrechte eingehalten werden und wer Zugang zum Internet haben darf und wer nicht.

Was aber für die Demokratie- und Regimeforschung eine Herausforderung darstellt, kann für die Umsetzung der Menschenrechte in diesen Ländern auch eine Chance sein. Denn ebenso wenig, wie Regierungen die Grundrechte alleine schützen können, können sie diese auch nicht einschränken. Der sekundenschnelle, milliardenfache Datenfluss entzieht sich meist jeder staatlichen Kontrolle. Vielmehr werden die Daten von privaten Unternehmen verwaltet und nicht selten von privaten Akteuren und zivilgesellschaftlichen Gruppen – und dazu gehören auch Menschenrechtsverteidiger – genutzt und weiterverarbeitet. In Autokratien, in denen öffentliche Proteste verboten werden und Opposition eine Farce ist, stellen der digitale Raum und Soziale Netzwerke oft die einzige Möglichkeit dar, Menschenrechte einzufordern – ungeachtet des Katz-und-Maus-Spiels staatlicher Zensurbehörden, Filtern und Trollen. Damit ist der digitale Raum zugleich eine Gefahr und eine Chance für die Grund- und Freiheitsrechte (Stier 2016).

2. Hetze und Fake News

Im Folgenden wird dargelegt, welche Herausforderungen Hetze, Verleumdungen und Fake News im Internet für die Grund- und Freiheitsrechte darstellen und welchen Schutz die Bürger innerhalb der EU genießen. In diesem Kontext wird oft der Bezug zu Cyber- oder Internet Governance, Cyberkriminalität und -gerechtigkeit und virtueller Gerichtsbarkeit hergestellt (Stöcker 2011, 236ff.). Vor allem bei den Themen Hetze und Hasskommentare, Verleumdungen und Fake News reagieren Öffentlichkeit und Politik nervös. Jennifer Eickelmann (2017) nennt diese Herausforderung die neue »digitale Verletzbarkeit«, die allein durch staatliche Stellen und Einrichtungen zur Bekämpfung von Internetkriminalität nicht behoben werden kann. Denn es ist noch nicht gänzlich ausgemacht, wer die Verursacher und wer die Opfer dieser »Verletzbarkeit« sind, und wer Internetkriminalität ausüben oder verhindern kann.

Die alleinige Feststellung, dass Menschenrechte sowohl online als auch offline dieselben sind, was die UN Generalversammlung bereits 2011 und 2013 wiederholt bestätigte, reicht nicht mehr aus. Ebenso wenig das jährliche Ausrufen von Safer-Internet-Days, die zahllosen Aufrufe zur Internet-Literacy, oder Facebooks »Election Operation Center« in Dublin, das Fake News zur Europawahl 2019 vom Netz nehmen wollte bis hin zu den Warnungen vor Selbstzensur. Sie alle scheitern an der Unbegrenztheit des digitalen Raums und der Geschwindigkeit, mit der Daten von einem Server auf den anderen, von einem Land ins andere verschoben und gepostet werden können.

Bei der Einhaltung und Umsetzung dieser Freiheitsrechte sind es vor allem private und kommerzielle Akteure und Dienstleister, die zur Verantwortung gezogen werden. So hat innerhalb der EU jeder das Recht, vor einer Behörde oder Gericht gehört zu werden und seine Akten einzusehen. Vor dem Gerichtshof der Europäischen Union in Luxemburg hat dies bereits zu Verfahren geführt, die Banken und Behörden entweder zum Löschen digitaler Daten aufgefordert oder zu deren Offenlegung gezwungen haben. Ähnliches wird für die Offenlegung von Algorithmen großer IT-Firmen gefordert. Im Zuge der Kontroversen um Fake News und Meinungsfreiheit unterstreicht Artikel 11 der Charta die freie Meinungsäußerung und Informationsfreiheit ebenso wie die Freiheit der (Sozialen) Medien, der Pluralität der Meinungsbildung Ausdruck zu verleihen, solange damit Dritte nicht zu Schaden kommen. Das heißt keineswegs, dass im Internet jeder sagen und posten kann, was er oder sie will. Beeinträchtigen Informationen und Daten das Wohl eines Dritten, müssen sie unterbunden werden. Wer aber soll im täglichen Ablauf millionenfacher Posts darüber entscheiden, wann der Schaden eintritt und worin dieser besteht? Jeden Fall vor ein Gericht zu bringen, würde schon an der Masse der Posts scheitern – geschweige denn, dass Richter mit der Geschwindigkeit des Postens je mithalten können. Jedes Verfahren würde Monate oder Jahre dauern. Hier sind also auch die kommerziellen Anbieter von Plattformen und Suchmaschinenbetreiber gefragt, Menschenrechtsstandards konsequent einzuhalten und Prozesse in Gang zu setzen, die nicht willkürlich sind, sondern diesen Standards folgen.

Durch »naming and shaming« sowie durch den Entzug von Vertrauen durch die Nutzer können private Anbieter dazu gebracht werden, bestimmte Darstellungen zu löschen oder ihre Firmenpolitik zu ändern, wie dies Facebook oder Google bereits mehrmals in den vergangenen Jahren getan haben. Oft sind es zivile Proteste oder die Intervention von privaten Hackern, die dazu führen, dass die Webseite geblockt oder die Nachrichten als Spam gefiltert werden.

Allein zur Europawahl in 2019 entfernte Facebook nach eigenen Angaben mehrere Tausende fingierte Nutzerkonten, die meisten davon Spam-Anbieter. Um Falschmeldungen geht es dabei weniger, sondern um Manipulation. Aber es gibt keine Instanz, die das überprüft (Facebook Newsroom, 29. März 2019).

Zudem kann man falsche Meldungen zwar löschen, aber falsche Behauptungen nicht, die etwa gegen Politiker gerichtet sind. Die werden in der Regel von Meinungsfreiheit abgedeckt. Facebook und andere Plattformen verweisen daher auf Faktenchecker, die inzwischen auf jedem Nachrichtenportal zu finden sind, aber keine signifikanten Verbesserungen des Menschenrechtsschutzes hervorgebracht haben. Einmal getwittert, sind Fake News oder Hetze schwerlich zu löschen und finden sich spätestens im Darknet wieder. Selbst wenn es ein »Menschenrecht auf Vergessen oder Löschen« gäbe, so wird es technisch und juristisch kaum möglich sein, dieses durchzusetzen.

Um Schaden durch Hetze und Verleumdungen zu vermeiden, müssen die Anbieter und Verantwortliche diese transparent machen und die Täter aufgrund ihrer IP-Adressen auch durch selbst auferlegte und immer wieder neu ausgehandelte Sanktionen zur Rechenschaft ziehen. Zahlreiche Urteile des Europäischen Gerichtshofs für Menschenrechte verpflichten bereits ihre Mitgliedsstaaten und ansässigen Provider und Unternehmen, ihre Kunden oder Nutzer zu »entlarven«, damit sie zur Verantwortung gezogen werden können (Free Media Center 2018, 5f.). Der Datenschutz wird somit bei Menschenrechtsverletzungen eingeschränkt, aber diese müssen (bislang) von einem Gericht als solche benannt werden. Hinzu kommt, dass nur wenige EU-Mitgliedstaaten Daten zu Straftaten, die im digitalen Raum stattfinden, erheben. Sie werden oft nicht ausgewiesen. Darüber hinaus führt mangelndes Vertrauen in die Strafjustizsysteme und den Rechtsstaat dazu, dass die Mehrheit der Opfer von Verleumdungen im Internet diese nicht melden. Vor allem Migranten, Angehörige von Minderheiten und Frauen, die besonders stark von Verleumdungen und Bedrohungen betroffen sind, scheuen aus Furcht vor Repressalien eine öffentliche Anzeige. Selbstzensur und die Einschränkung der Nutzung des digitalen Raums ist die häufigste Folge.

Hetze gegen Migranten, Flüchtlinge oder gegen Roma, LGBTQI und Muslime nehmen insbesondere seit 2015 zu und wurden durch die populistischen Bewegungen seither verstärkt. Das Free Media Center in London hat 2018 eine Studie zur Umsetzung und Verletzung der Meinungsfreiheit im Netz herausgegeben (Free Media Center 2018). Sie fanden heraus, dass in Großbritannien »Hassreden« gegen EU-Migranten seit der Brexit-Kampagne 2016 massiv zugenommen haben. Politiker, darunter auch der ehemalige britische Premierminister David Cameron, hatten im Vorfeld der Kampagne angekündigt, Migrationsrechte im Kampf gegen den Terrorismus einzuschränken. Pauschalisierungen dieser Art schürten die Hetze gegen Migranten im Internet. In Polen und Ungarn haben nationale Regierungen eine Antimigrationspolitik geschürt. Und in Italien, Deutschland und Österreich war eine einseitige Berichterstattung über Einwanderung Teil der öffentlichen Debatte während der Wahlkampagnen. Rechte Parteien, Politiker und Beamte sowie explizit fremdenfeindliche Bewegungen verantworten gemeinsam die steigende Feindseligkeit gegenüber Minderheiten, Migranten und Flüchtlin-

gen im Internet und Sozialen Medien. Sinkendes Vertrauen in politische Parteien und Regierungen und die Wahlsiege populistischer und rechtsgerichteter Parteien waren eines der Ergebnisse. Diese Beispiele zeigen, dass ein Großteil der Verantwortung auch bei Regierungen und nicht allein bei anonym organisierten rechten Gruppierungen oder privaten Internetseitenbetreibern im Darknet liegt.

Mit der wachsenden Verlagerung von Wahlkämpfen in den digitalen Raum verändert sich auch die politische Kultur; wie das Beispiel der Präsidentschaftswahl in der Ukraine in 2019 zeigt, wo der Gewinner, Wolodymyr Selenskyj, seinen Wahlkampf maßgeblich in Sozialen Medien und auf YouTube gestaltet hat (Kosmehl 2019, 12). Eine direkte Auseinandersetzung im öffentlichen Raum, bei der auch Fakten überprüft und gegebenenfalls korrigiert werden können, findet trotz einzelner Initiativen (z.B. im SWR der »Faktencheck Fakenews«) nicht immer hinreichend statt. Überzeugungsarbeit und politische Auseinandersetzung im digitalen Zeitalter brauchen keinen persönlichen Kontakt. Vertrauen soll stattdessen dadurch gewonnen werden, indem der Kandidat permanent virtuell präsent ist, Posts und Twitter-Nachrichten anderer dementiert und diesen seine eigenen entgegensetzt, wie es der US-amerikanische und der brasilianische Präsident per Twitter praktizieren, ohne sich dabei einer direkten Auseinandersetzung stellen zu müssen. Noch sind die Folgen, die dies für unsere politische Kultur hat, nicht abzuschätzen.

Ähnliches trifft für Kraftausdrücke, Stereotypisierungen, Zuschreibungen und eine Abwertung anderer zu. Sie sind nicht immer sofort als Hassreden oder Hetze mit Folgeschäden identifizierbar wie etwa: »Er ist zwar Araber, aber trotzdem fleißig.« Aufforderungen, wie »Politiker an den Galgen« verführen womöglich gar zu Gewalttaten und verletzen die Würde und Unversehrtheit des Einzelnen. Fake News und Lügen, wie »Flüchtlinge begrapschen Schulmädchen«, sind gefährlich, denn was sie alle gemein haben ist das Ziel der Aus- und Abgrenzung und die Folgen davon sind Diskriminierung und Gewalt. Sie verletzen das Gleichheitsprinzip mit den Folgen verbaler und zum Teil physischer Gewalt (Mueller 2004, 245ff.).

Wie dargelegt, besteht noch kein hinreichender Schutz gegen Hetze und Fake News. Manche Staaten zeichnen sich durch eine Doppelrolle aus. Sie sind nicht nur Beschützer, sondern teils auch Angreifer der Menschenrechte. So kommen Hetze und Fake News zum Teil als politisches Instrument zum Einsatz. Ihre Rolle als Beschützer ist zudem durch die Undurchsichtigkeit des Datenflusses eingeschränkt, wodurch vermehrt Anbieter die Rolle einnehmen, die Grund- und Freiheitsrechte zu schützen. Seitens der Nutzer, insbesondere der Minderheiten, wurde das Problem der Selbstzensur und der ausbleibenden Meldung von Straftaten identifiziert.

3. Künstliche Intelligenz und Big Data und Grundrechte

Künstliche Intelligenz (KI) und Big Data[3] dominieren neben dem Thema Hetze und Fake News inzwischen auch die wissenschaftlichen Debatten um menschenrechtsbasierten Schutz von Grund- und Freiheitsrechten. Dabei spielen ethisch-moralische Fragen nach der Würde ebenso eine Rolle wie die der Justiziabilität und die Frage, in welcher Gesellschaftsordnung wir in Zukunft leben wollen.

Da die Dimension des digitalen Raumes teilweise mit unseren normalen Vorstellungen von Räumlichkeit und ihrer Begrenztheit nichts mehr zu tun haben, kommt der Einsatz von KI ins Spiel, zum Beispiel indem Algorithmen eine mögliche Verletzung von Grundrechten automatisch anzeigen und den Provider oder Nutzer blockieren, was teilweise mit den Filtern bei Facebook, YouTube und Google schon passiert. Allerdings werfen die Filter bei diesen Anbietern eher neue Fragen auf, als dass sie diese beantworten, wenn beispielweise ein Algorithmus das Posten von Fotos antiker Skulpturen nicht als Kulturgut, sondern als Pornographie identifiziert und diese automatisch löscht. Sollte einem Algorithmus tatsächlich die alleinige Entscheidung überlassen werden, was Kunst und was Meinungsfreiheit ist und was nicht? Wenn solche Fragen auftauchen, ist das Konzept problematisch. Sicherlich kann man diese Algorithmen nachprogrammieren, aber übrig bleibt die Frage, wie viel menschliche Intervention am Ende komplementär zu jedem Algorithmus stehen muss.

Für die Europäische Kommission sind KI-Systeme, die intelligentes Verhalten zeigen, indem sie ihre Umgebung analysieren und mit einem gewissen Grad an Autonomie Maßnahmen ergreifen und menschliche Entscheidungen vorwegnehmen, problematisch. Vor allem im Online-Marketing und der Weiterverarbeitung unserer Daten kommt dies zum Ausdruck. KI-basierte Systeme können rein softwarebasiert sein und daher zunächst nur in der virtuellen Welt unsere freie Entscheidungsfindung beeinträchtigen, ohne dass ein Programmierer je diese Absicht gehabt hätte. Das trifft beispielsweise bei Sprachassistenten, Bildanalyse-Software, Suchmaschinen, Sprach- und Gesichtserkennungssystemen zu. Dadurch kann das Maß an Entscheidungshoheit und damit die Würde des Menschen angegriffen werden. Die High Level Expert Group on Artificial Intelligence beschäftigt sich daher auch mit den Fragen, wie bei der Früherkennung von Krankheiten oder bei der Gleichstellung der Geschlechter, Stichwort Gender-Neutrales-Internet, Diskriminierung und Ausgrenzung verhindert werden können. Das sind grundlegende Menschenrechtsfragen, bei denen es um die Würde des Einzelnen und das Gemeinwohl geht (FRA 2018b, 43ff.). Ob lernende Roboter, autonome Fahrzeuge oder der Einsatz von Drohnen und das Internet-of-Things und in Smart-Cities – in jedem Fall sollte der Mensch die letzte Entscheidungsinstanz sein (FRA 2018a). Denn

3 Vgl. hierfür auch den Beitrag von Lena Ulbricht in diesem Band (Ulbricht 2019).

es besteht die Gefahr der »Eigendynamik« dieser Systeme, die unsere selbstständige Entscheidungsfindung vorwegnimmt und nicht mehr kontrollierbar sein kann. Nur wie wir KI am besten nutzen, ohne unsere Entscheidungshoheit abzugeben, darauf hat auch die Grundrechtecharta keine Antwort.

Zeitgenössische Modernisierungstheoretiker wie Inglehart und Welzel (2007), die sich unter anderem mit der Wirkung globaler Werte auf unser soziales Ordnungssystem, zu denen heute auch KI-gesteuerte Infrastrukturprojekte gehören, befassten, sehen darin dennoch auch eine Chance.

Darüber hinaus wird KI vor allem in alltäglichen Kontexten diskutiert, also all jenen Bereichen, die uns tagtäglich umgeben, zum Beispiel in der Weiterverarbeitung von personenbezogenen Daten durch Smartphones und dem täglichen Gebrauch von Suchmaschinen und Apps. Seit 2010 bis heute hat sich das Datenvolumen verdreifacht (Handelsblatt 2019). KI betrifft inzwischen alle Lebensbereiche wie etwa unsere freie Entscheidung, geschützte Kommunikation oder die persönliche und öffentliche Sicherheit. Die EU bietet beispielsweise Leitlinien für die Entwicklung von Gesetzen und Empfehlungen für die Verwendung von KI an. Darin geht es vor allem auch um das Bewusstsein und die Vermeidung schlechter und das heißt falscher Daten und den Schaden, den KI damit anrichten kann (Europäische Kommission, 8. April 2019).

Bei den Diskussionen der Gesetzgeber geht es darum, wie falsche und unvollständige Daten erkannt und gelöscht werden können. Konto- und Gesundheitsdaten oder Verbraucherdaten sind persönliche und werden verarbeitet. Aber wenn diese Daten falsche Angaben und Aussagen über uns enthalten, können sie die Gleichstellung und Chancengleichheit auf dem Arbeitsmarkt oder im Versicherungswesen verletzen. KI kann den Prozess der unautorisierten Weitergabe falscher Angaben noch beschleunigen und stellt darin eine Verletzung der Grundrechte dar (Europarat 2018).

Programmierer ebenso wie Politiker wissen, dass ein Algorithmus in seiner Anwendung nur so gut sein kann wie die Daten, die er verwenden kann. Aber die Deutung darüber, welche Daten verwendet werden sollen, ist auch eine gesellschaftspolitische Aufgabe und keine von Programmierern. Genau dem stellen sich die Ethikräte, die unter anderem eine menschenrechtsbasierte Anwendung von Daten bei der Programmierung fordern. Unautorisierte und falsche Daten, die beabsichtigt oder unbeabsichtigt aus dem Kontext heraus weiterverarbeitet werden, können zu falschen und gefährlichen Ergebnissen, zum Beispiel in der Flugsicherung oder in der Finanzbranche, bei Marktanalysen oder der Kriminalitätsbekämpfung, führen (FRA 2018). Denn selbst wenn die Daten akkurat sind, beispielsweise bezüglich des Geschlechts und der Ethnie oder des Einkommens, kann ihre Weitergabe zu Diskriminierung führen, zum Beispiel bei Einstellungsverfahren. Dies hat die EU-Grundrechteagentur (FRA) in Wien in einem Fokuspapier untersucht (FRA Focus 2018). Aus dem Kontext genommene Daten, die nicht die Bevölkerung repräsentie-

ren, können folglich zu voreingenommenen Entscheidungen und Analysen führen, vorhandene Vorurteile und diskriminierendes Verhalten widerspiegeln, die dann von einem KI-System aufgegriffen und verstärkt werden.

Damit wird das Grundrecht auf Nichtdiskriminierung, Artikel 21 der EU-Grundrechtecharta, verletzt. Die Verwendung von nicht repräsentativen oder voreingenommenen Daten kann zu einer Ungleichbehandlung von Personen aufgrund der im Datensatz stehenden Attribute führen (FRA 2018a). Somit kann KI die Ungleichheit zwischen Ethnien, Geschlechtern, bei Altersunterschieden, Behinderung erhöhen und verstärken (Prates/Avelar/Lamb 2018, 1ff.). Im Kontext dieser Diskussionen hat die High-Level Expert Group der EU zu KI im April 2019 die ersten Ethik-Richtlinien veröffentlicht, die unter anderem eine genaue Datenprüfung als eine der Anforderungen einer vertrauenswürdigen KI einschließen (European Union High Level Expert Group 2019). Daten können sowohl von dem KI-System als auch von Menschen falsch eingegeben, eingeschätzt und interpretiert werden. Menschenrechtsbasierte Richtlinien sollen helfen, diese Fehleinschätzungen zu verhindern.

Aber nicht nur die EU sieht die Notwendigkeit transnationaler Richtlinien. In der im Mai 2018 verabschiedeten Erklärung von Toronto (The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems), weisen grenzüberschreitend Juristen, IT-Vertreter und Wissenschaftler auf die Möglichkeit zur Vermeidung von Voreingenommenheit und Diskriminierung in maschinellen Lernsystemen hin. Die Initiatoren fordern kommerzielle Unternehmen wie Google oder Amazon auf, den Risiken Rechnung zu tragen, die mit maschinellen Lernsystemen verbunden sind. Diese sollen transparente Qualitätskriterien aufstellen, um unvollständige oder nicht-repräsentative Daten oder Datensätze zu vermeiden (Toronto Declaration 2018).

Insgesamt zeichnet sich der Umgang mit KI durch eine umfassende ethische Auseinandersetzung seitens staatlicher und ziviler Akteure aus. Statt einer grundlegenden Skepsis nachzugehen, gilt es, eine Offenheit zu bewahren und Anwendungsbereiche zu bestimmen, in denen KI-Systeme wie beispielweise automatisiertes Entscheiden sinnvoll sind, also trotz Risiken geduldet werden können (Trute 2018).

4. Mögliche (Regulierungs-)Ansätze zum Grundrechte-Schutz

Hinsichtlich der generellen Problematik des Schutzes der Menschenrechte im digitalen Zeitalter diskutieren sozialwissenschafliche Autoren mit einer theoriebasierten Einschätzung dessen, was unter den oben skizzierten Bedingungen (Entgrenzung und Beschleunigung des Datenflusses, Hetze, Fake News etc.) zum Schutze der Grund- und Freiheitsrechte möglich ist. Zentral ist in der aktuellen For-

schung außerdem die Frage, welche Kriterien eine Ordnungsstruktur für den digitalen Raum beachten sollte und von wem und wie der Schutz der Grundrechte umgesetzt werden könnte. Im Folgenden werden die Überlegungen und dazugehörige Beispiele entlang der Punkte »Demokratischer Aushandlungsprozess & digitaler Gesellschaftsvertrag« (Abschnitt 4.1), »geteilte (globale) Verantwortlichkeit« (Abschnitt 4.2), »Modernisierung und menschenrechtsbasierter Ansatz« (Abschnitt 4.3) sowie »Selbstzensur und Selbstjustiz« (Abschnitt 4.4) dargestellt.

4.1 Demokratischer Aushandlungsprozess und digitaler Gesellschaftsvertrag

Der Rechtsphilosoph John Rawls, der die Menschenrechte im Sinne Immanuel Kants Naturrechtsthese als ein »Recht der Völker« erklärt, arbeitet Herausforderungen heraus, die dem Schutz der Grund- und Freiheitsrechte gegenüberstehen, er legt jedoch keine dauerhafte Lösung vor, wie diese umgesetzt, eingehalten oder gar regiert werden sollen. Immerhin konstatiert Rawls in seiner Theorie vom Recht der Völker, dass Menschenrechte nur in liberal-demokratischen Gesellschaften verwirklicht werden können. Gleichwohl liegt deren fundamentale Herausforderung darin, egalitäre Prinzipien und Regeln für alle zu etablieren und diese dauerhaft aufrechtzuerhalten. Denn ohne diese Prinzipien und Regeln können Menschenrechte nicht eingehalten werden. Daher sind die freie, egalitäre und faire Teilhabe aller Menschen die Grundvoraussetzung, damit Menschenrechte überhaupt umfassend verwirklicht werden können. Wenn dies aber nur in liberaldemokratischen Ordnungssystemen möglich ist, von denen gegenwärtig nur ein Bruchteil der Weltbevölkerung profitiert, dann ist der Schutz der Grund- und Freiheitsrechte im digitalen Zeitalter schon jetzt zum Scheitern verurteilt. Dennoch, so Rawls, können nur unter diesen Bedingungen die Menschenrechte freier und sich respektierender Völker verwirklicht werden (Rawls 1999). Rawls' Diskurs von einst ähnelt in vielerlei Hinsicht demjenigen über den Schutz der Grundrechte im digitalen Zeitalter. Denn er beschreibt Gesellschaftsformen, in denen es wenig staatliche Kontrolle gibt, gleich ob im virtuellen oder realen Raum. Gleichzeitig aber betont er die Notwendigkeit, dass die (neuen) egalitären und partizipativen Prinzipien durch die unterschiedlichsten privaten, zivilen und politischen Akteure demokratisch ausgehandelt werden können, um eine gesellschaftliche Ordnung (im digitalen Raum) herzustellen.

Im Gegensatz zum Rawls'schen Ziel einer rechtsstaatlichen Ordnung, beschreibt der Internetpionier John Perry Barlow in seiner »Unabhängigkeitserklärung für den Cyber-Raum« den digitalen Raum als nicht regierbar und nichtregiert (Barlow 1996). Barlow war sich damals sicher, dass die Internetgemeinde bestehend aus kommerziellen Unternehmern, Zivilgesellschaft und Politik ihren eigenen Gesellschaftsvertrag entwickeln werde, um zu bestimmen, wie sie mit

den Herausforderungen umgehen wolle. Für ihn stand dabei allerdings auch fest, dass diese Internet-Governance-Strukturen auf Grundlage der Menschenrechte nach demokratischen Prinzipien gebildet werden müssten und den Bürgern nicht aufoktroyiert werden könnten (Mihr 2016). Darin findet sich ebenso wie bei Rawls der Anspruch einer demokratischen Leitkultur für das Internet. Zudem findet sich darin ein Verständnis davon, von wem eine Regulierung des digitalen Raums ausgehen soll.

Am deutlichsten ist dieser gegenwärtig stattfindende Aushandlungsprozess auf EU-Ebene zu beobachten. Ein Beispiel dafür ist die 2018 gegründete High Level Expert Group on Artificial Intelligence, die aus über 50 Vertreterinnen von Wirtschaft, Politik und Wissenschaft besteht. Das Panel beschäftigt sich mit dem Verhältnis zwischen Ethik, Wirtschaftsinteressen und Menschenrechten und der Frage, ob und inwiefern Freiheitsrechte der Bürger beeinträchtigt werden.[4]

Darüber hinaus gibt es eine Vielzahl nationaler, virtueller, kommerzieller und internationaler Gremien, Arbeitsgruppen, Foren und Organisationen, die sich derzeit weltweit genau mit dieser Frage beschäftigen. Es gibt kaum ein Land, welches nicht ein nationales Internet Governance Forum oder eine Ethik-Kommission und eine Zivilgesellschaft oder Wissenschaftsräte hat, die über Künstliche-Intelligenz-Strategien (kurz: KI-Strategien) diskutieren (Global Cybersecurity Index 2018).

Aus sozialwissenschaftlicher Sicht wird auch die Frage nach dem gesellschaftlichen Wandel durch neue Technologien diskutiert und inwiefern globale Menschenrechtsnormen zu einer neuen transnationalen und globalen Ordnungsstruktur im digitalen Raum beitragen. Vertreter konstruktivistischer Theorien oder des Neuen Institutionalismus befassen sich ebenso mit dieser Frage wie beispielsweise innerhalb der Internationale Beziehungen oder der Demokratie- und Autokratieforschung. Wie also können Menschenrechtsnormen Regimebildung zu Internet-Governance steuern oder wie kann E-Governance das Verständnis von Regieren verändern?

Mit anderen Worten: Wann wird Virtualität zur Realität und wann umgekehrt? Eine Antwort ist, dass auch dies in jedem Fall neu ausgehandelt werden muss, aber dies nicht allein durch langwierige Gerichtsverfahren geschehen kann, sondern durch selbstauferlegte und ausgehandelte Regeln und Sanktionen – im Sinne eines digitalen Gesellschaftsvertrages- und die bei der Missachtung von Menschenrechten unmittelbar wirken, z.B. Löschen einer Plattform oder Verweigerung ei-

4 Rechtlicher und politischer Maßstab für die Gruppe ist die EU-Grundrechtecharta von 2000, die unter anderem den Schutz personenbezogener Daten, in Artikel 8 der Charta festlegt, und die Achtung des Privat- und Familienlebens in der Wohnung und Informationsfreiheit (Artikel 7) im privaten Raum mit dem digitalen Raum gleichsetzt. Das betrifft unsere Privatsphäre auf sozialen Plattformen und Netzwerken ebenso wie die Nutzung unserer Daten innerhalb der Anwendungen von KI. Hier gelten dieselben Prinzipien der Würde, Freiheit und Sicherheit, wie im Nicht-Digitalen (Jorgensen 2006, 1ff.).

nes Zugangs. Nur willkürlich und ohne jede multi-akteursbasierte Kontrolle darf dies nicht geschehen. Ebenso wie die Richter an den internationalen Menschenrechtsgerichtshöfen, in jedem Fall neu festlegen müssen, welchen Schaden ein Eintrag auf Facebook tatsächlich angerichtet hat, müssen auch Sanktionen klaren und transparenten Regeln und einem Deutungsschema folgen. Diese sind unter anderem abhängig von der unmittelbaren Gefahr, die eine Nachricht oder Blog im Internet verursachen kann. Außerdem muss es Einspruchsmöglichkeiten geben, da sich selbstverständlich auch ein Algorithmus »irren« kann. Wenn es allein danach geht, stellt der Schutz der Grundrechte im digitalen Raum eigentlich keine besondere Herausforderung dar. Sieht man sich aber die Geschwindigkeit und die Dimension an, mit der diese Einträge gepostet und gelöscht werden, dann wird schnell klar, dass selbst mit den modernsten technischen und demokratischsten aller Methoden und Gremien, der Schutz der Grundrechte allein nicht aufrechterhalten werden kann.

4.2 Geteilte (globale) Verantwortlichkeit

In der weiten gesellschaftlichen Debatte ist die Frage noch ungeklärt, wie viel Kontrolle dem Staat oder internationalen Organisationen, und wie viel den kommerziellen Anbietern und Providern wie Google und Microsoft gegeben werden sollte. Sollen Programmierer für Facebook und Alibaba selbst darüber entscheiden, was Hasskommentare und Pornographie sind? Und sollen Unternehmen wie Google Glasfaserkabel auf eigene Kosten verlegen, um einen Zugang zum Internet zu garantieren? Die Frage: »Wer entscheidet und wer regiert und kontrolliert den digitalen Raum?«, ist aktueller denn je, und eine abschließende Antwort gibt es nicht. Und vor allem: Wer hat am Ende die Autorität und Legitimität, um Menschenrechte im digitalen Raum umzusetzen und einzufordern? Noch vor einigen Dekaden wurde diese Frage stets damit beantwortet, dass es der Staat sei, der im Sinne des Völkerrechts primär die Verantwortung hat, die Grundrechte seiner Bürger zu schützen. Das sieht heute ganz anders aus. Firmen und Anbieter, Blogger und Nutzer, staatliche Behörden können sowohl Täter als auch Opfer sein. Heute geht man von einer geteilten Verantwortlichkeit, der so genannten shared-responsibility, aus (Büst 2015), bei der alle, gleich ob Provider, Staat oder Nutzer, die zu den Folgen von Hasskommentaren und Verleumdungen beigetragen haben, ihren Teil der Verantwortung tragen sollen. So können Online-Plattform-Betreiber, Suchmaschinen, Blogger, politische Parteien, Messenger-Dienste, und all jene, die aufgrund von Falschaussagen oder Hasskommentaren, bei der eine Person zu Schaden kam, in geteilter Weise für die Entschädigung in Form von Zahlung oder gar Haftstrafen in Frage kommen. Den *einen* Verantwortlichen – nämlich den Staat – wird es in Zukunft wohl kaum noch geben bzw. man wird ihn kaum mehr allein zur Verantwortung ziehen können. Das zeigt schon die Diskussion und Entwicklung um

internationale Strafgerichtsbarkeit, bei dem einzelne War Lords und Firmenchefs vor Gericht stehen, und nicht mehr der Staat. Das aber sind nicht nur juristische Fragen, sondern gesellschaftliche und politische, die dahingehend zu beantworten sind, wer am Ende die legitime Autorität und Verantwortung besitzt. Deutlich ist, dass die Grund- und Freiheitsrechte im digitalen Zeitalter kein nationales Politikfeld sind, sondern transnational durch mehrere Akteure geschützt werden müssen.

Ähnliches sieht bereits die UN-Resolution 70/125 von 2015 zum Multi-Stakeholder-Ansatz vor, ein Ergebnis der IGF-Initiativen der Jahre zuvor. Darin fordern die 193 UN-Mitgliedstaaten sich selbst und andere auf, Verantwortlichkeiten und Entscheidungsbefugnisse im digitalen Zeitalter neu zu verteilen. Das Internet und den digitalen Raum allein der Privatwirtschaft und Nutzern zu überlassen, wie es in oft korrupten und schwachen Staaten der Fall ist, ist dabei nicht gemeint. Aber die Praxis zeigt, dass in ärmeren und weniger demokratischen Ländern, private Dienstleister den Zugang zum Internet überhaupt erst ermöglichen. Hier ist es das Ziel, mehr staatliche Verantwortung wieder ins Spiel zu bringen, damit das Internet neutral, für alle zugänglich und sicher zu machen und von kommerziellen Anbietern abzukoppeln (Mihr 2017).

Auf der anderen Seite sollen Unternehmen wie Google, Facebook, Telegramm, Twitter, Skype, Ebay und Amazon in die Pflicht genommen werden. Verbraucherdaten sollen mit Rücksicht auf die Menschenrechte erst dann dem freien Markt zur Verfügung gestellt werden, wenn diese dem Datenschutz und damit auch den Grundfreiheiten der User entsprechen, z.B. indem Datenschutz und Privatsphäre deutlich geschützt sind. Europaweit wurde dies u.a. mit der EU-Datenschutz-Grundverordnung versucht umzusetzen, womit ein Großteil der Verantwortung für den Datenschutz auch auf die Unternehmen und Verbraucher verteilt worden ist. Damit folgt die EU vor allem einer Grundsatzentscheidung des Gerichtshofs der Europäischen Union (EuGH) vom Mai 2014, der alle EU-Staaten aufforderte den in der Grundrechtecharta verankerten Datenschutz umzusetzen.[5] Dies gilt auch für die Entscheidung des Gerichtshofes aus dem Jahr 2015 zum Thema »sicherer Hafen« für Datenübermittlung in die USA.[6] Dies sind Präzedenzfälle, auf die sich zukünftige Rechtsprechungen berufen werden. Grundsätzlich geht es bei all diesen Entscheidungen um die anteilige Verantwortung verschiedener Akteure.

Ingelhart und Welzel (2007) kommen zum Schluss, dass wertelegitimierte Autorität zunehmend vom Staat auf Einzelpersonen, also den (lokalen) Nutzern und zu privaten, kommerziellen Akteuren wandert. »Self-expressive values« führen zu kulturellem Wandel (Inglehart/Welzel 2007, 29ff.). Dieser wiederum determiniert unsere soziale Ordnung, auch im digitalen Raum, die festlegt, wer welche Entscheidungskompetenzen hat. Am Ende sind es nicht nur der Staat oder Firmen,

5 Info Curia – Rechtsprechung des Gerichtshofs: Urteil des EuGH, C-131/12, 13.5.2014.

6 Info Curia – Rechtsprechung des Gerichtshofs: Urteil des EuGH, ECLI:EU:C:2015:650, 6.10.2015.

sondern auch die Zivilgesellschaft und der einzelne User, die bestimmen, inwiefern seine Rechte eingeschränkt oder geschützt werden. Freilich gibt es berechtigte Zweifel daran, dass die ca. 4 Mrd. Internetuser, die sich täglich im digitalen Raum austauschen, informieren und posten, gleichermaßen aufgeklärt sind über ihre Menschenrechte, Grundverordnungen (EU-Grundrechtecharta/DSGVO) oder ihr Recht, bei Google, Facebook, Instagram, Amazon, YouTube und Co-Einspruch einzulegen und Daten zu löschen. Aber es geht bei diesen theoretischen Erklärungsversuchen in erster Linie darum, den sich gegenwärtig abzeichnenden dramatischen Wandel hin zur internetbasierten Individualgesellschaft zu deuten und zukünftige Ordnungsszenarien zu verstehen und zu prognostizieren.

Insgesamt kann festgehalten werden, dass die Frage nach dem Wer situationsspezifisch beantwortet werden sollte.

4.3 Modernisierung und menschenrechtebasierter Diskurs

Parallel zu konkreten rechtlichen Maßnahmen sowie Eingriffen durch zivilgesellschaftliche und wirtschaftliche Akteure ist die globale Verbreitung der Grund- und Freiheitsrechte in den letzten Jahrzehnten maßgeblich mitverantwortlich für einen globalen Normen- und Wertewandel hin zu einem stärkeren Menschenrechtsbewusstsein und -handeln. Dieser wiederum verändert unser Verständnis von Recht und sozialer Ordnung, offline wie auch online. Modernisierungstheoretiker wie Anthony Giddens (1992), Ronald Inglehart und Christian Welzel (2007) gehen der Frage nach, inwiefern Werte und Menschenrechte in der post-industriellen und postmodernen Gesellschaft neue Entscheidungsstrukturen schaffen. Sie schreiben dieser Kraft des Normativen nicht nur institutionelle Veränderungen zu, sondern auch moralisch, ethisch und damit gesellschaftliche und politische. Giddens stellt in seiner reflexiven Modernisierungstheorie den materiellen Ressourcen, wie etwa neuen Technologien und dem Internet, die immateriellen (autoritativen) gleich, so wie etwa die Grund- und Freiheitsrechte. Beide Ressourcen verändern eine Gesellschaft und ihre legitime Ordnung sowie die Interaktion auch im digitalen Raum. Mit der Zeit werden sich Praktiken entwickeln, die neue Regeln und Mechanismen schaffen, um die Menschenrechte einzufordern. Inwiefern diese durchgesetzt werden, muss zwischen den betreffenden Akteuren neu ausgehandelt werden (Giddens 1992). Giddens' Ansatz nimmt den gegenwärtigen Diskurs vorweg, der sich damit beschäftigt, inwiefern staatliche, zivilgesellschaftliche und privat-kommerzielle Akteure die Menschenrechte im digitalen Raum nicht nur schützen können, sondern auch schützen wollen. Denn zwingen kann man die privaten Akteure und Unternehmen nur bedingt, vielmehr müssen diese einen Nutzen, auch kommerziellen Profit darin sehen, die Grund- und Freiheitsrechte ihrer User zu schützen.

Mit dem menschenrechtsbasierten Ansatz (human rights based approach), argumentieren Beobachter wie Vandenhole und Kollegen (2014), können Grund- und

Freiheitsrechte auch im digitalen Zeitalter besser geschützt werden. Zwar geben auch sie zu, dass dieser Ansatz eher pragmatischer Natur ist und auf empirischen Beobachtungen in einzelnen Ländern und anhand von Fallbeispielen beruht und daher noch keine Theorie als solche darstellt. Es zeichnet sich jedoch langsam ein Muster ab, das sich zur Theoriebildung eignet. Sie beobachten, dass aufgeklärte lokale, individuelle und zivilgesellschaftliche Aktionen eher zu einem Wandel und institutioneller Anpassung führen, als wenn diese von staatlichen Stellen verordnet werden (Vandenhole et al. 2014, 275). Dabei zeichnet sich ab, dass sofern soziale Gruppen bzw. die User, den Menschenrechten eine Priorität einräumen, denen sich andere Werte wie etwa ethnische Zugehörigkeit, Religion, Nationalität oder Clanzugehörigkeit unterordnen, eine größere Chance haben, befolgt zu werden. Wie schon Inglehart und Welzel zu den Konsequenzen des globalen Wertewandels angemerkt haben, fordern immer mehr Akteure menschenrechtsbasiertes Handeln mit der Folge, dass sich bestehende Institutionen und Praktiken anpassen und verändern, bis hin zur Forderung nach mehr Demokratie. Dabei fordern Aktivisten (1) mehr Rechenschaftspflicht für Provider, aber auch für Blogger und User, (2) mehr Transparenz von Anbietern ihre Algorithmen offen zu legen, und (3) eine stärkere, transparentere und fairere Beteiligung unterschiedlicher Akteure aus Wirtschaft, Politik und Zivilgesellschaft am Aushandlungsprozess (siehe Forderungen des Multi-Stakeholder-Ansatzes).

4.4 Selbstzensur und Selbstjustiz

Selbstzensur ist nicht die Antwort auf die Herausforderungen, darauf weisen auch Inglehart und Welzel hin, wenn es um die effektive Regierbarkeit der postmodernen Gesellschaft geht (Inglehart/Welzel 2007, 191f.). Einhergehend mit Rawls' Einschätzung, dass am Ende nur liberal-demokratische Ordnungs- und Herrschaftsformen die Menschenrechte einhalten können, ist Selbstzensur die schlechteste aller Optionen. Nutzer werden indes zunehmend misstrauisch gegenüber den privaten Anbietern und geraten in eine Spirale aus Selbstzensur. Selbstzensur wiederum ist schädlich für die Demokratie und ganz ohne eine demokratische Grundordnung, können nach Rawls die Menschenrechte nicht eingehalten werden. Diese Grundordnung lebt von einer aktiven und freien Zivilgesellschaft und Bürgerschaft und wenn diese sich selbst zensiert und damit den demokratischen Prinzipien entzieht, können Grund- und Freiheitsrechte nicht geschützt werden.

Da die politischen und richterlichen Organe kaum noch angemessen auf die Geschwindigkeiten und die Datenexplosion im digitalen Zeitalter reagieren können, kommt es nicht nur zur Selbstzensur, sondern auch zur Selbstjustiz. Bei letzterer handelt es sich um selbsternannte Helfer und Hacker der Gerechtigkeit und Grundfreiheiten. Sie machen sich auf, Blogs und Einträge zu löschen, Dokumente zu leaken und Meinungen »richtig« zu stellen, allerdings oft nach Gutdünken.

Für Hacker ist beispielsweise Doxing zur politischen Waffe geworden. Der Begriff kommt von »docs«. »Doxer« sammeln Daten und Informationen und veröffentlichen diese dann anonym oder pseudonym auf speziellen Upload-Diensten oder sozialen Plattformen. Dabei sind die Grenzen zwischen selbsternannten Rettern für Transparenz und Gerechtigkeit, wie Wikileaks und Wistleblowern, und jene, die dabei selbst zu Verleumdern werden, oft fließend. Sie leaken und entlarven oder stellen Meinungen »richtig« aber nicht unbedingt im Sinne der Menschenrechte (Brühl, 2019).

Auch der Börsenspitzenreiter Alphabet-Holding, hinter dem sich der Google-Gigant und die Nummer Eins in der Datenverwertung verbirgt, geben vor, grundlegende Freiheitsrechte und vor allem wirtschaftliche und soziale Rechte zu fördern, indem sie Innovation, Start-Ups, Unternehmertum und Chancen für alle fordern – ungeachtet deren Herkunft. Informationsaustausch, Weiterbildung, Geschäftsgründung, Gesundheitsvorsorge politische Partizipation, Warenverkehr, und dergleichen, nichts geht mehr ohne die Produkte und Geschäftsmodelle von Alphabet, wie etwa YouTube, Google Play, Apps oder diverse Navigationsanbieter. Aber dabei geht es den Unternehmen nicht um einen holistischen Menschenrechtsansatz, sondern darum, die Daten ihrer Nutzer für weitere Geschäftsmodelle zu verwerten. Mit diesem Monopol wird der Gigant zum politischen Akteur, ohne demokratisch legitimiert zu sein. Denn beim Aushandeln eines möglichen neuen Gesellschaftsvertrags im Sinne von Barlow (1996) oder gar eines Ordnungsmodells im Sinne von Giddens (1992) sitzen Google und die anderen Datengiganten zwar mit am Tisch, und übernehmen staatliche Aufgaben als Dienstleister und bei Infrastrukturprojekten, wie etwa Googles Initiative zur Glasfaserkabelverlegung und kostenfreiem Zugang zum Internet in den USA und die Bereitstellung von Notfall-Apps in Indien, ohne sich aber dabei einer staatlichen Kontrolle oder den Menschenrechtsprinzipien beugen zu müssen. Daher ist die Forderung nach dem neutralen Internet, dass ohne Werbung kommerzieller Profitmaximierung auskommt, die vor allem in weniger wohlhabenden Ländern und Gesellschaften laut wird, auch eine Verwirklichung der Grund- und Freiheitsrechte auf Information und Teilhabe (Rifkin 2014, 255ff.).

5. Fazit

Der Schutz der Menschenrechte steht im Zeitalter der Digitalisierung weiterhin vor Herausforderungen, die mit den gängigen Kontroll- und Überprüfungsmechanismen nicht zu bewältigen sind. Durch die Digitalisierung entsteht ein schier unbegrenzter und beschleunigter Datenfluss, der durch die vorhandenen Regelungen und Gesetze schwerlich kontrolliert werden kann. Es konnte herausgearbeitet werden, dass die Funktion des Staates, die Grund- und Freiheitsrechte der Bürger zu

schützen, nicht im ausreichenden Maße greift. Neben staatlicher Zensur oder der Missachtung der Grundrechte seitens privater, global operierender Unternehmen, sind es vermehrt Hetze, Fake News sowie KI-Systeme, um die aktuelle Debatten um den Schutz der Menschenrechte kreisen.

Allen Diskussionen ist gemein, dass die Lösung dieser Herausforderungen nicht einem Akteur allein zugesprochen werden kann und am wenigsten dem staatlichen. Ausgehandelt werden muss, welche Rolle staatliche, private, kommerzielle und zivilgesellschaftliche Akteure im Multi-Stakeholder-Prozess von Internet-Governance und damit auch bei der Umsetzung und dem Schutz von Grund- und Freiheitsrechten in Zukunft haben.

Im Sinne von Giddens (1992) und Rawls (1999) liegt die Herausforderung von Verantwortung und Rechenschaftslegung maßgeblich in der Verteilung und der fairen Partizipation von Akteuren, entsprechende (demokratische) Strukturen zu schaffen, die den digitalen Raum mit dem analogen verbinden, also bestehende staatliche und zivilgesellschaftliche Strukturen mit denen im virtuellen Raum zu kombinieren, um die Menschenrechte im digitalen Zeitalter zu schützen. Ein solcher Schutz kann aber nur von allen ausgehen, entsprechend einem Gesellschaftsvertrag, wie Barlow (1996) ihn vorschlägt, der auch Sanktionsmöglichkeiten beinhaltet. In diesem Sinne überraschte auch der Vorschlag der High Level Expert Group der EU nicht, die in ihrem Dossier von 2019 von »Data-Governance« spricht, und nicht von staatlicher oder Internet-Governance im engeren Sinne.

Literaturverzeichnis

Barlow, John Perry (1996): A Declaration of the Independence of Cyberspace, Davos. URL: www.eff.org/cyberspace-independence (11.07.2019).

Becker, Carlos/Seubert, Sandra (2019): Die Stärkung europäischer Grundrechte im digitalen Zeitalter: demokratiepolitische Potentiale am Beispiel des Privatheitsschutzes. In: Hofmann et al. (Hg.): Politik in der digitalen Gesellschaft. Bielefeld, S. 225–245.

Büst, René (2015): Das große Missverständnis: Shared Responsibility in der Public Cloud.URL: https://www.crisp-research.com/das-grose-missverstandnis-shared-responsibility-der-public-cloud/(22.05.2019).

Brühl, Jannis (2019): Doxing – eine alte Hacker Waffe trifft den deutschen Mainstream, 8. Jan 2019. In: Süddeutsche Zeitung online. URL: https://www.sueddeutsche.de/digital/hack-doxing-privatsphaere-1.4278901 (10.07.2019).

Buolamwini, Joy/Gebru, Timnit, (2018): Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification«. In: Proceedings of Machine Learning Research – PMLR 81, S. 77–91.

Eickelmann, Jennifer (2017): »Hate Speech« und Verletzbarkeit im digitalen Zeitalter: Phänomene mediatisierter Missachtung aus Perspektive der Gender Media Studies. Bielefeld.

Europarat (2018): Europäische Ethik-Charta zum Einsatz künstlicher Intelligenz in Justizsystemen und deren Umfeld. URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c (22.05.2019).

European Union High Level Expert Group on Artificial Intelligence (2019): Guidelines. URL: https://ec.europa.eu/futurium/en/ai-allianceconsultation/guidelines#Top (22.05.2019).

Europäische Kommission (2019): Künstliche Intelligenz, 08. April 2019. URL: https://ec.europa.eu/commission/news/artificial-intelligence-2019-apr-08_de (26.08.2019).

Europäische Union (2000): EU-Grundrechtecharta. URL: https://www.europarl.europa.eu/charter/pdf/text_de.pdf (22.05.2019).

Europäische Union (Dezember 2015): EU Richtlinien zur Cybersicherheit URL: www.europarl.europa.eu/pdfs/news/expert/infopress/20151207IPR06449/20151207IPR06449_en.pdf (22.05.2019).

Facebook Newsroom (2019): Unsere Maßnahmen zum Schutz der Europawahl, 29. März 2019. URL: https://de.newsroom.fb.com/news/2019/03/unsere-massnahmen-zum-schutz-der-europawahl/(10.07.2019).

Free World Center (2018): Article 19. Responding to ›hate speech‹: Comparative overview of six EU countries. URL: https://www.article19.org/wp-content/uploads/2018/03/ECA-hate-speech-compilation-report_March2018.pdf (22.05.2019).

Fundamental Rights Agency (FRA) Focus (2018a): #BigData: Discrimination in data-supported decision making.

Fundamental Rights Agency (FRA) (2018b): Under watchful eyes biometrics, EU IT systems and fundamental rights.

Giddens, Anthony (1992): Kritische Theorie der Spätmodernen. Wien.

Heide, Dana (2019): Studie zum Internetausbau. In: Handelsblatt. URL: https://www.handelsblatt.com/politik/deutschland/studie-zum-internetausbau-verdreifachung-des-datenvolumens-weltweit-bis-2019/13716800-2.html (26.08.2019).

Inglehart, Roland/Welzel, Christian (2007): Modernization, Cultural Change, and Democracy, The Human Development Sequence. Cambridge.

International Telecommunication Union (2018): Global Cybersecurity Index. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

Internet Rights & Principles Coalition (2014): Die Charta der Menschenrechte und Prinzipien für das Internet, United Nations, 2013. URL: www.inter-

netrightsandprinciples.org/site/wpcontent/uploads/2014/06/IRPC_booklet_29May2014_German.pdf (22.05.2019).

Islam iQ (2019): Terrorverdacht wegen arabischem Namen. URL: www.islamiq.de/2019/04/30/terrorverdacht-wegen-arabischem-namen/(22.05.2019).

Japkowicz, Nathalie/Stefanowski, Jerzy (Hg.) (2016): Big-Data-Analyse: Neue Algorithmen für eine neue Gesellschaft. Wiesbaden.

Jorgensen, Rikke Frank (2006): Human Rights in the Global Information Society. London.

Kleinwächter, Wolfgang (2006): Globalisierung und Cyberspace. Der Weltgipfel über die Informationsgesellschaft weist den Weg. In: Zeitschrift Vereinte Nationen 6 (1-2), S. 38–44.

Kosmehl, Miriam (2019): Die Ukraine als europäische Wohlstandsoase – Wasyl Holoborodkos Vision hat überzeugt. In: Ukraine-Analysen 217, S. 12–14.

Lipton, Jacqueline (2015): Rethinking Cyberlaw, A new Version for Internet Law. Cheltenham.

Mihr, Anja (2017): Cyber Justice: Human Rights and Good Governance for the Internet. Wiesbaden.

Mihr, Anja (2016): Ein Cyber-Gesellschaftsvertrag für die Menschenrechte. In: Zeitschrift für Menschenrechte10 (1), S. 44–59

Mueller, Milton L. (2004): Ruling the Root. London.

Papier, Hans-Jürgen (2018): Herausforderungen des Rechtsstaats im Zeitalter der Digitalisierung. In: Bär et al. (Hg.): Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht. Berlin und Heidelberg, S. 171–183.

Prates, Marcelo/Avelar, Pedro/Lamb, Luis (2018): »Bewertung der geschlechtsspezifischen Abweichungen bei der maschinellen Übersetzung – Eine Fallstudie mit Google Translate«, AdRR abs/1809.02208, S. 1-31.

Rawls, John (1999): The Law of the Peoples. Cambridge.

Rifkin, Jeremy (2014): The Zero Marginal Cost Society, The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism. Basingstoke.

Stier, Sebastian (2016): Internet und Regimetyp. Netzpolitik und politische Online-Kommunikation in Autokratien und Demokratien. Heidelberg.

Stöcker, Christian (2011): Nerd Attack! Eine Geschichte der digitalen Welt von C64 bis zu Twitter und Facebook. München.

The Toronto Declaration (2018): Protecting the rights to equality and non-discrimination in machine learning systems, May 2018. In: Access now Policy Team. URL: https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/(22.05.2019).

Trute, Hans-Heinrich (2018): Rechtliche Herausforderungen der Digitalisierung. Daten – Algorithmen – Wissen. In: Bär et al. (Hg.): Digitalisierung im Span-

nungsfeld von Politik, Wirtschaft, Wissenschaft und Recht. Berlin und Heidelberg, S. 303–313.

Ulbricht, Lena (2019): Big Data und Governance im digitalen Zeitalter. In: Hofmann et al. (Hg.): Politik in der digitalen Gesellschaft. Bielefeld, S. 289–307.

Vandenhole, Wouter et al. (2014): Some Crosscutting Issues and their policy implications.In:Gready/Vandenhole (Hg.): Human Rigths and Development in the New Millennium, Towards a Theory of Change. London, S. 272–300.