Personalisierung durch Profiling, Scoring, Microtargeting und mögliche Folgen für Demokratie – Funktionsweisen und Risiken aus datenschutzrechtlicher Sicht

Ulrich Kelber, Nils Leopold

1. Einleitung

Dass die weitgehende kommerzielle Datenausspähung der großen Internetunternehmen nicht allein ein Problem der davon betroffenen Bürgerinnen und Bürger ist, sondern letztlich auch weitreichende gesellschaftliche Folgen hat, wurde mit dem Aufkommen des Rechtspopulismus in den USA, Brasilien und Europa zum Thema mindestens der Diskussion in Fachkreisen. Hass und Hetze im Netz, Fake News, politische Wahlwerbung und Manipulation in Social Media sind als Bedrohung für die freiheitlichen Demokratien westlicher Ausprägung unübersehbar geworden.

Wenn es einen maßgeblichen Wendepunkt zu benennen gälte, der das Zusammenspiel aus Digitalisierung und der Furcht vor der Bedrohung der Demokratie ins kollektive Bewusstsein gehoben hat, so war es der Cambridge Analytica-Facebook-Fall. Vergleichbar den Snowden-Enthüllungen und dem folgenden weltweiten Geheimdienstskandal, wurden wie unter einem Brennglas gravierende negative Konsequenzen der rapiden globalen Digitalisierung deutlich. Als wenn ein Vorhang weggezogen wurde und den Blick freigibt auf die Hintergründe einer eigentlich bekannt-vertrauten Social Media-Szenerie: das gemütliche digitale Wohnzimmer, dem Millionen sich täglich so sehr anvertrauen, lag ausgebreitet vor uns, nur dieses Mal schauten überall die Drähte der Maschinen heraus. Es wurde klar, dass es eine sorgfältig gestellte digitale Kulisse war.

Genau diesen Vorhang immer wieder einen Stück weit zur Seite ziehen, um den Blick auf komplexe Mechanismen freizugeben, bewusst und sichtbar[1] zu machen, in welchem Umfang wir Menschen uns bereits in einem komplexen Zusammenspiel mit IT-Systemen befinden, stellt eine enorme Herausforderung dar. Charakteristisch für die digitale Entwicklung im

1 Vgl. Wischmeyer, AöR 2018 S. 20.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Umfeld gerade der Social Media Plattformen ist es, dass unser Selbstverständnis von Autonomie durch die Art der Behandlung der Nutzerinnen und Nutzer als Quasi-Objekte ihnen unbewusster Steuerung weitgehend in Frage gestellt wird. Während der Umfang der kommerziellen Interessen der Plattformbetreiber und die eigentlichen Funktionsweisen der eingesetzten Techniken und Verfahren weitgehend im Dunklen bleiben, wird das Verhalten der Nutzer für Zwecke der Unternehmen umso transparenter gemacht, detailliert analysiert, kategorisiert, zum Teil vorhersagbar und damit manipulierbar. Eine solche Entwicklung ist bedeutsam sowohl für Gemeinwohlziele wie Datenschutz als auch für die Demokratie selbst. Die Sorge um die Zukunft der Demokratie[2] im Kontext der Digitalisierung hat inzwischen den Blick geschärft für diese gesellschaftlichen Zusammenhänge und Gefährdungen, die bis dahin allenfalls in Fachkreisen andiskutiert waren. Die Frage, inwieweit die Spezifika von Internetkommunikation und Social Media Plattformen unsere politische Öffentlichkeit verändern, und inwieweit der Schutz demokratischer Strukturen und Verfahren womöglich Anpassungen bedarf, wird zumeist nicht vorrangig dem Datenschutz zur Beantwortung angetragen. Zu sehr wird die Aufgabe des Datenschutzes allein mit dem „Schutz der Einzelnen vor der Preisgabe ihrer persönlichen Daten" assoziiert. Allerdings werden Erscheinungsformen, Funktionsweisen und auch bestimmte Auswirkungen von personalisierten digitalen Diensten im Rahmen datenschutzrechtlicher Vorgaben bereits seit Jahren diskutiert und bearbeitet.

Privatheit und Datenschutz erfüllen im Digitalen, natürlich neben zahlreichen anderen Regelungsgebieten, schon heute eine Vielzahl von Funktionen. In der Digitalisierung sind Datenschutz und Privatheit dabei auch nicht nur für die Rechte Einzelner von großer Bedeutung. Schon das Bundesverfassungsgericht hatte in seinem bis heute prägenden Volkszählungsurteil zwar mit der „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen" den individualrechtlichen Charakter des Rechts auf informationelle Selbstbestimmung hervorgehoben. Es hatte andererseits aber auch die Beeinträchtigung individueller Selbstbestimmung als Beeinträchtigung des Gemeinwohls betont, "weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."[3] Und es

2 Letztlich hat vor allem der furchterregende weltweite Aufstieg rechtspopulistischer und rechtsextremer Parteien die diskutierte Fragestellung befördert.

3 BVerfGE 65, Rdnr. 146.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

zählt zu den Grundlagen des Datenschutzverständnisses, dass gerade der Schutz der Privatheit zu einer pluralistischen Gesellschaft beiträgt.[4]

Digitalisierung bedeutet heute im Verhältnis von Unternehmen zu Bürgern bzw. deren Rolle als Verbraucherinnen und Verbraucher vor allem eines, nämlich Personalisierung: die mit dem Ziel der Personalisierung geschaffenen Geschäftsmodelle, Instrumente und Praktiken zielen auf die personengenaue Erfassung, Auswertung, Ansprache und Beeinflussung/Manipulation der Bürgerinnen und Bürger. Die dabei entstehenden Risiken für die Privatheit sind, je nach Kontext und Ausgestaltung, massiv und bedrohen, zumindest bei Bekanntwerden im Rahmen von Skandalen, das Vertrauen in die Entwicklung der Digitalisierung.

In den letzten Jahren ins Blickfeld gerückt ist die umfassende Diffusion des Einsatzes von Techniken und Verfahren der Personalisierung in die gesamte Erlebniswelt der Online-Nutzerinnen und Nutzer, bei Recherche, Spielen, Kommunizieren, Mobilität und durch die Erfassung von Körperwerten. Oftmals werden sämtliche Informationen als auch Kommunikationen individuell auf die mutmaßlichen Präferenzen zugeschnitten. Nachrichtenfeeds, Kontakte als auch Suchmaschinentreffer sind zunehmend individuell vorselektiert. Einen Sonderfall bildet die politische Ansprache und Werbung über kommerzielle Plattformen auf der Grundlage der Personalisierungsmöglichkeiten.

Der vorliegende Artikel zeigt die Funktionsweisen der bekannten Verfahren und ihre datenschutzrechtlichen Implikationen auf. Das dabei entstehende Bild gibt zumindest Hinweise auf nicht weniger als signifikante Einschränkungen von Öffentlichkeiten klassischen Typs und wirft auch aus datenschutzrechtlicher Sicht Fragen nach weiteren gesetzgeberischen Anstrengungen zum Schutz demokratischer Öffentlichkeiten auf.

Der Fall Cambridge Analytica und die Debatte um den Einfluss von Facebook auf die US-Präsidentenwahl im Jahr 2016 sowie die Abstimmung im Vereinigten Königreich über den Austritt aus der Europäischen Union („Brexit") zeigen als schon oft untersuchte Beispiele die Bedeutung insbesondere algorithmengesteuerter Meinungs- und Willensbildung bei Online-Angeboten wie Suchmaschinen und sozialen Netzwerken.

4 Vgl. Albers DVBl. 2010, S. 1062.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

2. Digital unterwegs sein bedeutet personalisiert werden

a. Grundlagen

Wer digitale Technik nutzt und keine aktiven und zumeist zumindest für Durchschnittsnutzer aufwändig herzustellende Gegenmaßnahmen trifft, verliert seine Anonymität. An die Stelle der aus dem Alltag bekannten relativen Anonymität des Alltages tritt die allgegenwärtige Datenerfassung durch die Anbieter digitaler Dienste. Aus den Datenspuren und Datenteppichen der Vergangenheit wird so die Datenwolke, die sich mit jeder Handlung oder Nichthandlung verändert, durch eigenes Zutun, durch Interaktion oder durch die Ableitung der Handlung Dritter.

Aus der Perspektive des Datenschutzes rückte bei der Entwicklung der Informationstechnik zunächst die automatisierte rechnergestützte Datenverarbeitung der einzelne Personen betreffenden Informationen und Daten in den Mittelpunkt. Die Verarbeitung auch von personenbezogenen Daten in Computersystemen, die beliebig lange Speicherung, Rekombination, Bewertung, multifunktionelle Nutzung und schließlich die Übermittlung dieser Informationen zwischen verschiedenen Rechnersystemen schuf neue Risiken der Auswertbarkeit, Überwachbarkeit und, auf der Grundlage des generierten Wissens, auch der Beeinflussung/Manipulierbarkeit von Menschen. Mit der Entstehung von neuen Informations- und Kommunikationstechnologien, insbesondere des Internets als eines digitalen Netzwerks der Netzwerke, also einer Verschaltung von Rechnernetzwerken und einzelnen Rechnern wurde die eindeutige Identifizierbarkeit von Informationsaustausch und von Kommunikationshandlungen ermöglicht und auf eine neue Stufe gehoben.

Die Funktionsweise des Datenaustausches über die technisch normierten Internetprotokolle erzwingt die zumindest temporäre Zuteilung von eindeutigen Rechneradressen und den Abgleich von Informationen zumindest zur Erreichbarkeit von sendenden und empfangenden Rechnerstellen. So wird etwa mittels der IP-Adresse eine eindeutige Übermittlung von Datenpaketen innerhalb des Internet ermöglicht, mittels dieser in Servern für den Weitertransport zwingend laufend erfassten IP-Adresse aber auch die Rückverfolgbarkeit von Personen/ Beteiligten einer Kommunikation oder Handlung ermöglicht. Schon für den bloßen Aufruf einer Webseite erfolgen entsprechende Datenerfassungen entlang der gesamten digitalen Infrastruktur. Welcher Rechner, wann, wie lange auf welche Inhalte zugegriffen hat wird damit vollständig erfassbar und gespeichert. Aus diesen technischen Gegebenheiten folgt die grundsätzlich stets bestehende Identifizierbarkeit der Nutzerinnen und Nutzer. Wollen Nutzer des

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Internets ihre Identität vor Anderen, etwa wie im wirklichen Leben beim Bummel durch ein Kaufhaus, verborgen halten, müssen Sie schon selbst aktive Maßnahmen für den Erhalt ihrer Anonymität ergreifen. Denn die Default-Einstellung online ist Rückverfolgbarkeit und potentielle Identifizierbarkeit. Und neben die IP-Adresse sind längst zahlreiche andere Technologien der Identifikation von Nutzerinnen und Nutzer getreten. So gesehen stellt die Personalisierung, hier verstanden als allgemeine Erfassbarkeit und Personenbeziehbarkeit von digitalen Informationshandlungen, schon sehr früh den maßgeblichen Risikokontext des Datenschutzes dar.

Heute müssen Nutzerinnen und Nutzer für zahlreiche Dienste des Internet keine Gebühr bezahlen. Viele Unternehmen finanzieren Ihren Aufwand durch Werbung, die auf den entsprechenden Plattformen und Websites geschaltet wird oder mit dem Sammeln und Verkaufen von Informationen ihrer Nutzerinnen und Nutzer. Jeder Mensch hinterlässt beim Browsen im Internet unzählige Daten (z.B. durch Online-Einkäufe, Social Media Posts, Suchmaschinen-Eingaben, Verweildauer, Interaktion etc.) und wird zusätzlich gezielt getrackt (etwa mit der sog. Cookie-Technologie). Mit Hilfe dieser Daten können Unternehmen das Verhalten von Konsumenten analysieren, kategorisieren und vorhersehen (Grundlage ist das Profiling, darunter auch das Scoring, zunehmend unter Zuhilfenahme intelligenter Systeme) und so u.a. Werbekampagnen gezielt aussteuern (das sog. Targeting), aber auch zu entscheiden, wer für Angebote z.B. von Verträgen überhaupt in Frage kommt und wer ausgeschlossen bleibt.

Je mehr man über die Nutzerinnen und Nutzer weiß, desto (vermeintlich) genauer können Werbekampagnen adressiert werden. Die Hoffnung besteht dann in höheren Erlösen für Werbeeinblendungen als bei konventionellen Maßnahmen wie z.B. kontextbasierter Werbung. Die mitunter hohe Präzision der kommerziellen Werbekampagnen zeigt, dass dieses Targeting durchaus funktioniert und auch auf andere Einsatzbereiche angewendet werden kann. Untersuchungen legen nahe, dass auch im politischen Wahlkampf datenbasierte Werbemodelle zunehmend genutzt werden, um mit politischer Werbung den Wahlausgang aktiv zu beeinflussen.

Zur Macht der digitalen Plattformbetreiber gehören demnach eine Vielzahl technischer Verfahren vorrangig mit dem Einsatzziel, das Verhalten von Personen in statistisch relevanter Weise annähernd genau vorherzusagen, und damit für die Platzierung von Werbebotschaften und das Setzen von Kaufanreizen zu nutzen. Für die Verfahren der Online-Personalisierung können regelmäßig grob drei verschiedene Stadien im Prozess der Informationsgenerierung unterschieden werden: 1. Die Datengewinnung, 2. Die Datenanalyse und Datenbewertung, 3. Die gezielte Ansprache der Nutzer.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

b. Data Warehousing und Data Mining als Vorläufer von Big Data

Fortschreitende Digitalisierung und globale Vernetzung haben bereits seit einigen Jahrzehnten die immer weitere Erfassung von Lebensbereichen zur Folge. Wer Internetdienste, Mobiltelefone und Kundenkarten nutzte, musste schon früh die weitgehende Preisgabe vielfältiger persönlicher Daten an die beteiligten Unternehmen gewärtigen. Während Erfassung und Speicherung von anfallenden Daten für die Unternehmen immer einfacher und kostengünstiger wurden, wuchs das Interesse an der Auswertung und Verwertung der anfallenden Datenmengen. Die Kommerzialisierung der Datenverarbeitung war bereits Mitte der 90er Jahre in vollem Gange. Das Verständnis von Datenbeständen als weitgehend ungenutzt bleibendes Informationskapital der Unternehmen setzte sich langsam durch. Vor diesem Hintergrund entstanden IT-Strategien des sog. Data Warehousing und die damit verbundenen IT-Technologien, um unterschiedlichste Datenbestände von Unternehmen in einheitlichen, von den operativen Daten getrennten Datenbanken für unterschiedlichste Zwecke der Unternehmen verfügbar machen zu können.[5]Daten verschiedenster Geschäftsbereiche werden danach gesondert gebündelt, aggregiert und in einheitlichen Datenbanken gespeichert und aufbereitet, um auf diesen Datenbeständen möglichst genaue Auswertungen, etwa nach Produktionsartikeln, Kunden, Regionen oder Zeiträumen händisch oder mit unterstützenden Tools durchführen zu können. Diese gezielte Nutzung von zu anderen Zwecken erlangten Informationen und Daten zur gezielten Beobachtung und Analyse von Kundenpräferenzen und Kundenverhalten stellt die Grundlage für die Bildung von Kundenprofilen, das sog. Profiling[6] dar.

Im Mittelpunkt datenschutzrechtlicher Bewertung standen und stehen dabei Geschäftsmodelle des Customer Relationship Management, bei denen Kundendaten gezielt zur Kundenbindung einschließlich der gezielten Kundenansprache ausgewertet werden. Typischerweise können dabei auch weitere, die Kunden betreffende Daten von außen einbezogen und zur Anreicherung der Datensätze genutzt werden. Es entstehen umfangreiche Datensammlungen mit aussagekräftigen Kundenprofilen. Auch wenn dabei automatisierte Tools zur Verfügung stehen, bleibt es bei der Auswertung auf der Basis von Analysten und deren erstellten Hypothesen. Oft bilden

5 Vgl. hierzu insgesamt Scholz in : Roßnagel, Handbuch Datenschutzrecht 2000, 9.2, S. 1837.

6 Vgl. dazu die Legaldefinition in Art. 4 Abs. 4 DSGVO sowie Art. 22 DSGVO zu speziellen Anforderungen, näher dazu unten.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

die enormen Datenmengen des Data Warehousing die Grundlage für auf diese Datenmengen zum Einsatz kommende automatisierte Analyseverfahren.

Unter dem Schlagwort Data Mining etwa werden schon seit 20 Jahren diverse Methoden und Verfahren bezeichnet, mit denen eine automatisierte Analyse von großen Datenbeständen mit Hilfe von Algorithmen erfolgt. Dabei geht es um die Suche nach Mustern und Zusammenhängen in den Daten mittels Datenanalysen, zunehmend auch, um neue, bislang unbekannte Wissenszusammenhänge aufzudecken. Die Suche nach typischen Verhaltensmustern von konkreten Kunden und die automatische Erstellung von ganzen Kundenklassen nach den so auffindbaren Mustern rückte damit weiter in den Vordergrund. So können Kunden z.B. aus den Unternehmensinteressen heraus als unsichere Schuldner oder als potentiell wechselwillige Vertragsnehmer identifiziert und rechtzeitig entsprechend angesprochen/ behandelt werden. Grundlage für diese Auswertungen des Data Warehouse sind wiederum Kundenprofile, seien sie nun individualbezogen (etwa aufgrund der Einkaufshistorie) oder als nach bestimmten Merkmalen typisierte Kundenklassen, die Einzelnen zugeordnet werden.

So bedeutsam diese Entwicklung aus der Sicht der Unternehmen etwa für die Effektivierung der Kundenansprache und damit für die Erreichung ihrer geschäftlichen Ziele auch geworden ist, für den Datenschutz der Betroffenen bedeutet diese Entwicklung eine erhebliche Verschlechterung: besonders das wichtige Schutzkonzept der Zweckbindung von personenbezogenen Daten gerät unter Druck, mit dem der Dekontextualisierung von aus unterschiedlichsten Lebenszusammenhängen stammenden Informationen und Daten entgegengewirkt werden soll. Die Betroffenen werden damit für die Unternehmen umfänglicher durchleuchtbar und letztlich potentiell auch leichter manipulierbar. Es entsteht ein zunehmendes Machtungleichgewicht zwischen datensammelnden und –verarbeitenden Unternehmen auf der einen Seite sowie den Bürgerinnen und Bürgern auf der anderen Seite.

c. Konzepte des Scoring

Zu den bereits älteren Verfahren der Personalisierung zählt auch das sog. Scoring. Scores oder Kundenwerte bilden einen Unterfall des rechtlich geregelten Profiling. Mit Kreditscoring bezeichnet werden etwa mathema-

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

tisch-wissenschaftlich nachvollziehbare[7] Bewertungsmodelle[8], bei denen Bürgerinnen und Bürger nach bestimmten Merkmalen klassifiziert werden, so etwa im Hinblick auf ihre Bonität oder ihre Profitabilität für das Unternehmen. Eingesetzt werden auch hier seit langem algorithmengestützte Verfahren. Fragwürdig sind häufig die Qualität der verwendeten Datenbasis sowie die Kriterien, die sich häufig nach bloßen Ähnlichkeiten bestimmen, ohne notwendig mit der Lage der Person übereinzustimmen, wie z.B. Zugehörigkeit zu einer bestimmten Gruppe in der Bevölkerung im Hinblick auf Wohnort, Alter, Migrationshintergrund, Beruf oder Hobby. Der zu Personen ermittelte Scorewert stellt somit einen Wahrscheinlichkeitswert über ein bestimmtes zukünftiges Verhalten einer natürlichen Person dar und wird entweder inhouse oder bei einem externen Dienstleister erstellt. Das bekannteste Scoring-Verfahren ist das Kreditscoring der Auskunfteien wie der SCHUFA. Ein anderes Beispiel ist das sog. Geoscoring, also die Bestimmung von Scorewerten nach dem örtlichen Umfeld wie etwa der Zahlungsfähigkeit der Wohngegend/ Nachbarschaft unter Außerachtlassung der individuellen Situation der Betroffenen genießt ebenfalls einen schlechten Ruf, nicht zuletzt auch mit Blick auf die gesellschaftlichen Auswirkungen, wenn entsprechende Bewertungen Vorurteile gegenüber ganzen Stadtteilen erst schaffen oder vorhandene Vorurteile praktisch validieren und perpetuieren. Bekannt ist der Einsatz von Scoreverfahren den Bürgerinnen und Bürgern auch aus dem Online-Versandhandel: nur wer die erforderlichen Scorewerte erreicht, erhält die gewünschte Ware bzw. Dienstleistung per Rechnung, bekommt die Gelegenheit, über das elektronische Lastschriftverfahren zu bezahlen oder darf kostenfrei zurücksenden.[9]

Die quantitative und qualitative Zunahme von Distanzgeschäften, insbesondere per Internet, steigert die praktische Bedeutung der Verfahren für die Betroffenen. Scores bestimmen inzwischen auch seit langem, mit welcher Werbung man konfrontiert wird, ob überhaupt, und wenn ja welche Verträge mit welchen Bedingungen angeboten werden, ob eine Information bereitgestellt oder eine Zugangserlaubnis erteilt wird.[10] Das Grundproblem dieser Verhaltensbewertung auf der Grundlage von blei-

7 Zu den Anforderungen an die Wissenschaftlichkeit vgl. Ehmann in: Simitis, Kommentar zur DSGVO, 2019, Anh. 2 zu Art. 6, Rdnr. 39.

8 Bloße statistische Korrelationen werden daher nicht als Scoring eingestuft, vgl. Ehmann in: Simitis, Kommentar zur DSGVO, 2019, Anh. 2 zu Art. 6, Rdnr. 29.

9 Vgl. etwa Moos/Rothkegel ZD 2016, S. 561.

10 So Weichert, ZRP 2014, 168 mit Verweis auf eine schon damals vom BMJV in Auftrag gegebene Forschungsstudie.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

benden statistischen Verfahren liegt darin, dass relevante, das Leben zum Teil ganz erheblich beschränkende Entscheidungen über Personen getroffen werden, die primär auf der Basis eines statistischen Urteils getroffen werden, welches zumeist auch noch intransparent bleibt. Statistiken können im Einzelfall jedoch durchaus danebenliegen, bestimmte Personen oder Personengruppen ungerechtfertigt diskriminieren und ihre Marginalisierung zementieren. Zur Behebung von Machtasymmetrien im Wirtschaftsleben hat unsere Rechtsordnung aufwändige Regelungen geschaffen. Sie zielen durchweg auf Mitsprache und Stärkung der wirtschaftlich Schwächeren, um ihnen eine gerechte Teilhabe am Wirtschaftsleben zu ermöglichen. Transparenz und Beteiligungsrechte sichern dieses Menschenbild etwa der mündigen Verbraucher ab. Scoringverfahren ohne ausreichende Transparenz, Qualitätskontrolle, menschliche Aufsicht und Mitsprache der davon Betroffenen stehen tendenziell im Widerspruch zu diesen Maßstäben unserer Rechtsordnung.

d. Big Data, Algorithmen und Künstliche Intelligenz

Unter Big Data werden begrifflich Konzepte und technische Verfahren zusammengefasst, bei denen große Mengen an Daten gesammelt, verfügbar gemacht und für sog. Big Data-Analysen u.a. mit dem Ziel der Mustererkennung ausgewertet werden. Das, was heute „Big Data" genannt wird, ist nichts völlig Neues, sondern hat sich aus bestehenden Instrumenten wie eben den oben beschriebenen Data Warehousing-Praktiken weiterentwickelt.[11]Große Datenmengen fallen insbesondere bei der Nutzung des Internets und der Beobachtung von Internetaktivitäten an, bei Nutzung von Wearables, bei Vorhandensein von Sensoren oder bei altbekannten Produkten, die nun vernetzt sind, wie z.B. Fahrzeugen. Ihre Erzeugung ist inzwischen in allen Bereichen der Wirtschaft Ziel einer sog. Datenpolitik bzw. Datenökonomie und Gegenstand von zahlreichen Regulierungsanstrengungen.[12]

Big Data-Verfahren zeichnen sich u.a. durch Weiterentwicklungen bei den Faktoren Menge an Daten, Geschwindigkeit der Bereitstellung sowie der Breite der erfassbaren Datenformate aus. Das Versprechen für die Unternehmen bleibt wie bei den Vorläufern des Data Warehousing das-

11 Ebenso vgl. Weichert ZD 2013, 251.

12 So etwa beim Entwurf der EU-Kommission für einen Data-Governance-Act, ferner bei den Datenstrategien der EU sowie der Bundesregierung von 2020.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

selbe: die Entdeckung von bislang verborgenen Zusammenhängen in Datenmengen, mit deren Hilfe Geschäftsmodelle effektiviert und Innovationen ermöglicht werden sollen. Unterschieden[13] werden etwa Verfahren nicht personalisierter Musterkennung für Verhaltensmodelle (predictive analytics), Simulationen oder intelligente Stromnetze, ferner datenschutzrechtlich wesentlich problematischere Verfahren der Kumulation von Daten zur Identifikation und Selektion von Personen im Wege der Erkennung von Mustern aus einer unstrukturierten Datensammlung. Ziel dabei ist gerade, konkrete Individuen zu isolieren und zu erkennen wie z.B. bei Betrugspräventionsverfahren oder bei Formen des völlig zu Recht heftig umstrittenen Predictive Policing. Schließlich unterschieden werden Verfahren, bei denen durch laufende Kumulation, Aggregation und Auswertung vorhandener Daten bzw. unter Hinzuspeichern weiterer Daten zu einem bereits existierenden Datensatz neue, spezifischere Informationen zu einer bereits zuvor individualisierten natürlichen Person generiert werden, so etwa beim Tracking und Targeting oder etwa speziellen Versicherungstarifen wie den sog. Pay-as-you-Drive-Angeboten.[14]

Grundlage sind auch hier zunächst die zum Teil mit dem Begriff der Künstlichen Intelligenz gleichgesetzten Algorithmen. Unter einem Algorithmus kann eine eindeutige, ausführbare Folge von klar definierten Handlungsanweisungen endlicher Länge zur Lösung eines Problems verstanden werden.[15] Algorithmen können zum Zweck der Datenauswertung, Wissensgenerierung und damit Ermittlung von Entscheidungskriterien eingesetzt werden. Algorithmen, die zur Entscheidung selbst eingesetzt werden, stellen eine Weiterentwicklung dar und werden oft unspezifisch als „intelligente Systeme“ bezeichnet. Diese intelligenten Systeme sind im Wesentlichen durch drei Elemente gekennzeichnet: Sie setzen große, hochqualitative Datenmengen für ihren Erfolg voraus, sind als eigenständig lernende Algorithmen konstruiert (also nicht mehr vollständig vorab durch Menschen programmiert) und sind nach wie vor in gewissem Umfang von menschlicher Begleitung bei Entwicklung und Einsatz abhängig.[16] Sie gelten als Schlüsselressource des 21. Jahrhunderts und sollen in praktisch allen Lebensbereichen die digitale Entscheidungsautomatisierung bis hin zu autonomen Systemen (zum Beispiel selbstfahrende Autos)

13 Vgl. Schulz in Gola, DSGVO, 2018, Art. 6 Rdnr. 254.
14 Gola, a.a.O., Rdnr. 258.
15 Ernst, JZ 2017, 2019.
16 Vgl. dazu im Einzelnen Wischmeyer, AöR 2018, S. 10 ff.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

vorantreiben und damit die Wettbewerbsfähigkeit der Wirtschaft sichern helfen.

In der Praxis der Online-Welt hingegen sieht ihr Einsatz so aus: der News Feed[17] von Facebook und der den Nachrichten zugrundeliegende Algorithmus ist weitgehend intransparent.[18] Soweit bekannt, vermischt er politische und soziale News mit kommerzieller Werbung und dürfte entsprechend der kommerziellen Zielsetzungen des Unternehmens im Ganzen hochgradig personalisiert sein. Es liegt nahe, dass der Algorithmus allein oder vorrangig darauf ausgerichtet ist, Informationen einzuspielen, für welche eine Person zu bezahlen bereit sein wird und sie außerdem möglichst lange auf der Plattform zu binden. Dementsprechend wird der Algorithmus auch entscheiden, dieser Person andere, womöglich unter Vielfaltsgesichtspunkten oder Nachrichtenwert bedeutsame Informationen ggf. vorzuenthalten. Denn datenbasierte algorithmische Auswertungssysteme „erkennen" nicht wirklich, ob es sich um neutrale Inhalte (z.B. Kuchenrezept) oder um meinungsrelevante Inhalte (z.B. Tagesgeschehen, politische Äußerungen usw.) handelt und nicht, ab wann ein zunächst neutraler Inhalt meinungsrelevant wird. Das System differenziert technisch bedingt individualisiert nach zahlreichen Interessen und Informationen, die sich bei der Interaktion zwischen Nutzer, Werbetreibenden und Intermediär ermitteln lassen.[19]Eine ausgewogene Meinungsvielfalt, wie sie etwa nach der Rundfunkfreiheit des Grundgesetzes als Zielvorstellung besteht, dürfte mit zahlreichen Angeboten der bestehenden Plattformen von kommerziellen Informationsintermediären daher schon aus technischen Gründen kaum vereinbar sein. Im Gegenteil: Fast zwangsläufig „wählen" die Algorithmen die emotionale Zuspitzung aus, weil diese die Interaktionen der Nutzerinnen und Nutzer mit der Plattform und anderen erhöht.

Zutreffend ist längst erkannt, dass die nunmehr der Digitalisierung zugrundeliegenden Algorithmen und zunehmend intelligenten Systeme selbst eine Art der Regulierung darstellen, allerdings eine, der sich die Betroffenen, anders als bei der demokratisch erzeugten Regulierung durch Recht, nicht entziehen können. Die derart ausgeübte faktische Macht fordert die Demokratie heraus und erfordert Antworten zugunsten von Recht (als Freiheitsordnung), Selbstbestimmung und demokratischen Struktu-

17 Dass der Newsfeed von Facebook je nach Einspielung von eher positiven oder negativen Nachrichten die Stimmungen der Nutzerinnen und Nutzer wirkungsvoll und gezielt emotional beeinflussen kann gilt als wissenschaftlich gesichert, vgl. Böhme-Neßler, GewA 2019, S. 219 m.w.N.

18 Gillespie Fn. 6, zitiert bei Boehme-Neßler, GewA 2019, 129.

19 Schwartmann/Hermann/Mühlenbeck, MMR 2019, 498, 501.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ren. Mit einer bloßen Ethik allein der Programmierer und der von diesen in Algorithmen eingeschriebenen, häufig eher technodeterministischen Weltbilder ist es nicht getan.

Die rechtlichen Konsequenzen des Einsatzes von intelligenten Systemen bei der Personalisierung von Online-Diensten sind schon für sich betrachtet, also ohne das Zusammenspiel mit den Personalisierungsverfahren selbst, vielfältig. Ihre auf Korrelationen basierende, nicht-deterministische Funktionsweise und ihre dynamisch sich laufend ändernden Systemzustände machen sie für Laien praktisch kaum noch verstehbar bzw. intransparent und auch für herkömmliche externe Beaufsichtigung kaum zugänglich. Der aufwändige Prozess der Entwicklung und Anlernung der Systeme wirft schwierige Fragen danach auf, wie z.B. der tatsächliche Erfolg bzw. die Geeignetheit ihres Einsatzes gemessen/nachgewiesen und mögliche Diskriminierungen bestimmter Personengruppen verhindert werden können. Aus datenschutzrechtlicher Perspektive potenzieren sich damit die auch bereits beim Einsatz der deterministischen Vorläuferprogramme aufgeworfenen Fragen insbesondere der Transparenz bzw. schon der Nachvollziehbarkeit der Funktionsweise der Programme.

e. Targeting und Microtargeting

Microtargeting stellt eine besondere Form und Weiterentwicklung des gewöhnlichen Targeting dar.

Mit Targeting bezeichnet man im Marketing die zielgruppenorientierte und gezielte (Timing; Ort; Art der Darstellung etc.) Platzierung von Ansprache und Werbung, u.a. auf der Grundlage der zuvor beschriebenen Schritte der Sammlung und Analyse von Profilen. Die individuelle Ansprache mit Werbung richtet sich nach bestimmten unterschiedlichen Kriterien und Vorgehensweisen. Je nach verwendeten Kriterien unterscheidet man etwa Keyword Advertising, Geotargeting, Semantisches Targeting und etwa auch das Predictive Behavioral Targeting. Das Keyword Advertising und Semantisches Targeting kommt insbesondere bei Suchmaschinen sowie bei der Auswertung von geschriebenen Texten/aufgerufenen Webseiten zum Einsatz, die etwa beim Auftauchen eines bestimmten Begriffs in der Suchmaske dieses Keyword in einem vollautomatischen Prozess und nahezu in Echtzeit an Werbetreibende als potentielles Werbeziel melden

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

und die Schaltung der Werbung versteigern.[20] Bei Geotargeting hingegen geht es um die Schaltung regionaler, standortabhängiger Werbung in Abhängigkeit vom Vorliegen etwaiger hinreichend brauchbarer Standortinformationen. Diese können etwa über die IP-Adressen von Computern, aber inzwischen bei Mobilfunkgeräten auch über die Erfassung der Einwahldaten in TK-Netze ermittelbar werden.

Beim Predictive Behavioural Targeting werden zunächst, gewissermaßen im Kleinen, Interessengruppen durch gezielte Auswertung von soziodemografischen Angaben, Surfverhalten, Vorlieben und Abneigungen und z.B. auch Befragungen ermittelt. Diese in ihrem Verhalten und bei Vorliegen der Merkmale relativ gesichert vorhersehbaren Gruppen werden nun mit Hilfe von komplexeren algorithmischen Verfahren auf alle Nutzerinnen und Nutzer im Wege statistischer Verfahren erweitert.

In Social Media Plattformen kommen alle der bekannten Formen des Targeting nebeneinander zum Einsatz.[21] Dabei ist davon auszugehen, dass diese Plattformen vollständig geloggt und für Zwecke der Werbung und Kundenbindung ausgewertet werden d.h. praktisch jede unterscheidbare Interaktion der Nutzerinnen und Nutzer mit diesen Plattformen kann der Auswertung für personalisierte Werbung oder Bindungsmaßnahmen zugeführt werden. Wie im Fall von Facebook kann die Zusammenführung und Verknüpfung der Daten unterschiedlichster datensammelnder Dienste des Unternehmens für das Targeting eingesetzt werden.[22]

Das sog. Microtargeting stellt im Wesentlichen eine Weiterentwicklung des Behavioural Targeting auf der Grundlage von Big Data-Analysen und dem Einsatz von intelligenten Systemen dar. Genutzt werden psychometrische Verfahren, um Vorhersagen über Persönlichkeit und emotionale und motivationale Lebenslagen zu machen. Auf dieser noch feiner granulierten Basis soll Werbung gezielter ausspielbar werden. Es werden nicht nur die Inhalte, sondern auch die Art und Weise der Ansprache individualisiert. Microtargeting nutzt dazu Kundendaten und demografische Daten, um die Interessen einzelner oder kleiner Gruppen ähnlich denkender Personen zu identifizieren.[23] Der Kreis der Kunden wird dann auf der Grundlage dieser Gruppen kategorisiert. Ziel ist, das Verhalten der Nutzer auf der Grundlage des Wissens über sie in Richtung der eigenen kommerziellen

20 Vgl. zu diesem unübersichtlichen Feld statt aller Christl/Spiekermann, Networks of Control, Wien 2016 (auch online abrufbar).

21 Zur datenschutzrechtlichen Bewertung liegt eine aktuelle Stellungnahme des Europäischen Datenschutzausschusses.

22 Vgl. NZKart 2020, 473-483.

23 Vgl. TAB-Bericht Kind/Weide, Themenkurzprofil Nr. 18 Mai 2017.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Interessen und der der eigenen Werbekunden zu beeinflussen. Entscheidend ist nun, dass in der Summe der zur Anwendung kommenden Verfahren durchgehend alle angezeigten oder eben auch die überhaupt nicht auftauchenden Inhalte der technischen Kuratierung durch Algorithmen und damit auch der individualisierten Sortierung unterliegen. Im Ergebnis erleben die Nutzer der großen Plattformangebote alle ein unterschiedliches Facebook, Google usw. Im Hinblick auf die Schaltung von Werbung wird dieses Vorgehen gerechtfertigt mit dem unterstellten Wunsch auch der Nutzer, möglichst passgenaue Angebote zu erhalten.

Das politische Microtargeting im Fall des Unternehmens Cambridge Analytica wurde zunächst ermöglicht durch Bereitstellung einer App („thisisyourdigitallife"), mit der Umfragen geschaltet wurden. Über eine Programmierschnittstelle von Facebook konnten problemlos auch die Daten der Kontakte der App-Nutzer hinzugezogen und verknüpft werden. Auf diese Weise waren die Daten von mehr als 50 Millionen Menschen weltweit erfasst und für Zwecke politischer Wahlwerbung verfügbar.[24] Zu den Kennzeichen dieser psychometrisch unterstützten Ausspielung politischer Werbung zählt, dass sie in bislang nicht erreichter Datendichte arbeitet. Facebook etwa bietet Anzeigenkunden –und damit auch politischen Parteienwährend des Wahlkampfs – die Möglichkeit den Kreis der Empfänger mittels psychografischer Eigenschaften zu bestimmen und anhand von Geschlecht, Alter, Aufenthaltsort, besuchten Webseiten, politischer Einstellung und anderen Datenpunkten die Zielgruppe einer Anzeige zu bestimmen.[25] Für die Öffentlichkeit werden diese Kampagnen praktisch nicht sichtbar, denn sie sind nur für den bestellten Zeitraum und nur für den ausgewählten Empfängerkreis sichtbar. So erlaubt dieses Instrument Parteien potentiell nicht nur, zeitgleich widersprüchliche politische Aussagen je nach Zielgruppe zu treffen oder Kampagnen gezielt auf die Hinderung bestimmter Gruppen an der Teilnahme an Wahlen auszurichten. Es verhindert insbesondere, dass der Rest der demokratischen Öffentlichkeit von den Aussagen Kenntnis nehmen, diese auf den Wahrheitsgehalt der Aussagen hin zu prüfen und sie bei der eigenen Willensbildung auf die eine oder andere Weise zu berücksichtigen vermag.[26]

---

24 Zum Fall insgesamt Wolfie Christl, in APuZ 24-26/2019, https://www.bpb.de/apuz/292335/datenoekonomie.

25 Sehr detailliert beschrieben und erläutert bei Christl, APUZ 24/26, 2019, abrufbar unter https://www.bpb.de/apuz/292349/microtargeting-persoenliche-daten-als-politische-waehrung.

26 Schemmel, Der Staat 2018, 501–527.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Während es zutrifft, dass womöglich auch mit Hilfe des Microtargeting sich wieder mehr Bürgerinnen und Bürger für Politik und Demokratie interessieren und die nach Art. 21 Grundgesetz geschützten politischen Parteien auch mit diesem Instrument ihrem Auftrag womöglich besonders effektiv nachgehen könnten, liegen die Risiken für die Meinungsbildung als auch für die demokratische Kultur insgesamt auf der Hand: der Einsatz von politischem Microtargeting erlaubt zumindest bei bestimmten Vorgehensweisen nicht weniger als die gezielte Manipulationen der öffentlichen Meinung (nicht nur bei anstehenden Wahlen), ohne dass dieses von den nicht adressierten Teilen der Öffentlichkeit wahrgenommen werden können. Dass selbst einige Plattformen die Auswirkungen zunehmend mit einer gewissen Angst wahrzunehmen scheinen, zeigt sich in den Versuchen, mehr Transparenz in die geschalteten Anzeigenkampagnen zu schaffen, in dem es Übersichtsseiten für eine Überprüfung geben soll.

3. Folgerungen für Öffentlichkeit und Demokratie

a. Beitrag zur Fragmentierung der Öffentlichkeit

Auch das Phänomen der Öffentlichkeit und dessen Verbindung mit den Funktionsweisen von Demokratie ist wesentlich medial bedingt. Anders gesagt: Entwicklungen bei Informations- und Kommunikationstechniken fungieren als Medienfaktoren und können den Wandel von Legitimations- bzw. Demokratieprozessen befeuern.[27]

Das Gesamtbild des Einsatzes von Personalisierungstechniken bei bekannten digitalen Angeboten gerade im Bereich Social Media belegt eine schon heute hohe Dichte von mit modernster Technik individualisierten Oberflächen und Funktionen. Die zum Einsatz kommenden Verfahren und Technologien erzeugen eine digitale Erfahrung, die mit der Erfahrung von anderen Nutzern derselben Plattform kaum vergleichbar, jedenfalls praktisch kaum jemals identisch sein dürfte. Die damit einhergehende Individualisierung der online erlebten Wirklichkeit vermag so, spätestens mit der sich abzeichnenden weiteren Zunahme[28] der Nutzung digitaler Medienöffentlichkeiten, wohl auch gesamtgesellschaftliche Wirkungen er-

27 Ingold, Der Staat 56 (2017), 491–533.

28 Bislang nutzt die deutliche Mehrheit der bundesdeutschen Bevölkerung noch die etablierten Kanäle von Funk, Fernsehen und Druckpresse zur Information und Meinungsbildung.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

zeugen, etwa zu einer weiteren Fragmentierung[29] von Öffentlichkeit als Bühne und zentralem Element der Meinungsbildung beizutragen. Die medienwissenschaftliche Wirkungsforschung gilt dazu bis heute allerdings als noch zu wenig aussagekräftig.[30] Die mit Medien wie Facebook oder etwa auch Twitter geschaffenen, besonderen Formen von selektiven Teil-Öffentlichkeiten sind von vornherein und jeweils individuell vorgefiltert und bestätigen eher die kritische Vermutung der Entstehung von sog. Filterblasen,[31] in denen gleichförmige Aussagen und Gleichgesinnte überwiegen und die Konfrontation mit der Lebenswirklichkeit und der tatsächlich bestehenden Vielfalt von Auffassungen, aber auch mit hochwertigen und gesicherten Inhalten stark herabgesetzt sein kann. Die Konfrontation sowie die inhaltliche Auseinandersetzung mit anderen Meinungen, aber auch die Gewöhnung an den Umgang etwa mit wissenschaftlich belegten bzw. objektivierten, qualitätsgesicherten Inhalten kann dann vermindert sein.

Es ist bezeichnend, dass das Bundesverfassungsgericht kürzlich in einer Entscheidung zum öffentlich-rechtlichen Rundfunk (unter Bezugnahme auf die Arbeiten des Deutschen Bundestages in der Enquete Internet und Digitale Gesellschaft) hervorgehoben hat, dass die Gefahr hinzukomme, „dass – auch mit Hilfe von Algorithmen – Inhalte gezielt auf Interessen und Neigungen der Nutzerinnen und Nutzer zugeschnitten werden, was wiederum zur Verstärkung gleichgerichteter Meinungen führt. Solche Angebote sind nicht auf Meinungsvielfalt gerichtet, sondern werden durch einseitige Interessen oder die wirtschaftliche Rationalität eines Geschäftsmodells bestimmt, nämlich die Verweildauer der Nutzer auf den Seiten möglichst zu maximieren und dadurch den Werbewert der Plattform für die Kunden zu erhöhen. Insoweit sind auch Ergebnisse in Suchmaschinen vorgefiltert und teils werbefinanziert, teils von „Klickzahlen" abhängig."[32]

---

29 Vgl. dazu Spiecker gen. Döhmann, Kontexte der Demokratie: Parteien – Medien – Sozialstrukturen, VVDStRL 77 (2018); Schemmel, a.a.O.; kritisch differenzierend mit Blick auf den Begriff der Öffentlichkeit Ingold, Der Staat, 2017, S. 509.

30 So etwa Ingold, a.a.O.; Neuere Hinweise bei EU Kommission, COM(2021) 262 final.

31 Zu dem von Eli Pariser geprägten Begriff der Filter Bubble als einer Art kommunikativer Komfortzone vgl. bestätigend Hoffmann-Riem, AöR 2017, S. 13, der auch gesamtgesellschaftliche Wirkungen wie die Fragmentierungsthese für möglich hält. Zur Diskussion insgesamt vgl. auch Lischka/ Stöcker, Digitale Öffentlichkeit, Bertelsmann-Stiftung 2017; ferner die Nachweise unter Fn. 21.

32 Vgl. BVerfG, Beschluss des Ersten Senats vom 20. Juli 2021 - 1 BvR 2756/20 -, Rn. 1-119.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Der These von der auf diese Weise einfachen Manipulierbarkeit politischer Meinungen könnte zwar entgegengehalten werden, dass es derartige Filterblasen doch schon immer (etwa in Gestalt der selektiv präsentierten Inhalte einer Tageszeitung) gegeben habe und doch die Verbreitung etwa von politischer Werbung über digitale Plattformen insoweit ein Wahlkampfinstrument wie jedes andere darstelle. Doch dies verkennt, neben den bereits genannten Möglichkeiten gezielter missbräuchlicher Nutzung, schon die mangelnde Vergleichbarkeit qua hybrider Aufmachung und interaktiver Form der Kommunikation als Grundlage. Soziale Netzwerke kommen öffentlich nicht als Werbeunternehmen daher, die sie ihrem Unternehmensziel nach sind. Das Bewusstsein der Nutzerinnen und Nutzer über die auch bei Funktionen wie Newsfeeds durchweg nach kommerziellen Interessen präsentierte und „ge-nudgte" Realität dürfte weithin nach wie vor zu gering sein.

Der Vollständigkeit halber sei hier gesagt, dass auch andere Auswirkungen des Micro-Targeting verheerend sein können, so z.B. Verwirrungsstrategien gegenüber entstehenden sozialen Bewegungen durch Fake-Profile mit gezielten Ansprachen. Die Fragmentierungsgefahr, die von mancher Seite bestritten wird, steht also keineswegs allein, sondern ist nur die am meisten untersuchte bzw. diskutierte potenzielle Auswirkung.

b. Addiction by Design – Engführung von Aufmerksamkeit auch per Oberflächengestaltung

Datenverarbeitungstechnik wirkt sich stets auf die Datenbasis und die gewinnbaren Informationen aus. Und ihr Einsatz und ihre Anwendungen wirken auf soziale Zusammenhänge zurück und prägen letztendlich, als sog. soziotechnisches System, auch soziale Systeme und deren Abläufe. In datenschutzrechtlicher Hinsicht bestimmen vor allem diese sozialen Auswirkungen die rechtliche Bewertung, nicht die Technik selbst.

In komplexen soziotechnischen Systemen hilft damit der alleinige Blick auf die eingesetzten Technologien nicht weiter. Auch das weitere Setting des Technikeinsatzes muss betrachtet werden. Eigentlich bieten im Onlinebereich gerade die Mensch-Maschine-Schnittstelle der Angebotsoberflächen und die damit bestehenden Interaktionsmöglichkeiten reichlich Platz für Reflexion, Selbstbestimmung und Demokratie stärkende Elemente. Konkret angelegt sind solche Elemente etwa in den gesetzlichen datenschutzrechtlichen Regelungen für mehr Transparenz und die Absicherung der Zustimmung der Nutzerinnen und Nutzer. Dagegen stehen freilich die auf Automatisierung und eher Unhinterfragbarkeit angelegten

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Geschäftsmodelle. Gerungen wird seitens der Unternehmen deshalb mit Gesetzgeber und Aufsichtsbehörden gerade bei diesen Fragen um jeden Millimeter dieser Oberfläche. Ein gutes Beispiel dafür bieten die endlosen Debatten und rechtlichen Entscheidungen zu Opt-In/ Opt out bei Cookie-Bannern im Internet, zur Ausgestaltung von online abrufbaren AGB, der Anzahl der zu setzenden Häkchen der User usw.[33]

In der Realität bleiben Social-Media-Umgebungen auf weitgehend automatisierte Abläufe und Entscheidungsentlastung angelegt. Dieses im Design angelegte, gezielte Unterlaufen bewusster Reflexion scheint durchweg in Abläufe und Funktionen eingebaut, worauf etwa die wachsende auch datenschutzrechtliche Debatte um Designelemente digitaler Oberflächen wie die sog. dark patterns und auch das sog. Nudging, also das gezielte kommerzielle Ausnutzen von angeborenem bzw. erlernten menschlichen Verhaltensmuster wie Heuristiken und Biases hinweisen.[34] Dazu zählt z.B. auch die gezielt auf Abhängigkeiten (Addiction by Design) setzende Steuerung der Newsfeeds mit laufend neuen emotionalen Inhalten, um die Aufenthalts- und Nutzungszeit der Nutzer gezielt auszudehnen. Als Grundeinstellung sind viele Feeds auf automatische Einspielung des nächsten Beitrags als eines endlosen Streams ausgerichtet. Die Sorge um den Menschen als „Digital Unconscious", also als Objekt unbewusster Steuerung, erhält damit auf gleich mehreren Ebenen Nahrung. Das Postulat individueller Autonomie aus Artikel 2 Abs. 1 Grundgesetz droht faktisch durch technisch fundierte, als solche nicht oder eben nur schwer erkennbare Fremdsteuerungen unterlaufen zu werden.[35]

4. Antworten des Datenschutzes und Grenzen

Für die meisten der hier im Einzelnen und beispielhaft vorgestellten Techniken und Verfahren gibt es im Datenschutzrecht bereits relativ etablierte rechtliche Maßstäbe und es gilt die Datenschutzgrundverordnung. Die Frage nach den Auswirkungen der digitalen Personalisierung insbesondere

33 Vgl. EuGH, Urteil v. 1. Oktober 2019 – C-673/17 und auch BGH, Urteil v. 28. Mai 2020 – I ZR 7/16.

34 Aus der juristischen Literatur etwa Weinzierl, NVwZ 2020,1087. Instruktiv dazu sind die Untersuchungen von VZBV und Stiftung Neue Verantwortung, vgl. https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste/dark-patterns-so-wollen-websites-und-apps-sie-manipulieren-58082 mit weiteren Nachweisen.

35 Hoffmann-Riem, AöR 2017, S. 6.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

bei den genannten Plattformen als sogenannte „Informationsintermediäre" für Öffentlichkeit und Demokratie berührt auch den Datenschutz, kann aber sicher mit diesem allein angesichts der überindividuell angelegten Problematik der Wahrung von Meinungsvielfalt nicht beantwortet werden.

Auf die Grenzen der Bearbeitbarkeit der mit Big Data und intelligenten Systemen einhergehenden strukturellen Machfragen durch ein vorrangig auf den Schutz individueller Persönlichkeitsrechte ausgerichtetes Datenschutzrecht wird denn auch durch eine Reihe von Autoren zutreffend hingewiesen.[36]

Das Grundrecht auf Datenschutz nach Art. 8 der Grundrechtecharta (und Art. 16 AEUV) statuiert das Recht jeder Person auf den Schutz der sie betreffenden personenbezogenen Daten. Datenschutz soll nicht etwa die Daten schützen, sondern gegen Gefährdungen durch die automatisierte Datenverarbeitung. Im Mittelpunkt steht, wie schon unter der alleinigen Geltung des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 Grundgesetz, der Schutz der Persönlichkeit und auch der Erhalt des Würdeschutzes. Der Datenschutz dient insoweit dem Schutz der Bürgerinnen und Bürger vor der Herabwürdigung zu einem bloßen Objekt der Entscheidung, Ausspähung oder auch der Manipulation. Er zielt auf Transparenz und die Mitbestimmung und Beteiligung der von Datenverarbeitung Betroffenen. Die Bausteine seines Schutzprogramms werden bei den genannten Verfahren und Datenverarbeitungen der Personalisierung auf Plattformen der Informationsintermediäre in unterschiedlichem Umfang relevant.

Nach dem grundgesetzlichen Datenschutzkonzept findet auch die Demokratie als Schutzgut insoweit regelmäßig mit Erwähnung, weil das Bundesverfassungsgericht die Demokratie als auf der selbstbestimmten Entfaltung seiner Bürgerinnen und Bürger basierend versteht: Ohne selbstbestimmten Informationsaustausch ist jede Verwirklichung von Grundrechten durch Kommunikation gefährdet.[37] Zugleich ist informationelle Selbstbestimmung die Grundlage einer demokratischen Kommunikationsverfassung. Denn Selbstbestimmung ist „eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens.[38] Auch individuel-

36 Hoffmann-Riem, a.a.O., S. 7; ferner Wischmeyer a.a.O., S. 31.

37 Roßnagel, ZD 2013, S. 562, mit umfänglichen Erwägungen zu den konzeptionellen Herausforderungen von Big Data.

38 BVerfGE 1, 43.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

le Entwicklung und Entfaltung kann nur gelingen, wenn grundlegende Schutzmuster des Datenschutzes die Betroffenen und damit auch die Demokratie selbst wirkungsvoll zu schützen vermögen.

Angesicht dieses eher weiten Schutzkonzepts des Datenschutzes mit einer Vielzahl von Schutzgütern erscheint es nicht ausgeschlossen, dass mögliche Auswirkungen der Personalisierung auf die Demokratie und die Wechselwirkungen zwischen technisch enggeführten digitalen Öffentlichkeiten einerseits und den zu schützenden individuellen Entwicklungsmöglichkeiten der Bürgerinnen und Bürger andererseits schon de lege lata unter gewissen Umständen datenschutzaufsichtsbehördliche Berücksichtigung finden. Denn Umfang und Tiefe der Personalisierung sowie die weitgehende Intransparenz der Datenverarbeitung ermöglichen tiefgreifende Beeinflussungs-/Manipulationsmöglichkeiten auch im Hinblick auf öffentliche Diskurse und damit demokratische Verfahren, die auf die informationelle Selbstbestimmung zurückwirken. Je mehr valide Hinweise auf demokratie- als auch persönlichkeitsrelevante manipulative Vorgehensweisen wie Desinformation, Aufstachelung zum Hass und gezielte gesellschaftliche Spaltung bis hin zu politischem Microtargeting demokratiegefährdender Prägung bekannt werden, desto eher können solche Praktiken einschränkende Entscheidungen gerechtfertigt sein.

Der Datenschutz befasst sich wie bereits gezeigt seit langem mit Social Media, Big Data und KI. Im Mittelpunkt stand und steht dabei die mögliche Beeinträchtigung der Persönlichkeitsrechte der Bürgerinnen und Bürger durch die mit diesen Geschäftsmodellen und Verarbeitungspraktiken verbundenen Methoden und Verfahren. Im Rahmen einer aufsichtsbehördlichen Prüfung wird deren Einsatz je gesondert auf Zulässigkeit geprüft und bewertet.

Die DSGVO als rechtlicher Rahmen

Nach der Datenschutzgrundverordnung (DSGVO) bedarf es für die von Webplattformen eingesetzten Verfahren der Personalisierung einer eindeutigen Rechtsgrundlage nach Artikel 6 DSGVO. In der Regel bleibt den Unternehmen angesichts der hier in Rede stehenden weitgehenden Datenverarbeitung nichts anderes als die Einwilligung nach Art. 6 Abs. 1 a. samt der Anforderungen für die Einwilligung nach Art. 7 DSGVO. Was zunächst als eine die Selbstbestimmung der Nutzerinnen und Nutzer bestmöglich berücksichtigende Lösung und als Königsweg einer freiheitlichen Gesellschaft angesehen wurde, hat sich in der Praxis gerade der großen On-

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

line-Plattformen allerdings längst in sein Gegenteil verkehrt.[39] Die Einwilligungslösung nach der DSGVO bietet den Informationsintermediären Raum für weitreichende Alles-oder-Nichts-Vertragslösungen. In der Kombination mit umfänglichen AGB und zumeist vage formuliert, nutzen die zu ihren Gunsten laufende völlige Asymmetrie der Informationsverteilung und die Überforderung der Nutzerinnen und Nutzer für ihre Zwecke aus und erhalten Einwilligungen als vermeintlichen Freibrief mindestens für den impliziten Einsatz aller genannten Personalisierungsverfahren. Die datenschutzrechtlichen Prinzipien der Zweckbindung und Datenminimierung laufen weitgehend leer, wenn und weil auf Grundlage der so eingeholten Einwilligung die Daten bei Einbindung in Big-Data-Analysen laufend und für höchst unterschiedliche Zwecke eingesetzt werden.

Auf diese fragwürdige datenschutzrechtlich vielfältig angreifbare Praxis der Webunternehmen haben auch die Datenschutzaufsichtsbehörden bislang leider noch keine durchgreifende Antwort finden können. Das hat, neben weiteren Gründen[40], mit praktischen Mängeln des europäischen Abstimmungsverfahrens der Aufsichtsbehörden zu tun. Denn die Mehrzahl der großen Plattformunternehmen haben ihre europäischen Hauptniederlassung in nur wenigen EU-Mitgliedsstaaten wie Irland und unterliegen nach dem sog. One-Stop-Shop-Verfahren zunächst der alleinigen Aufsicht der bisher äußerst langsam agierenden dortigen Behörde.[41]

Weitere Aspekte der Datenschutzgrundverordnung betreffen die Regelung des Profiling in Art. 4 Nr. 4 DSGVO und die automatisierte Entscheidung im Einzelfall nach § 22 DSGVO.

Profiling nach Art. 4 Nr. 4 ist jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Deutlich wird, dass die Definition die weiteren hier getroffenen Unterscheidungen nach technischen Verfahren wie Tracking, Scoring oder Tar-

---

39 Vgl. statt vieler: Hoffmann-Riem, a.a.O., S. 23.

40 Dazu zählen etwa die Unbestimmtheit und zum Teil zu enge Fassung potentiell einschlägiger Bestimmungen der DSGVO dar, siehe nachfolgend.

41 Und das Kooperations- und Kohärenzverfahren zur Klärung von Streitigkeiten über die mehrere Aufsichtsbehörden erlaubt es bislang nicht hinlänglich, insoweit gegen das Nichthandeln einzelner Aufsichtsbehörden wirksam vorzugehen, vgl. Weber/Dehnhardt ZD 2021, S. 63.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

geting nicht kennt, sondern allein nach dem Ziel der Verarbeitung einordnet. Die weit gehaltene Definition und Einordnung bleibt im Hinblick auf das grundsätzliche Verbot der ausschließlich automatisierten Verarbeitung (einschließlich Profiling) in Artikel 22 DSGVO folgenlos, denn für die Rechtfertigung gelten wie bereits erläutert die allgemeinen Zulässigkeitsbestimmungen des Artikel 6 DSGVO, womit pauschal der Weg zur Einwilligung eröffnet bleibt.

Es ist besonders misslich, dass der europäische Gesetzgeber sich im Hinblick auf die Personalisierungsverfahren auf keine differenzierenden und den Datenschutz der Betroffenen in den Mittelpunkt stellenden Regelungen einigen konnte. Hier muss dringend nachgebessert werden.[42]

In ihrem nicht verfügenden Teil gibt die DS-GVO ferner vor, Betroffenen „aussagekräftige Informationen über die involvierte Logik" mitzugeben (Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g, Art. 15 Abs. 1 lit. h) sowie „geeignete mathematische oder statistische Verfahren für das Profiling" sowie Korrekturmechanismen zu verwenden, um die Risiken für die Persönlichkeit sowie Diskriminierungsgefahren zu minimieren (ErwGr 71 UAbs. 2 S. 1). Umfang und Inhalt dieser Bestimmungen sind umstritten, böten allerdings durchaus ebenfalls Möglichkeiten, etwa mit Blick auf den Einsatz intelligenter Systeme und deren derzeitig ungelöstes Transparenz- bzw. Nachvollziehbarkeitsproblem grundlegendere Fragen an die Plattformbetreiber zu stellen.

Insgesamt sollte deutlich geworden sein, dass auch der jetzige, wenn bereits in Teilen reformbedürftige datenschutzrechtliche Rahmen durchaus Anknüpfungspunkte für das Einschreiten von Aufsichtsbehörden gegen aktuelle Praktiken bei den Personalisierungsverfahren der Plattformen bietet. Dabei handelt es sich allerdings um zeitlich wie inhaltlich aufwändige Verfahren, die schlussendlich auch nicht primär das gewünschte Ziel der Sicherstellung von Meinungsvielfalt auf Plattformen als zunehmend relevante Teilöffentlichkeiten der Demokratie verfolgen, sondern am Schutz der Datenschutzrechte der betroffenen Nutzerinnen und Nutzer ausgerichtet sind.

---

42 Vgl. die Forderungen der Datenschutzbehörden aus Anlass der ersten Evaluation der DSGVO im Erfahrungsbericht der Datenschutzkonferenz vom 6.11.2019, abrufbar unter https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/20191113_Erfahrungsbericht_DS-GVO.pdf.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

5. Elemente der rechtspolitischen Debatte

a. EU-Vorschläge zur Regulierung des digitalen Sektors

Das Thema der Auswirkungen der Digitalisierung auf die Demokratie, etwa wie hier in Gestalt der Fragmentierung durch Personalisierung, führt direkt in die zentrale und strittige Debatte um Plattform- und Algorithmenregulierung. Die Digitalisierung der Medien und insbesondere die Netz- und Plattformökonomie des Internet einschließlich der sozialen Netzwerke begünstigen Konzentrations- und Monopolisierungstendenzen bei Anbietern, Verbreitern und Vermittlern von Inhalten. So ist schon deshalb klar, dass weit über das Datenschutzrecht hinaus Bereiche wie etwa das Wettbewerbs- und Kartellrecht betroffen sind.

Der digitale Wandel fordert die Diskussion über Umfang und Inhalt des Datenschutzes und erforderliche Weiterentwicklungen auf vielen Feldern heraus. Über den weiteren Umgang mit den auch in diesem Kontext maßgeblichen, die Verfahren und Technologien prägenden und steuernden Algorithmen bei Online-Plattformen scheint zumindest in Brüssel derzeit die Grundentscheidung getroffen. Mit der Vorlage des weltweit ersten Gesetzentwurfs zur KI-Regulierung, dem sog. Artificial Intelligence Act[43], hat die EU-Kommission ihren Anspruch unterstrichen, wertegeleitete Regulierung auch bei dieser als wirtschaftlich besonders schützenswerten Innovation in Anschlag zu bringen. Im Hinblick auf den Einsatz von intelligenten Systemen für die hier gegenständlichen Personalisierungsverfahren erscheint es durchaus sachgerecht, im Rahmen dieses Gesetzgebungsverfahrens rote Linien etwa für die Zulässigkeit des Microtargeting für Werbezwecke zu ziehen.

Mehr Regulierung soll ferner sowohl europäische Datensouveränität als auch den Schutz der Persönlichkeitsrechte und die Datenschutzrechte der Bürgerinnen und Bürger stärken und die Markt- und Meinungsmacht der bestehenden großen Plattformen einhegen.[44] Zutreffend wird die Verantwortung und auch Schutzpflicht für einen effektiven Schutz der Grund-

---

43 Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES ZUR FESTLEGUNG HARMONISIERTER VORSCHRIFTEN FÜR KÜNSTLICHE INTELLIGENZ (GESETZ ÜBER KÜNSTLICHE INTELLIGENZ) UND ZUR ÄNDERUNG BESTIMMTER RECHTSAKTE DER UNION, COM(2021) 206 final.

44 Vgl. etwa die EU-Datenagenda und die inzwischen vorliegenden Gesetzentwürfe der EU-Kommission insbesondere zum sog. Digital Markets Act sowie zum Digital Services Act.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

rechte und die Umsetzbarkeit bestehender gesetzlicher Schutzprogramme beim Staat verortet. Im Detail enthalten diese Gesetzentwürfe allerdings allesamt deutliche Schwächen und auch Regelungslücken. Was von den Plänen letztlich im politischen Prozess umsetzbar sein wird bleibt abzuwarten.

Von Datenschutzbehörden[45] bereits gefordert und unterstützungswürdig erscheint die Initiative von einer Reihe Abgeordneten aus dem Europäischen Parlament zum Digital Services Act für eine erhebliche Beschränkung und letztlich das Ende des feingranulierten Online-Microtargeting, wie es gerade von den großen Plattformunternehmen praktiziert wird.[46]

Von grundlegender Bedeutung ist auch der im Entwurf für den Digital Services Act vorgesehene Datenzugang gerade für Behörden, aber auch für Forscher in Art. 31 DSA-E. Er könnte, datenschutzrechtlich sauber geregelt, tatsächlich dabei unterstützen, die Phänomene von Hassrede und Falschnachrichten einschließlich der etwaigen Beschleunigung durch die Systemfunktionalitäten der großen Plattformen besser zu verstehen, Wirkungsweisen zu validieren und auf dieser Basis sachgerechte Problemlösungen zu entwickeln[47]. In diese Richtung geht auch die Bestimmung des § 5a des Netzwerkdurchsetzungsgesetzes (NetzDG), der Forschungsinstitutionen Zugang zu den Nutzungsdaten der Intermediäre einräumt, um die Wirkungsweise des Einsatzes von Algorithmen zu untersuchen und besser zu verstehen.

b. Privacy-by-Design als weiterhin möglicher Ausweg

Die umfassende Personalisierung der Nutzererfahrung und die damit ermöglichte Ausspähung und Manipulation im Online-Bereich mag einen Ausblick darauf geben, was erst mit den erwartbaren Angeboten des Internet of Things (IoT)[48] und dem sog. Ubiquitous Computing auf der

45 Vgl .Stellungnahme 1/2021 zum Data Services Act des Europäischen Datenschutzbeauftragten, abrufbar unter https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf.

46 Tracking-Free-Ads-Coalition, vgl. etws den Bericht unter https://www.heise.de/news/Targeting-EU-Abgeordnete-fordern-Aus-fuer-spionierende-Werbung-5041368.html. Die Forderung der entsprechende Initiative hat bislang nicht Eingang in die Position des federführenden EU-Ausschusses gefunden.

47 Vgl. dazu sowie zu DMA und DSA insgesamt etwa Gielen/Uphues EuZW 21, 627.

48 Vgl. aktuell zu Entwicklungen des IoT Kreye, SZ vom 2.10.2021.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Grundlage allgegenwärtiger Sensorik des Alltages insgesamt auf unsere Gesellschaften zukommt.

Statt angesichts der weitreichenden Folgen der Personalisierungen nun das Recht, den Datenschutz oder auch die Demokratie gleich ganz neu zu erfinden, mag es angesichts der bedeutenden Veränderungen der Online-Kommunikationen, die ja nur Vorboten sehr viel weiter gehender Veränderungen aller unser Lebensbereiche sind, darauf ankommen, erst einmal das bestehende Recht innovativ weiter zu entwickeln. Hierzu liegen inzwischen eine Fülle von Vorschlägen vor, die auch die Regulierung der hier gegenständlichen Personalisierung der Angebote von Informationsintermediären bzw. großen Informations- und Kommunikationsplattformen zumindest in ihren Teilaspekten angehen. Die größte Aufmerksamkeit erfährt dabei die Regulierung der Künstlichen Intelligenz.

An erster Stelle wird im Datenschutz seit langem die Kooperation von Technik und Recht genannt, konzeptionell im Datenschutz bekannt als Privacy-By-Design.[49] Erst mit einem eingebauten Datenschutz ab Werk (auch als sog. Privacy-By-Default) würde es dem Datenschutz gelingen, gewissermaßen vor die Lage zu kommen und bereits im Entwicklungsprozess Berücksichtigung bei Unternehmen und Programmierern zu finden, die noch auf absehbare Zeit die Hoheit über den Entstehungsprozess behalten werden. Dazu müsste die Anwendung dieses weiterhin wichtigen Konzeptes, auch wenn es jahrelang lediglich als wenig schlagkräftiges Soft Law behandelt wurde, allerdings auch verpflichtend auf die Hersteller von IT-Systemen erstreckt werden.

Im Rahmen der Debatte um Künstliche Intelligenz wird dies als Eingriff in die Algorithmenentwicklung diskutiert, um bestimmte rechtliche Zielsetzungen zu gewährleisten. In dieselbe Richtung gehen Vorschläge, KI selbst für die Durchsetzung von rechtlichen Zielen einzusetzen, eine wachsende Debatte in vielen Bereichen. So wird im Verbraucherschutzrecht die Idee personalisierter Verbraucherinformationen diskutiert.[50]

---

49 Geregelt in der DSGVO in Art. 25 Abs. 1. Als technische und organisatorische Maßnahmen, die proaktiv einzurichten und aktiv zu betreiben sind, gelten insbesondere Datenminimierung, Pseudonymisierung, Schnittstellen zur Transparenz für Information, Intervention und Audit, sowie die Überwachung durch Verantwortliche. Eine Grundlage zur Planung von „Privacy by Design" ist die Datenschutz-Folgenabschätzung mit einer zugehörigen Risiko-Analyse für die Privatheit der Anwender des Systems in Art. 35 DS-GVO.

50 Vgl. zur noch jungen Debatte die Gutachten unter https://www.svr-verbraucherfragen.de/2021/09/21/personalisierte-verbraucherinformation-ein-werkstattbericht/.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Schließlich hat die EU-Kommission in ihrem Democracy Action Plan[51] weitere Maßnahmen zum Erhalt der Medienfreiheit und des Pluralismus angekündigt und dabei konkret unter dem Gesichtspunkt der Gefahr von Desinformation angekündigt, etwa das Problem der politischen Werbung regulierend aufgreifen zu wollen.[52]

6. *Das Gutachten der Datenethikkommission*

Das Gutachten der Datenthikkommission (DEK)[53] hat die Wahrung und Förderung von Demokratie und gesellschaftlichem Zusammenhalt als einen der Leitgedanken ihrer umfänglichen Studie zur Digitalisierung formuliert. Hervorgehoben werden Digitale Technologien als systemrelevant für die Entfaltung der Demokratie. Sie ermöglichen neue Formen der politischen Beteiligung, können aber auch Gefahren im Hinblick auf Manipulation und Radikalisierung mit sich bringen. Die DEK empfiehlt Maßnahmen gegen ethisch nichtvertretbare Datennutzungen, darunter auch gegen die Integrität der Persönlichkeit verletzende Profilbildung, gezielte Ausnutzung von Vulnerabilitäten, sog. Addictive Designs und Dark Patterns, und dem Demokratieprinzip zuwiderlaufende Beeinflussung politischer Wahlen.[54]

Mit Blick auf Künstliche Intelligenz und die besonderen Gefahren von Medienintermediären mit Torwächterfunktion für die Demokratie empfiehlt die DEK der Bundesregierung umfängliche ex-ante-Verfahren der Zulassung zu prüfen. Der EU-Gesetzgeber hat diese Vorschläge in seinem bisherigen Vorschlag allenfalls unzureichend aufgegriffen und setzt eher auf eine Selbstregulierung der Anbieter. Die DEK empfiehlt allerdings auch, die Anbieter in diesem engen Bereich zum Einsatz solcher algorithmischer Systeme zu verpflichten, die den Nutzern zumindest als zusätzliches Angebot auch einen Zugriff auf eine tendenzfreie, ausgewogene und die plurale Meinungsvielfalt abbildende Zusammenstellung von Beiträgen

51 Aktionsplan für die Demokratie, vgl. https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_de.

52 Vgl. dazu die aktuelle Mitteilung der EU-Kommission COM(2021) 262 final, abrufbar unter.

53 Gutachten von 2018, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6.

54 Vgl. S. 18.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

und Informationen verschaffen.[55] Eine entsprechende Pflicht zur Statuierung von Neutralitätsgeboten und Vielfaltsvorgaben erscheint der DEK etwa auch mit Blick auf den Schutz Minderjähriger vor Beeinflussung durch und über soziale Netzwerke geboten.[56]

7. Ausblick

Eine generelle Zurückdrängung personalisierter Angebote in digitalen Angeboten erscheint mit Blick auf die langjährige Praxis und Akzeptanz durch Nutzerinnen und Nutzer weder erreichbar noch sonderlich sinnvoll. Schließlich werden Funktionen der auf persönliche Präferenzen setzenden Unterstützung angesichts der wachsenden Auswahl an Informationen immer relevanter. Gleichwohl gilt es, auch mit deutlichen, schon auf die Erhebung von Daten beschränkenden Vorgaben dort zu reagieren, wo Demokratie und persönliche Selbstentfaltung gravierend beeinträchtigt werden.

Im Einklang mit dem Europäischen Datenschutzbeauftragten fordert auch der BfDI deshalb langfristig ein Verbot von gezielter Online-Werbung, die auf durchdringenden Formen des Tracking basiert sowie eine Einschränkung sensibler Datenkategorien, die für solche Werbemethoden verarbeitet werden können. Mit der wirkungsvollen Beschränkung von zumindest einzelnen Elementen der Personalisierung kann der Datenschutz, wenn auch mittelbar, einen Beitrag auch zum Erhalt pluraler Meinungsvielfalt und demokratischen Strukturen leisten. Darüber hinausgehende Anstrengungen insbesondere des europäischen Gesetzgebers sind erforderlich, um dem Menschenbild der europäischen Grundrechtecharta als auch dem Grundgesetz entsprechend Demokratie und Selbstbestimmung auch in der beschleunigten Digitalisierung zu gewährleiten.

55 Vgl. S. 30.
56 Vgl. S. 230.

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

https://doi.org/10.5771/9783748932741-149 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY