Die Digitalisierung – Feind oder Freund der Demokratie

Staatlicher Schutz des Meinungsbildungsprozesses in sozialen Netzwerken gegen potentielle Beeinträchtigungen durch Meinungsroboter

Alexander Iben

Seit der US-Präsidentschaftswahl 2016 stehen soziale Netzwerke wegen politisch motivierter Manipulationen der Willensbildung im Fokus. Neben *Cambridge Analytica* sorgten vor allem sog. *Social Bots* für weltweite Aufmerksamkeit. So sollen zusammenagierende, automatisch gesteuerte Fake-Accounts in sozialen Netzwerken politische Propaganda zugunsten der Kandidaten betrieben haben. Damit stieg auch in Deutschland die Angst vor einer Manipulation, weshalb immer wieder eine Regulierung des neuen Phänomens gefordert wurde.[1] Ob diese Forderung berechtigt ist, hängt von den konkreten Auswirkungen der Meinungsroboter auf die sozialen Netzwerke und die Willensbildung der Nutzer ab (I.). Wegen der demokratischen Bedeutung, kann sogar die Frage nach einer staatlichen Handlungspflicht gestellt werden (II.).

I. Grundlagen – Die Beeinflussung des Meinungsbildungsprozesses durch Meinungsroboter innerhalb sozialer Netzwerke

1. Meinungsroboter in sozialen Netzwerken

Soziale Netzwerke basieren auf Verbindungen zwischen den Nutzern (Abonnement, Freundschaftsanfrage o.ä.) und den darauf basierenden Interaktionen. Auf der Startseite wird jedem Nutzer eine Übersicht von Beiträgen aus seinem persönlichen Netzwerk angezeigt (sog. Feed). Die Beiträge werden von einem Ranking-Algorithmus nach verschiedenen Kriterien ausgesucht und in Abhängigkeit von der ermittelten Relevanz angezeigt.[2] Auf die Beiträge kann man reagieren, sie mit seinem Netzwerk teilen oder kommentieren. Dadurch kommen auch andere Nutzer mit Inhal-

1 So etwa BR-Drs. 519/18 oder BT-Drs. 18/1856, S. 2.

2 Vgl. hierzu etwa *Drexl*, Bedrohung der Meinungsvielfalt durch Algorithmen, ZUM 2017, 529 (532f.) zum (überholten) Algorithmus von Facebook.

ten in Kontakt, zu denen sie ansonsten keinen Bezug hätten. Über eine Suchmaske kann man aber auch nach bestimmten Signalwörtern, Personen, Seiten oder Beiträgen suchen. Besonders prägnant sind sog. Hashtags, die zur Kennzeichnung bestimmter Themen genutzt werden.

Social Bots sind letztlich normale Nutzerkonten, die eine menschliche Identität suggerieren. Ihre Aktionen werden (halb-)automatisiert durch ein Programm gesteuert. Die Programmierschnittstellen (sog. API) der Netzwerke ermöglichen dabei den externen Zugriff auf die Netzwerke. Je nach Aufwand und Geschick des Urhebers können die Bots simple Interaktionen, wie das Hinzufügen von Nutzern zum Netzwerk, bis hin zu komplizierten Aufgaben, etwa das Reagieren auf bestimmte Signalwörter oder Kommentare, übernehmen. Vor dem Hintergrund des zunehmenden technischen Fortschritts sind hier – jedenfalls theoretisch – keine Grenzen gesetzt.[3] Weil (gute) Bots sich nach außen als normale Nutzer gerieren, sind sie für andere Nutzer nur schwer als solche identifizierbar.[4] Dadurch können sie letztlich unbemerkt Propaganda betreiben und Einfluss auf den Meinungsbildungsprozess innerhalb der Netzwerke nehmen, was letztlich zu ihrer Bezeichnung als Meinungsroboter führt.[5]

2. *Meinungsbildung und der Einfluss von Meinungsrobotern*

Meinungsbildung vollzieht sich auf drei unterschiedlichen Ebenen, gesellschaftlich (Makro-), individuell (Mikro-) und innerhalb bzw. durch Teil-Gruppen (Mesoebene), die sich wechselseitig beeinflussen. Betrachtet man die Mikroebene, um die es hier primär gehen soll, so hängt die Willensbildung von den eigenen Erfahrungen und dem eigenen Wissen aber auch von der Wahrnehmung der Umwelt und der vorhandenen Informationen ab.[6] Dabei kommt vor allem Medien eine zentrale Funktion zu. Zunehmend werden die herkömmlichen Print- und Rundfunkmedien durch so-

3 Etwaige Beispiele liefern bspw. *Thieltges/Hegelich*, Manipulation in sozialen Netzwerken – Risikopotenziale und Risikoeinschätzungen, ZfP 64 (2017), 493 (495ff.).

4 *Ferrara u.a.*, The Rise of Social Bots, Communications of the ACM 59 (2016), 96; *Kind u.a.*, Büro für Technikfolgenabschätzung, Social-Bots, Horizon-Scanning Nr. 3, April 2017, S. 4.

5 In diese Richtung auch *Haeg*, The Ethics of Political Bots, Journal of Practical Ethics Vol. 5 (2017), 85 (86); *Pfaffenberg/Adrian/Heinrich*, in: Holtz-Bacha (Hrsg.), (Massen-)Medien im Wahlkampf, 97 (98).

6 Vgl. *Schoen*, Kognitionspsychologische Einblicke in die black box politischer Meinungsbildung, Politische Vierteljahresschrift 47 (2006), 89 (92).

ziale Netzwerke und ihre personalisierten Feeds abgelöst, was auch an einem Vertrauensverlust in herkömmliche Medien liegt; der Ausdruck Lügenpresse ist dafür symptomatisch.[7]

Innerhalb der Netzwerke wird besonders der Einfluss der sozialen (Teil-)Gemeinschaft relevant: Sowohl bei der Informationsaufnahme als auch bei der Verarbeitung und Meinungsbildung kommen heuristische Denkweisen zum Einsatz.[8] Bei komplexen Themen versuchen wir auf logische Schlüsse zurückzugreifen, um uns mit wenig Aufwand eine erste klare Meinung zu bilden. Nach dem *Prinzip der sozialen Bewährtheit*[9] orientiert man sich hierbei an anderen: Wenn eine Mehrheit von Personen eine bestimmte Haltung zu einem bestimmten Thema hat, so ist die Wahrscheinlichkeit groß, dass auch der Einzelne diese Haltung annimmt. In sozialen Netzwerken ist dieses Prinzip in der Struktur verankert. Die Anzahl der Follower, Abos und Likes lassen solche Heuristiken ohne Weiteres zu und dienen als schnelle Entscheidungshilfen, etwa bei der Bewertung der Qualität eines Beitrags.[10] Auch der Ranking-Algorithmus der Netzwerke macht sich letztlich diese statistischen Daten zu Eigen.[11] Daneben kommt aber auch der sog. *Isolationsfurcht* und der dadurch bedingten Selbstzensur Bedeutung zu. Um von der sozialen Gemeinschaft nicht isoliert zu werden, tendiert man dazu, seine von der (situativen) Mehrheit abweichende Meinung nicht kundzugeben (Theorie der Schweigespirale)[12]. Diese zensierenden Effekte können in sozialen Netzwerken durchaus stärker sein als in der realen Welt.[13]

---

7 Vgl. hierzu *Schweiger*, Der (des)informierte Bürger im Netz, 2017, S. 105f.

8 Vgl. *Schweiger* (Fn. 7), S. 74ff.; *Weber/Knorr*, in: Appel (Hrsg.), Die Psychologie des Postfaktischen, 103 (110); *Schoen* (Fn. 6), S. 92.

9 Hierzu im Zusammenhang mit Meinungsrobotern *Klaas*, in: Möller (Hrsg.), Was tun gegen Fake News und Hate Speech?, 2019, 47 (52); *Graber/Lindemann*, in: Sachs-Hombach/Zywietz (Hrsg.), Fake News Hashtags & Social Bots, 2018, 51 (59ff.); *Pfaffenberger/Adrian/Heinrich*, in: Holtz-Bacha (Fn. 5), (Massen-) Medien, 97 (99).

10 *Klaas* (Fn. 9), S. 52; *Graber/Lindemann*, (Fn. 9), S. 59ff. Vgl. auch *Kaerlein*, in: Haug/Pallaver (Hrsg.), Talk with the Bots, 2018, 17 (23ff.).

11 Vgl. *Drexl* (Fn. 2), S. 532. Das gilt insbesondere dann, wenn Nutzertrends ausgewertet werden sollen oder eine Anordnung in Abhängigkeit von der Relevanz für andere Nutzer mit einem ähnlichen Nutzungsprofil vorgenommen wird.

12 Zurückgehend auf *Noelle-Neumann*, Die Schweigespirale, 1991.

13 So etwa *Neubaum/Krämer*, What do we fear? Expected sanctions for expressing Minority Opinions in offline and online Communication, Communication Research 45 (2018), 139 (157f.); *Hampton u.a.*, Social Media and the ‚Spiral of Silence', 2014, S. 3.

Unter Zugrundelegung dieser grob skizzierten Einflüsse lassen sich drei wesentliche Strategien der Meinungsroboter ausmachen: die Manipulation von statistischen Daten (Likes, Kommentare usw.), die Informationsdiffusion und die Veränderung des Meinungsklimas.[14] Indem massenhaft geliked, abonniert oder Inhalte veröffentlicht werden, wird sowohl den Nutzern als auch den Algorithmen ein Trend suggeriert und die Popularität bestimmter Inhalte erhöht,[15] wodurch sich auch die relevanten Parameter für heuristische Annahmen verändern. Zugleich wird dies auch für die Informationsdiffusion relevant:[16] Werden so Trends erschaffen, erkennen dies die Algorithmen und zeigen entsprechende Inhalte priorisiert im Feed an.[17] Reagiert ein Nutzer dann auf die Beiträge, so verbreiten sie sich innerhalb der Netzwerke seiner Abonnenten. Ein solches „Schneeballsystem" entsteht oftmals, wenn es um Fake News geht.[18] Und letztlich lässt sich so auch das Meinungsklima verändern, indem die zensierenden Effekte der Schweigespirale genutzt werden.[19] Denken Nutzer, sie vertreten die Mindermeinung, äußern sie sich womöglich nicht, wodurch sich Diskussionen stören, unterbinden oder umkehren lassen.[20] Meinungsroboter

14 Einordnung nach *Woolley*, Social bot interference in global politics., in: First Monday, abrufbar unter http://firstmonday.org/article/view/6161/5300, (Stand 14.02.2020). Instruktiv zum gesamten Thema *Thieltges/Hegelich* (Fn. 3), S. 493ff.

15 *Brings-Wiesen*, Meinungskampf mit allen Mitteln und ohne Regeln? – Eine Replik auf Jens Milkers „'Bot-Armeen' als Meinungsmacher im Wahlkampf", juwiss-Blog v. 30.11.2016, bezeichnet dies als „quantitative Legitimität". Vgl. hierzu auch *Thieltges/Hegelich* (Fn. 3), S. 497; *Mehrens*, in: Steinbrecher/Rager, Wenn Maschinen Meinung machen, 2018, 20 (25); *Müller/Denner*, Was tun gegen „Fake News"? – Eine Analyse anhand der Entstehungsbedingungen und Wirkweisen gezielter Falschmeldungen im Internet, 2017, S. 9; *Grimme u.a.*, Social Bots: Human-Like by Means of Human Control?, Big Data Vol. 5 (2017), 279 (281). Zur Beeinflussung des Ranking-Algorithmus etwa *Lazer u.a.*, The science of Fake News, Science Vol. 359 (2018), 1094 (1095).

16 Im Zusammenhang mit Fake News etwa *Boberg/Schatto-Eckrodt/Frischlich*, Welt und Frieden 2018, 44ff.; *Lazer u.a.* (Fn. 15), S. 1095. Zur Diffusion von Informationen siehe auch *Lou/Flammini/Menzer*, Information Pollution by Social Bots, 2019 (arXiv:1907.06130 [cs.CY]).

17 *Lazer u.a.* (Fn. 15), S.1095.

18 Vgl. *Mafi-Gudarzi*, Desinformation: Herausforderung für die wehrhafte Demokratie, ZRP 2019, 65. Ausführlich zur Verbreitung von Fake News *Vosoughi u.a.*, The spread of true and false news online, Science 359 (2018), 1146ff. Zu Grundlagen der Diffusion *Thieltges/Hegelich* (Fn. 3), S. 504ff.

19 *Frischlich/Boberg/Quandt*, in: Kaspar/Gräßer/Riffi (Hrsg.), Online Hate Speech, 71 (74); *Ross et al.*, European Journal of Information Systems Vol. 28 (2019), 394ff.

20 Siehe hierzu etwa *Stieglitz u.a.*, A Categorisation of Social Media Bot Accounts, 2017 oder *Thieltges/Hegelich* (Fn. 3), S. 498.

können also Einfluss auf die Informationsvermittlung, die Meinungsäußerung und auf die Meinungsbildung anderer Nutzer insgesamt haben.[21]

II. Staatliche (Schutz-)Verantwortung vor den neuen Risiken der Meinungsroboter

Freilich sehen die Nutzungsbedingungen der Netzwerke entsprechende Verbote derartiger „Manipulationen" vor. In der Vergangenheit wurden diese aber – wenn überhaupt – nur dann durchgesetzt, wenn entsprechender öffentlicher Druck aufkam. Insoweit stellt sich gerade die Frage nach einer staatlichen Verantwortung. Für den klassischen Rundfunk wurde diese wie selbstverständlich bejaht[22]. Im hiesigen Kontext soll es aber eher um die Frage einer staatlichen Schutzpflicht gehen: Weil die Grundrechte Private nur mittelbar binden,[23] die Grundrechte aber in erheblichem Umfang durch diese gefährdet werden können, ist man sich (mittlerweile)[24] einig, dass der Staat die grundrechtlichen Rechtsgüter auch vor nicht-staatlicher Gefährdung zu schützen hat.[25] Die hieraus resultierende Verantwor-

---

21 Vgl. *Frischlich/Boberg/Quandt*, in: Kaspar/Gräßer/Riffi (Fn. 19), S. 74.

22 St. Rspr. seit BVerfGE 12, 205 (260ff.) – *1. Rundfunkentscheidung*. Der Ansatz des BVerfG ist aber – zu Recht – nicht unkritisiert geblieben, ausführlicher zur Kritik etwa *Grabenwater*, in: Maunz/Dürig, GG, Art. 5 Abs. 1 Rn. 536f. m.w.N.

23 St. Rspr. des BVerfG seit BVerfGE 7, 196 (204ff.) – *Lüth*.

24 Zur anfänglichen Kritik siehe etwa das SV von den Richtern *Rupp-v. Brünneck* und *Simon*, BVerfGE 39, 1 (73ff.) – *Schwangerschaftsabbruch I*. Zur Kritik insgesamt vgl. *Isensee*, in: ders./Kirchhof, Handbuch des Staatsrecht Band IX, § 191 Rn. 165 ff. oder *Calliess*, in: Merten/Papier, Handbuch Grundrechte Band II, § 44 Rn. 8 mit entsprechenden weiteren Verweisen.

25 Siehe nur *Borowski*, Grundrechte als Prinzipien, S. 369f.; *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, S. 34 ff.; *Gerbig*, Grundrecht auf staatlichen Schutz, S. 33ff., 83; *Moritz*, Staatliche Schutzpflichten gegenüber pflegebedürftigen Menschen, S. 96; *Canaris*, Grundrechte und Privatrecht, AcP 184 (1984), 201 (225f.); *Böckenförde*, Grundrechte als Grundsatznormen, Der Staat 29 (1990), 1 (12); *Neubert*, Grundrechtliche Schutzpflicht des Staates gegen grundrechtsbeeinträchtigende Maßnahmen fremder Staaten am Beispiel der Überwachung durch ausländische Geheimdienste, AöR 140 (2015), 267 (270f.) m.w.N. Aus der Judikatur ohne Anspruch auf Vollständigkeit: zu Art. 2 Abs. 1 (Privatautonomie) BVerfGE 81, 242 (254f.) – *Handelsvertreter*; zum allg. Persönlichkeitsrecht BVerfGE 96, 56 (64) – *Vaterschaftsauskunft*; zur informationellen Selbstbestimmung BVerfG (K) MMR 2007, 93; zu Art. 4 GG BVerfG (K), NVwZ 2001, 908; BVerfGE 125, 39 (78ff.) – *Adventssonntage Berlin*; zu Art. 12 Abs. 1 BVerfGE 92, 26 (46) – *Zweitregister*; zu Art. 14 GG BVerfGE 114, 73 (90) – *Lebensversicherungen mit Überschussbeteiligung*.

tung richtet sich primär an den Gesetzgeber, der einen effektiven Schutz durch die Rechtsordnung zu gewährleisten hat.[26] Im Vergleich zum Abwehrrecht kann die Schutzpflicht auf keine genaue Dogmatik aufbauen, allein die (grobe) Differenzierung zwischen Tatbestand und Rechtsfolge hat sich etabliert.[27] Im ersten Fall geht es zunächst um die Frage, ob Schutzpflichten in einem Fall *abstrakt* bestehen, und im zweiten Fall um die Frage, was aus ihnen *konkret* folgt.[28]

1. Bestehen staatliche Schutzpflichten beim Einsatz von Meinungsrobotern?

Schutzpflichten wurden auch im Schrifttum bereits in dem hiesigen Kontext aufgegriffen.[29] Eine umfangreichere Aufbereitung des Problems sucht man aber vergebens. Interessant hierbei ist, dass häufig bloß darauf hingewiesen wird, dass Schutzpflichten zugunsten der Meinungsfreiheit dort eingreifen würden, wo diese ernsthaft bedroht sei,[30] ohne dass für diese Grenze überzeugende Argumente vorgetragen werden. Unklar ist allerdings, ob bereits das Bestehen der Schutzpflichten abgelehnt wird oder ob

---

26 *Dolderer*, Objektive Grundrechtsgehalte, S. 199; *Stern*, in: ders., Staatsrecht III/1, S. 951. *Krings*, Grund und Grenzen staatlicher Schutzpflichten, S. 243ff.

27 Siehe etwa *Isensee*, HbStR IX (Fn. 24), § 191 Rn. 217; *Calliess*, Die grundrechtliche Schutzpflicht im mehrpoligen Verfassungsverhältnis, JZ 2006, 320 (327).

28 Vgl. zu dieser Differenzierung zwischen abstrakt und konkret BVerfGE 142, 313 (337ff.) – *Zwangsbehandlung*.

29 So etwa bei *Milker*, „Social Bots" im Meinungskampf, ZUM 2017, 216 (220f.); *ders.*, InTeR 2017, 199 (202f.); *Löber/Roßnagel*, Kennzeichnung von Social Bots – Transparenzpflichten zum Schutz integrer Kommunikation, MMR 2019, 493 (496). Nur oberflächlich *Klaas*, Demokratieprinzip im Spannungsfeld mit künstlicher Intelligenz – Demokratische Entscheidungsfindung durch und mithilfe von selbstlernenden Algorithmen, MMR 2019, 84 (89); *Libertus*, Rechtliche Aspekte des Einsatzes von Social Bots de lege lata und de lege ferenda, ZUM 2018, 20 (22). *Dankert/Dreyer*, Social Bots – Grenzenloser Einfluss auf den Meinungsbildungsprozess?, K&R 2017, 73 (75) beschäftigen sich mit dem Ausgestaltungsauftrag hinsichtlich des Rundfunks.

30 Allgemein zur Meinungsfreiheit *Grabenwater*, in: Maunz/Dürig, GG, Art. 5 Abs. 1 Rn. 109. Zu Meinungsrobotern etwa *Löber/Roßnagel* (Fn. 29), ebd.; *Libertus* (Fn. 29), ebd.; *Semizoglu*, in: Hetmank/Rechenberg (Hrsg.), Kommunikation, Kreation und Innovation, 2019, 79 (95); Teilweise wird dies etwa dahingehend spezifiziert, dass konkrete Schutzpflichten dort bestehen, wo ein Diskussionskanal vollständig lahmgelegt wird, *Semizoglu*, ebd., S. 95; *Milker* (Fn. 29), S. 220; *Liesem*, in: Litschka/Krainer, Der Mensch im Digitalen Zeitalter, 183 (194). Lediglich *Brings-Wiesen* meint, dass Schutzpflichten schon jetzt einen zumindest vorsichtig regulierenden Eingriff erforderten, *Brings-Wiesen* (Fn. 15).

damit eine Einschränkung auf Rechtsfolgenseite gemeint ist.[31] Und generell lässt sich fragen, warum in einem so sensiblen grundrechtlichen Bereich mit der „ernsthaften Bedrohung" vergleichsweise restriktive Anforderungen gestellt werden. Mit Blick auf die Rundfunkfreiheit ist das BVerfG immerhin deutlich rigider und betont die Notwendigkeit präventiver Maßnahmen.[32] Jedenfalls besteht Anlass, näher über eine staatliche Schutzpflicht nachzudenken.

2. Nicht-staatlicher Übergriff auf grundrechtliche Schutzgüter

Zunächst setzt der Tatbestand eine eingriffsäquivalente Lage, einen nicht staatlichen Übergriff auf das grundrechtliche Schutzgut voraus.[33] Ein potentieller nicht-staatlicher Übergriff kommt hier vor allem hinsichtlich der Informations- und Meinungsäußerungsfreiheit des Art. 5 Abs. 1 S. 1 GG in Betracht.[34] Und weil der gesamte Kommunikationsvorgang Grundlage der Wahlentscheidung ist, wird auch die Freiheit der Wahl (Art. 28 Abs. 1 S. 2, 3. Var, Art. 38 Abs. 1 S. 1, 3. Var. GG) – zumindest verstärkend – relevant.[35] Die Informationsfreiheit ist dort tangiert, wo Bots Einfluss auf die Darstellung von Inhalten in den Netzwerken haben, etwa durch die Beeinflussung der Ranking-Algorithmen oder über die Informationsdiffusion. Aber auch dort, wo Diskussionen gestört und unliebsame Meinungen unterdrückt werden, kann ein Informationsverlust für potentielle Rezipienten die Folge sein. Letzteres tangiert wegen der selbstzensierenden Effekte

---

31 Wenn von *konkreten* Schutzpflichten gesprochen wird, deutet dies eher auf eine Beschränkung der Rechtsfolgenseite, vgl. hierzu BVerfGE 142, 313 (337ff.) – *Zwangsbehandlung*.

32 Siehe etwa BVerfGE 121, 30 (52) – *Parteibeteiligung an Rundfunkunternehmen*, m.w.N., auch wenn es sich dabei um den rundfunkrechtlichen Regelungsauftrag handelt.

33 Vgl. *Calliess* (Fn. 27), S. 326; *Isensee*, HbStR IX (Fn. 24), § 191 Rn. 225.

34 Ob wegen der kollektiven Sphäre der Diskussionen in sozialen Netzwerken, auch noch ein besonderer Schutz durch Art. 8 Abs. 1 GG eingreift, soll hier unbeachtet bleiben. Ausführlicher zu dieser Frage und i.E. bejahend *Möhlen*, Das Recht auf Versammlungsfreiheit im Internet - Anwendbarkeit eines klassischen Menschenrechts auf neue digitale Kommunikations- und Protestformen, MMR 2013, 221ff. Ablehnend hingegen *Depenheuer*, in: Maunz/Dürig, GG, Art. 8 Rn. 45. Siehe hierzu auch in diesem Band *Rike Sinder*, 223 ff.

35 Zum Zusammenhang zwischen Meinungsfreiheit und Freiheit der Wahl siehe etwa BVerfGE 20, 56 (97ff.) – *Parteibeteiligung an Rundfunkunternehmen*; 44, 125 (139) – *Öffentlichkeitsarbeit*.

auch die Meinungsäußerungsfreiheit anderer Nutzer. Dabei handelt es sich nicht um bloß innere Effekte, weil die Wirkung gerade künstlich herbeigeführt wird, also keine Begleiterscheinung „normaler" menschlicher Kommunikation ist. Und mit der Störung wird den bisherigen Teilnehmern die Wirkkraft ihrer Äußerungen genommen und damit die kommunikative Chancengleichheit berührt.[36] Ein die Schutzpflicht grundsätzlich auslösendes Drittverhalten läge somit also vor.

3. Überschreiten einer Gefahrenschwelle?

Unklar ist aber, ob dieses Verhalten eine bestimmte Qualitätsschwelle erreichen muss. Bestehen also generell Schutzpflichten und der Grad der Bedrohung wird allein auf Rechtsfolgenseite relevant,[37] oder ist dieser schon für den Anwendungsbereich maßgeblich?[38] Übereinstimmend werden aber Schutzpflichten jedenfalls dann angenommen, wenn eine Gefahr in entsprechender Anwendung der polizeirechtlichen Maßstäbe besteht. Entscheidend hierfür ist die Produktformel aus Schadensfolgen und Eintritts-

---

36 Kommunikative Chancengleichheit setzt die chancengleiche Teilhabe am Kommunikationsprozess voraus, siehe hierzu BVerfGE 44, 125 (142) – *Öffentlichkeitsarbeit*; *Hartl*, Suchmaschinen, Algorithmen und Meinungsmacht, 2017, S. 32 . Unterschiede die *kommunikativ* begründet sind, etwa aus der Überzeugungskraft des Äußernden resultieren, sind hierbei indes unproblematisch. Das gilt etwa für die stärkere Stellung von Medienunternehmen oder Influencern gegenüber Einzelpersonen. Dort wo die Mächtigkeit nicht mehr kommunikativ sondern technisch oder wirtschaftlich begründet ist, ergeben sich aber Probleme mit der kommunikativen Chancengleichheit, etwa dann wenn sie wirtschaftlich (hierzu insbesondere BVerfGE 25, 256 [258ff.]– *Blinkfüer*) oder technisch bedingt sind, (vgl. hierzu *Bortnykov*, Verbot des Access-Tierings: Ausfluss kommunikativer Chancengleichheit oder unzulässige "Gleichmacherei"?, K&R 2015, 703 [704]). Aber auch hier geht es gerade darum, die Rezeptionschancen auf technischem und nicht auf sachlich-kommunikativem Wege zu erhöhen.

37 In diese Richtung neben *Dietlein* (Fn. 25), S. 112, auch *Moritz* (Fn. 25), S. 112. Tendenziell auch *Szczekalla*, Grundrechtliche Schutzpflichten im deutschen und europäischen Recht, S. 303f.

38 So etwa mit der Parallele zum Gefahrenbegriff *Neubert* (Fn. 25), S. 272; *Isensee*, HbStR IX (Fn. 24), § 191 Rn. 235; *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 236; *Murswiek*, Die staatliche Verantwortung für die Risiken der Technik, S. 140ff.; *Epping*, Grundrechte, 2019, Rn. 124; *Schmidt am Busch*, in: Kollmer/Klindt/Schucht, Arbeitsschutzgesetz, A. Rn. 29; *Gärditz*, in: Landmann/Rohmer, UmweltR, GG Art. 20a Rn. 86; *Krings* (Fn. 26), S. 231.

wahrscheinlichkeit.[39] Dabei gilt: Je gravierender die potentiellen Folgen und je bedeutender das Rechtsgut, desto geringere Anforderungen sind an die Eintrittswahrscheinlichkeit zu stellen.[40]

Vorliegend wird gerade diese Qualitätsschwelle relevant: Anders als bei der Erzeugung von Kernenergie,[41] kann eine Gefahr bei Meinungsrobotern nicht ohne weiteres angenommen werden. Zwar haben verschiedene Studien entsprechende Phänomene in unterschiedlichen Ländern nachweisen können.[42] Hierzulande hielt sich der Umfang aber in Grenzen[43] und abseits theoretischer Befunde[44] ist in der Praxis ein Einflusspotential noch nicht nachgewiesen worden. Prima vista haben wir es hier also vor allem mit einem *Risiko*, der Vorstufe der Gefahr, zu tun. Allerdings bedeutet das nicht, dass Schutzpflichten bereits deshalb nicht bestehen. Wegen der flexiblen Produktformel kann schon ein reines Risiko eine Gefahr darstellen, wenn etwa die Anforderungen an die Wahrscheinlichkeit herab zu setzen sind.[45]

---

39 So etwa *Krings* (Fn. 26), S. 231. Deutlich ausführlicher zu dieser Produktformel *Murswiek* (Fn. 38) S. 165ff.

40 *Krings* (Fn. 26), S. 231; siehe auch *Di Fabio*, in: Maunz/Dürig, GG, Art. 2 Abs. 2 Rn. 90f. Das BVerfG betont dies bei Beeinträchtigungen des Lebensrechts, siehe hierzu nur BVerfG, NVwZ 2010, 702 Rn. 12 – *CERN*.

41 Vgl. BVerfGE 49, 89 (121f.) – *Kalkar I*; 53, 50 (57f.) – *Mühlheim-Kärlich*.

42 Siehe etwa zu Venezuela *Forelle u.a.*, Political Bots and the Manipulation of Public Opinion in Venezuela, 2017 (arXiv:1507.07109 [cs.SI]); zu Japan *Schäfer/Evert/Heinrich*, Japan's 2014 General Election: Political Bots, Right-Wing Internet Activism and Prime Minister Shinzo Abe's Hidden Nationalist Agenda, Big Data Vol. 5 (2017), S. 294ff.; zu den USA *Howard u.a.*, Journal of Information Technology&Politics Vol. 15, S. 81ff.; zu Deutschland in Ansätzen *Institut for Strategic Dialogue*, Make Germany Great Again, S. 18 f.; zu Mexiko *Suárez-Serrato*, in: SocInfo, Proceedings of the 8th International Conference, 269ff. und *Treré*, Trípodos, Número 39 (2016), 35 (39ff.); zum Iran *Thieltges u.a.*, Effects of Social Bots in the Iran-Debate on Twitter, 2018 (arXiv:1805.10105 [cs.SI]); zu Brasilien vgl. *Department of public policy analysis*, Bots and Brazil's Electoral legal system, Policy Paper 3, 2019. Weitere Nachweise bei *Woolley* (Fn. 14).

43 Hierzu *Pfaffenberger/Adrian/Heinrich*, in: Holtz-Bacha (Fn. 5), S. 99; *Grimme u.a.*, PropStop Bericht Bundestagswahl 2017, abrufbar unter: http://www.propstop.de/wp-content/uploads/2017/09/bundestagswahl-2017-social-media.pdf, (Stand 08.04.2020); *Medina Serrano u.a.*, Social Media Report: The 2017 German Federal Elections, 2018, S. 21ff.

44 Zur Meinungsklimaveränderung siehe *Ross et al.* (Fn. 19), 394 ff.; zum Einfluss und zur Weiterleitung der Informationen siehe *Freitas u.a.*, Social Network Analysis and Mining Vol. 6 (2016), Iss. 23; *Lou/Flammini/Menzer* (Fn. 16).

45 Das zeigt insbesondere die Judikatur zum Lebensrecht. So hat das BVerfG, NVwZ 2010, 702 Rn. 12 – *CERN*, bereits „theoretisch herleitbare Risiken" ausreichen lassen, um Schutzpflichten anzunehmen.

M.E. muss auch vorliegend die Gefahrenschwelle bereits als überschritten gelten. Maßgeblich hierfür sind mehrerer Argumente: Zwar ist hier nicht das Lebensgrundrecht betroffen. Gleichwohl geht es mit den Rechtsgütern des Art. 5 Abs. 1 S. 1 GG einerseits um die Entfaltung des Individuums in der politisch-sozialen Sphäre, also um seine „politisch-gesellschaftliche Existenz" und andererseits um die zentrale Voraussetzung für die Demokratie.[46] Dies verdeutlicht auch die Freiheit der Wahl, für die ein offener und pluraler Kommunikationsprozess elementar ist.[47] Wegen dieser grundlegenden Bedeutung sind entsprechende Risiken deutlich gewichtiger zu bewerten, als bei anderen Grundrechten.[48] Hinzu kommt, dass der Eintritt potentieller Schäden mehr als nur theoretisch herleitbar ist: Die Bots nutzen die Nutzeroberfläche ideal aus, verhalten sich wie mustergültige Nutzer,[49] wodurch die Grundlage eines Einflusses geschaffen ist.[50] Dass sie konkrete Auswirkungen auf die Meinungsäußerungsfreiheit haben können, indem wichtige Diskussionen angegriffen, gestört oder verzerrt werden, zeigen Beispiele aus dem Iran[51] und aus Mexiko[52], wo die Trending Hashtags auf Twitter in einem anderen Kontext verwendet wurden, um so die Aufmerksamkeit vom eigentlichen Diskussionsthema abzulenken. Im mexikanischen Fall war das auch vergleichsweise erfolgreich.[53] Je nachdem wie zentral die Diskussion ist, kann dies im Einzelfall stärkere Bedeutung haben.[54] Und auch das Meinungsklima lässt sich beeinflus-

46 Zu diesem Zusammenspiel siehe schon BVerfGE 5, 85 (204) – *KPD-Verbot*; 7, 196 (208) – *Lüth*.

47 Siehe hierzu schon BVerfGE 20, 56 (98) – *Parteifinanzierung I*; 44, 125 (139) – *Öffentlichkeitsarbeit*.

48 In diese Richtung auch *Semizoglu* (Fn. 30), S. 95.

49 *Kaerlein* (Fn. 10), S. 24.

50 Vgl. *Kaerlein* (Fn. 10), S. 24; *Thieltges/Hegelich* (Fn. 3), S. 504.

51 *Abokhodair/Yoo/McDonald*, in: Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing, S. 839ff.

52 *Suárez-Serrato u.a.* (Fn. 42).

53 Dort führte die Intervention immerhin dazu, dass die Diskussionen unter den entsprechenden Hashtags eingestellt und verlagert worden sind. Dabei nahm die Anzahl der Tweets sukzessive ab, was allerdings auch an dem zeitlichen Abstand liegen mag, hierzu näher *Suárez-Serrato u.a.* (Fn. 42).

54 Wegen der dezentralen Kommunikationsstruktur lässt sich nämlich nicht *der* „Diskussionskanal" ausmachen, der vollständig lahmgelegt wird (in diese Richtung allerdings u.a. *Milker* (Fn. 29), S. 220; *Semizoglu* (Fn. 30), S. 95. Denn themenbezogene Diskussionen findet man an verschiedenen Stellen. Vielmehr sind die besonderen Umstände der Diskussion für die Frage relevant, ob der Diskussionsort zentral ist oder nicht. So werden etwa Diskussionen unter Beiträgen von

sen,[55] was teilweise so weit geht, dass versucht wird, die Popularität eines Kandidaten in bestimmten ethnischen Bevölkerungsteilen zu steigern.[56] Auf diesem Wege lassen sich gerade die oben beschriebenen Effekte nutzen, um auf die Informationsaufnahme und Meinungsbildung einzuwirken.

Freilich werden Meinungsroboter Wahlen nicht allein entscheiden können. Zahlreiche Möglichkeiten abseits sozialer Netzwerke sichern jedenfalls die Versorgung mit qualitativ hochwertigen Informationen. Das bedeutet aber nicht, dass das Thema zu vernachlässigen ist. Wie stark der Einfluss im Einzelfall ist, hängt von vielen Faktoren auf Seiten der Bots und der potentiell betroffenen Nutzer ab.[57] Je stärker ein Nutzer soziale Netzwerke – insbesondere als Informationsmedium – nutzt, desto wahrscheinlicher wird ein Einflusspotential. Hier wird auch der Personalisierung und der Vermittlung der Inhalte durch die Algorithmen selbst Bedeutung zukommen. So können bestimmte Teilgruppen eher in den Kontakt mit entsprechenden Inhalten kommen, weil sie der Algorithmus als empfänglicher ansieht und wegen der Heuristiken können diese dann auch eher beeinflusst werden. Ein Einfluss ist auch dann naheliegender, wenn die unterschiedlichen Strategien kumulativ verfolgt werden. Insoweit können Meinungsroboter durchaus in der Lage sein, Nutzer zu einem gewissen Grad zu beeinflussen.[58]

Auch wenn sich der Einfluss zurzeit in Grenzen halten mag, ist damit eine potentielle Intensivierung nicht ausgeschlossen. Zugleich muss man sich vor Augen halten, dass die aktuelle Diskussionslandschaft ohnehin von einer starken Spaltung geprägt ist. Insoweit ist es umso kritischer zu

---

Medien oder Politikern tendenziell relevanter sein, als eine Diskussion unter einem privaten Beitrag, was regelmäßig schon die Teilnehmerzahl zeigt.

55 Zu Venezuela *Forelle u.a.* (Fn. 42); zu Japan *Schäfer/Evert/Heinrich*, (Fn. 42), S. 294ff.; zum Ukraine Konflikt *Hegelich/Janetzko*, in: Proceedings of the 10th International AAAI Conference on Web and Social Media (ICWSM 2016), S. 579ff.

56 So etwa im US-amerikanischen Wahlkampf, wo durch zahlreiche Accounts mit hispanischem Hintergrund versucht wurde den Eindruck zu erwecken, Trump genieße breite Zustimmung bei hispanischen Bevölkerungsteilen, obgleich sich sein Wahlkampf deutlich gegen diese richtete, hierzu *Thieltges/Hegelich* (Fn. 3), S. 498.

57 Auf Seiten der Bots etwa Anzahl, Vernetzung innerhalb des Netzwerks, konkrete Aufgaben, Intention, konkrete Inhalte u.v.m. Auf Seiten der Nutzer werden neben politischer Vorbildung (hierzu etwa *Schoen* (Fn. 6), S. 90f.), das Selbstbewusstsein, die Vernetzung im Netzwerk, Gruppenzugehörigkeit etc. Zu den Risikofaktoren siehe auch *Thieltges/Hegelich* (Fn. 3), S. 503ff.

58 *Kind u.a.*, (Fn. 4), S. 58ff. Differenzierend *Thieltges/Hegelich* (Fn. 3), S. 509f.

bewerten, wenn hier auch noch weitere Manipulationen vorgenommen werden. Und auch die Bedeutung der sozialen Netzwerke muss Berücksichtigung finden. Sie bieten die einzige Möglichkeit, sich an einem größeren Diskurs zu beteiligen und gewinnen jedenfalls in Wahlkampfzeiten deutlich an Bedeutung, sodass auch die Bots eher dann aktiv sein werden.[59] Wegen der tendenziell langen Periode dazwischen können also nur eingeschränkt Aussagen über die Aktivität gemacht werden. Zeigen aber (theoretische) Studien auf, dass Meinungsroboter das konkrete Potential haben, Einfluss auszuüben, muss dies ausreichen. Wegen der Bedeutung der betroffenen Rechtsgüter wäre es nicht ratsam höhere Anforderungen zu stellen, weil eingetretene Fehlentwicklungen sich nicht oder nur schwer rückgängig machen ließen.[60] Das lässt sich an dem deutlichen Vertrauensverlust in Medien und der Spaltung des Diskurses bereits erahnen. Deshalb ist der Staat bereits jetzt verpflichtet Schutz vor den Meinungsrobotern zu gewähren.

III. Rechtsfolge – Ausgestaltungsauftrag an den Gesetzgeber

Aus der Schutzpflicht folgen aber nicht zwingend konkrete, intensive und vor allem regulative Maßnahmen. Da die Schutzpflicht letztlich zu Eingriffen in die Freiheitsrechte Dritter führt, setzt die abwehrrechtliche Funktion der Grundrechte hier Grenzen. So hat man es vorliegend mit einem Spannungsverhältnis zwischen Meinungsrobotern, Netzwerkbetreibern und Nutzern zu tun. So streitet die Meinungsfreiheit für die Urheber der Roboter[61] und die Berufs- und Eigentumsfreiheit für die Betreiber. Inso-

---

59 In diese Richtung auch *Forelle u.a.* (Fn. 42), S. 6.

60 Diese fehlende Restitutionsfähigkeit betont das BVerfG etwa, wenn es um Gefahren für die Vielfalt im Rundfunk geht, so etwa BVerfGE 131, 30 (52) – *Runfunkbeteiligung v. Parteien*, m.w.N. Die Restitutionsfähigkeit wird auch als Grundlage für eine Herabsetzung des Maßstabes andernorts herangezogen, vgl. hierzu etwa *Klein*, Grundrechtliche Schutzpflichten des Staates, NJW 1989, 1633 (1638). So letztlich auch *Semizoglu* (Fn. 30), S. 96.

61 Ausführlich hierzu etwa *Milker* (Fn. 29), S. 220; *Schröder*, Rahmenbedingung der staatlichen Regulierung von Social Bots, DVBl. 2018, 465 (466ff.); *Semizoglu* (Fn. 30), S. 84ff. Dabei ist allerdings der Ansatz über den Schutz anonymer und pseudonymer Äußerungen m.E. nicht überzeugend. Diese sollen einerseits *chilling effects* vorbeugen und dienen andererseits dem Schutz der informationellen Selbstbestimmung. Dieser Zusammenhang besteht bei Meinungsrobotern indes nicht, vgl. *v. Ungern-Sternberg*, Demokratische Meinungsbildung und künstliche Intelligenz, in: Unger/dies., Demokratie und künstliche Intelligenz, 3 (17ff.);

weit greifen hier also auch Abwehrrechte ein, die staatliches Handeln durch das Übermaßverbot begrenzen. Der Ausgleich dieser widerstreitenden Interessen obliegt allein dem Gesetzgeber.[62] Das BVerfG gewährt ihm deshalb einen weitreichenden Spielraum bei der Umsetzung der Schutzpflicht.[63] Die Grenze ist – jedenfalls nach der jüngeren Judikatur – dort erreicht, wo das Untermaßverbot (evident) verletzt wird.[64] Dies ist nur dann der Fall, wenn ein wirksamer Schutz gar nicht besteht, das Konzept gänzlich ungeeignet oder völlig unzulänglich ist, das gebotene Schutzziel zu erreichen, oder erheblich dahinter zurückbleibt.[65] Insoweit ist die Frage der Existenz eines wirksamen Schutzkonzeptes (2.), auch in Abhängigkeit von dem konkreten Schutzbedarf zu beantworten (1.). Dabei ist entscheidend, ob ergriffene Maßnahmen eine sachgerechte Balance zwischen Schutz und Eingriff darstellen (3.). Daneben lassen sich auch de lege ferenda ergänzende Maßnahmen aufzeigen (4.).

1. Konkreter Schutzbedarf

Betrachtet man die Schutzbedürftigkeit der Nutzer, so muss bedacht werden, dass wesentliche Wirkungsvoraussetzungen nutzerseitig bedingt sind.[66] Das gilt besonders für die Auswahl und die Art des Konsums von Medien und ihren Inhalten. Abseits des Internets besteht immerhin eine vielfaltssichernde Medienpluralität.[67] Allerdings kann es durchaus rational bedingt sein, wenn die Meinungsbildung vor allem auf Grundlage der Netzwerke erfolgt und dabei alternativen Quellen eher Glauben geschenkt

---

Semizoglu, ebd. Entscheidender ist hier, dass sie potentiell auch schützenswerte Inhalte verbreiten ohne dabei zwingend demokratiefeindlich zu sein. Deshalb sollte von einer Schutzbereichsbeschränkung schon deshalb abgesehen werden.

62 Vgl. hierzu BVerfGE 96, 56 (64f.) – *Vaterschaftsauskunft.* Ausführlicher zu dem „Konfliktschlichtungsauftrag" des Gesetzgebers *Ruffert*, Vorrang der Verfassung und Eigenständigkeit des Privatrechts, S. 203ff. *Calliess* (Fn. 27), S. 329; *ders.*, in: FS Starck, 2007, 201 (216) spricht deshalb von einem „Handlungskorridor" des Gesetzgebers.

63 BVerfGE 142, 313 (337) – *Zwangsbehandlung*, m.w.N.

64 Aus der Lit. zustimmend etwa *Krings* (Fn. 26), S. 271; *Gröpl*, in: FS Käfer, 2009, 95 (107); *Hesse*, in: FS Mahrenholz, 1994, 541 (556f.). In diese Richtung auch *Ruffert* (Fn. 62), S. 215.

65 Zuletzt etwa BVerfG NJW 2018, 2312 (2313) – *Fliegerhorst Büchel* m.w.N.

66 Vgl. hierzu *Thieltges/Hegelich* (Fn. 3), S. 504ff. mit Blick auf die Informationsdiffusion.

67 Insbesondere hierauf verweisend *Semizoglu* (Fn. 30), S. 95.

wird.[68] Entscheidend ist vorliegend vielmehr, dass die suggerierten Mehrheiten oder scheinbar wahren Nachrichten nicht existieren und deshalb anders zu bewerten sind als (sachliche) Kritik gegen Mainstream-Themen durch alternative Anbieter. Die Aufmerksamkeit der Nutzer und die darauffolgende rationale Informationsverarbeitung wird „erschlichen".[69] Und auch das Argument der Medienpluralität ist nur begrenzt überzeugend, weil man damit tendenziell an das Idealbild eines vollends rationalen und gut informierten Bürgers anknüpft, was aber nicht der Realität entspricht.[70] Vielmehr muss man hier eher den tatsächlichen Medienkonsum berücksichtigen.

Mit Blick auf die Täuschungswirkung geht es primär um die Gewährleistung von Transparenz, um den Nutzern wesentliche Informationen für eine eigenständige Entscheidung zur Verfügung zu stellen, wodurch bereits die Entstehung bestimmter Heuristiken oder selbstzensierender Effekte verhindert werden kann.[71] Mit Blick auf bestimmte Inhalte und die kollektive Wirkungssphäre, wäre zudem denkbar, Schutz vor gemeinschaftsschädlichen Informationen zu gewähren.[72] Insoweit soll und kann es gar nicht um die Herstellung eines „repräsentativen Internets"[73] oder gar den Schutz vor jedweder Lüge gehen.

---

68 Vgl. *Drexl* (Fn. 5), S. 535.

69 In der Tendenz lässt sich diese Situation etwa mit der beim Influencer-Marketing vergleichen. Auch hier wird durch die Vorspiegelung privater Kommunikation letztlich verdeckte kommerzielle Interessen verfolgt, die für die Follower – so denn dies nicht kenntlich gemacht ist – nicht oder nur schwer erkennbar ist, hierzu etwa *Fries*, Influencer-Marketing – Informationspflichten bei Werbung durch Meinungsführer in Social Media, 2019, S. 163.

70 Die Verhaltensökonomik hat sich bereits von dem Idealbild eines *homo oeconomicus* verabschiedet, weil Verbraucher eben auch irrationale Handlungen treffen, siehe *Ebers*, Beeinflussung und Manipulation von Kunden durch Behavioral Microtargeting, MMR 2018, 423 (424). Im Zusammenhang mit den hier besprochenen Problemen siehe *Drexl* (Fn. 2), S. 534 und mit Blick auf die Veränderung der Informationsaufnahme siehe *Boehme-Neßler*, Das Ende der Demokratie?, 2018, S. 36f und *Kaerlein* (Fn. 10), S. 23f.

71 Die Korrelation zwischen Transparenz und Täsuchungswirkung betont u.a. auch *v. Ungern-Sternberg*, in: Unger/dies. (Fn. 61), S. 19. Zur Forderung nach Transparenz etwa *Löber/Roßnagel* (Fn. 29), S. 497 oder *Klaas* (Fn. 29), S. 90.

72 Hierauf wird noch unter 4. zurückzukommen sein.

73 So nämlich *Milker* (Fn. 29), S. 220.

2. Das bisherige Schutzkonzept des Gesetzgebers

Wegen des dichotomen nationalen Kompetenzgefüges im Kontext der Medienregulierung können auf Bundes- und Landesebene Schutzkonzepte bestehen.[74] Und auch die EU wird hier zunehmend aktiv.[75] Die bisherigen nationalen Regelungen gewähren aber keinen spezifischen Schutz vor Meinungsrobotern. Sie sind vielmehr individualschützend ausgerichtet. Für Netzwerkbetreiber bietet das Vertragsrecht, insbesondere die Nutzungsbedingungen, das Urheberrecht (u.a. § 97 Abs. 1 UrhG)[76] und die Datenveränderungstatbestände des StGB (§§ 303a, b StGB)[77] Grundlagen, um den Einsatz von Bots zu verhindern und ihm (wirksam) entgegen treten zu können. Gerade das ist aber das eigentliche Problem, weil die Betreiber oft nur durch äußeren Druck eigenständig Maßnahmen ergreifen.

Nutzer werden in erster Linie vor den konkreten Äußerungsinhalten geschützt (§§ 130, 185ff. StGB). Das NetzDG erweitert diesen Schutz auch gegenüber den Netzwerkbetreibern. Mit Blick auf die angesprochene Intransparenz sieht insbesondere der RStV in § 55 Abs. 1 eine Kennzeichnungspflicht vor,[78] die allerdings eher die Täuschung verstärkt,[79] sofern sie überhaupt befolgt wird.

Spezifische wahlrechtliche Regelungen bestehen zwar mit den §§ 107 ff. StGB oder etwa mit § 32 Abs. 1 BWahlG. Allerdings erfassen sie Bots nicht oder stehen ihnen jedenfalls nicht wirksam im Wege.[80] Mit der DS-GVO bestehen Regelungen, die die Datenverarbeitung für die Personalisierung der Netzwerkbetreiber einschränkt, also Auswirkungen auf die Informationsvermittlung im Feed haben kann.[81] Allerdings werden nur hinsichtlich

74 Das zeigen etwa die Regelungen des TMG und des NetzDG des Bundes und der RStV der Länder. Zu den Kompetenzen ausführlicher *Hain*, in: Spindler/Schuster, elektronische Medien, Erster Teil Rn. 154ff.

75 Neben der geänderten AVMD-RL in der Fassung von RL 2018/1808, Ambl. 2018 L 303/69 auch der Verhaltenskodex zur Bekämpfung von Desinformation und der Vorschlag einer VO zur Verhinderung der Verbreitung terorristischer Online-Inhalte, KOM(2018) 640 final.

76 Zur urheberrechtlichen Seite ausführlich *Wolf*, Social Bots im Wahlkampf – Das UrhG als Handhabe gegen „Meinungsroboter"?, WRP 2019, 440ff.

77 Ausführlicher hierzu *Libertus* (Fn. 29), S. 23f.

78 *Klaas* (Fn. 29), S. 89 m.w.N.

79 Der Anbieter wird immerhin verpflichtet, persönliche Informationen bereit zu halten und nicht etwa die Automatisierung kenntlich zu machen. Dadurch kann sich aber der Eindruck einer menschlichen Identität verstärken.

80 Zu den Regelungen der §§ 107ff. ausführlicher *v. Ungern-Sternberg*, in: Unger/dies. (Fn. 61), S. 15f.

81 Hierzu näher auch *v. Ungern-Sternberg*, in: Unger/dies. (Fn. 61), S. 22ff.

des Umfangs der Datenverarbeitung Grenzen gezogen, sie bleibt aber i.d.R. zulässig.

Am Rande sei hier erwähnt, dass auch die EU mit ihrem Verhaltenskodex zur Bekämpfung von Desinformation[82] erste Maßnahmen gegen Desinformation, Meinungsroboter und Intransparenz bei der Filterung von Inhalten ergriffen hat. Zwar verhindert man durch die Freiwilligkeit der Unterzeichnung eine Beschränkung der Freiheiten der Dienstleister, allerdings erfolgt dies auf Kosten einer wirksamen Durchsetzung, die allein von den Unterzeichnern abhängt. In gewisser Weise opfert man also den Schutzaspekt zugunsten einer Kooperation und „Besänftigung" der Dienstleister. Sinnvoller könnte es indes sein, verbindliche Mindestvorgaben zu machen, um zum einen eine wirksame Umsetzung zu gewährleisten und zum anderen ein potentielles Over-Blocking zu vermeiden.

Das bestehende Schutzkonzept überlässt die wirksame Bekämpfung in erster Linie den Netzwerkbetreibern. Eine wirksame (staatliche) Kontrolle ist kaum sichergestellt und angesichts der Zurückhaltung der privaten Anbieter in der Vergangenheit äußerst fraglich. Regelungen, die die spezifischen Wirkmechanismen auf das Netzwerk und seine Nutzer abseits konkreter Inhalte erfassen, existieren hingegen nicht.

3. *Der Medienstaatsvertrag als Antwort und Balance zwischen Schutz und Eingriff?*

Im Dezember 2019 einigten sich die Ländervertreter – endlich – auf einen Entwurf eines Medienstaatsvertrages, der einerseits der Umsetzung der AVMD-Richtlinie[83] dient anderseits auch den RStV an ein digitales Zeitalter anpassen und im September 2020 in Kraft treten soll. Für Meinungsroboter sieht § 18 Abs. 3 erstmals eine Kennzeichnungspflicht vor, [84] die den Umstand einer automatisierten Veröffentlichung erfasst, wenn die Äußerung durch ein Nutzerkonto erfolgt, welches gewöhnlich von natürlichen Personen genutzt wird.[85] Verstöße stellen eine Ordnungswidrigkeit dar

82 Abrufbar unter https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation, Stand (8.04.2020).

83 RL 2010/13/EU i.d.F. der RL 2018/1808, Ambl. 2018 L 303/69.

84 In Kalifornien hat man eine solche bereits eingeführt, siehe Business and Professions Code, Ch. 6 s. 17490 f. In Deutschland war sie bereits seit längerem in der Diskussion, siehe etwa BR-Drs. 519/18.

85 § 18 Abs. 3 MStV lautet: „Anbieter von Telemedien in sozialen Netzwerke sind verpflichtet, bei mittels eines Computerprogramms automatisiert erstellten Inhal-

(§ 117 Abs. 1 S. 2 Nr. 2 MStV). Weil aber die Regelung nach § 1 Abs. 7 MStV-E nur für inländische Urheber gilt und zudem (wohl) erkannt wurde, dass die Kennzeichnung durch die Urheber unwahrscheinlich ist, erweitert § 93 Abs. 4 MStV-E die Pflicht auf die Netzwerkbetreiber. Danach haben sie „Sorge zu tragen", dass die entsprechenden Inhalte auch nach § 18 Abs. 3 gekennzeichnet werden. Das kann nach dem Marktortprinzip des § 1 Abs. 8 MStV-E auch für im EU-Ausland ansässige Betreiber gelten.[86]

Ganz unproblematisch ist der neue Entwurf allerdings nicht. So bleibt fraglich, was unter „Sorge tragen" überhaupt zu verstehen ist. Unzweifelhaft ist wohl noch, dass die Netzwerke die Voraussetzungen für eine Kennzeichnung schaffen müssen.[87] Was darüber hinaus zu fordern ist, ist unklar. Von Identitätskontrolle bis hin zu einer proaktiven Überwachungspflicht und eigenständigen Kennzeichnung ist vieles denkbar. Letzteres führt prima vista zu Konflikten mit Art. 15 Abs. 1 der E-Commerce-RL. Allerdings könnte die Regelung damit legitimiert werden, dass einerseits die dem Art. 15 zugrundeliegende Wertung hier nicht betroffen ist[88] und zu-

---

ten oder Mitteilungen den Umstand der Automatisierung kenntlich zu machen, sofern das hierfür verwandte Nutzerkonto seinem äußeren Erscheinungsbild nach für die Nutzung durch natürliche Personen bereitgestellt wurde. Dem geteilten Inhalt oder der Mitteilung ist der Hinweis gut lesbar bei – oder voranzustellen, dass diese unter Einsatz eines das Nutzerkonto steuernden Computerprogrammes automatisiert erstellt und versandt wurde. (…)"

86 Auch insoweit bestehen Probleme hinsichtlich der Vereinbarkeit mit dem durch die E-Commerce-RL geschaffenen Herkunftslandprinzip des Art. 3 Abs. 1 der RL.

87 *Löber/Roßnagel*, (Fn. 29), S. 498

88 I.E. bleibt diese Haftung unberührt. Ob hier ein Hinweis ausreicht, dass es nur um Modalitäten und nicht um Inhalte geht, ist fragwürdig, immerhin führt auch hier die Überwachungspflicht zu einer weitgehenden Analyse der Netzwerkdaten, anders *Löber/Roßnagel*, (Fn. 29), S. 498. Entscheidender ist hier eher, dass keine Rechtsverletzung im eigentlichen Sinne, wie etwa bei Urheber- oder persönlichkeitsrechtlichen Fällen vorliegt, hierzu zuletzt EuGH, Urt. v. 3.10.2019 – Rs. C-18/18, ECLI:EU:C:2019:821 – *Glawischnig-Piesczek*. Eine Haftung besteht i.E. nicht und selbst wenn, könnten Dritte diese mangels Erkennbarkeit der Täuschung kaum begründen. Insoweit besteht also eine ganz andere Wertungslage. Hier sei auch nur am Rande darauf hingewiesen, dass in neueren Rechtsakten der Union den Betreibern ebenfalls proaktive Pflichten auferlegt werden sollen, ohne dass sich dies auf die Haftungsprivilegien auswirkt, siehe hierzu etwa Art. 6 Abs. 1 i.V.m. Erwggr. 5 des Vorschlags einer VO zur Bekämpfung von terroristischen Online-Inhalten KOM(2018) 640 final. Hier werden die Betreiber zur Verfolgung gemeinwohlorientierter Zwecke tätig. Nichts anders gilt auch für § 93 Abs. 4 MStV-E.

dem Art. 1 Abs. 6 der RL pluralismussichernde Regeln der Mitgliedstaaten gerade ermöglicht.[89]

Betrachtet man das verfassungsrechtliche Spannungsverhältnis zwischen Schutz und Eingriff, so ist zunächst zu begrüßen, dass der MStV von einer Pflicht der Betreiber nach dem Vorbild des NetzDG ausgeht, um die Durchsetzung der Vorgaben zu effektuieren. Abgesichert wird diese Pflicht zum einen durch den Ordnungswidrigkeitentatbestand des § 117 Abs. 1 S. 2 MStV-E und durch aufsichtsrechtliche Befugnisse der Landesmedienanstalten nach § 95 i.V.m. § 56 MStV-E bzw. nach § 111 MStV-E. Zwar werden die Betreiber damit in ihrer wirtschaftlichen Freiheit eingeschränkt. Aber zum einen ist dies nur ein vergleichsweise geringer Eingriff[90] und zum anderen lässt sich das gut mit einer Art „Garantenpflicht" für ihre Systeme begründen. Auch hier greifen im Übrigen die Aspekte, die auch einer mittelbaren Drittwirkung zugrunde gelegt werden: Relevanz des Dienstes, öffentliches Forum, Machtstellung usw.[91] Und auch die Meinungsfreiheit der Urheber wäre nicht über Gebühr belastet, weil nur die erschlichene Wirkung rückgängig gemacht wird, die Äußerung aber möglich bleibt.[92]

Probleme tun sich aber an anderer Stelle auf: So wird durch die Regelung – ginge man von einer Überwachungspflicht aus – nicht sicher gestellt, dass gewöhnliche Nutzer nicht als Bots gekennzeichnet werden. Ent-

89 Insoweit sichert dieser gerade die medienrechtliche bzw. kulturpolitische Kompetenz der Mitgliedstaaten ab. Und vorliegend geht es gerade um Vielfaltssicherung, die allerdings – wegen des Regelungsgegenstandes – anders ausfallen muss als etwa beim Rundfunk, vgl. hierzu die Mitteilung der Kommission im Notifizierungsverfahren, TRIS(2020) 00328 unter 8.

90 Das liegt einerseits an dem Freiraum, den die Norm gewährleistet, andererseits aber auch daran, dass durch gewisse Automatisierungsprozesse jedenfalls der primäre Arbeitsaufwand in Grenzen gehalten werden kann und nur eine sekundäre händische Kontrolle notwendig wäre. Zudem trifft die Pflicht nur Netzwerke mit einer gewissen Bedeutung, vgl. § 91 Abs. 2 Nr. 2 MStV-E.

91 Vgl. BVerfG NJW 2019, 1935 Rn. 15; OLG Dresden, ZUM-RD 2019, 2 (6); LG Bamberg, MMR 2019, 56; *v. Ungern-Sternberg*, in: Unger/dies. (Fn. 61), S. 27; Das LG Leipzig, Endurteil v. 12.7.2019 – 08 O 2491/18, GRUR-RS 2019, 38785 Rn. 47 spricht von einer „mit der traditionellen Pflichten- oder Garantenstellung des Staates vergleichbaren Lage".

92 Ausführlicher zu der Vereinbarkeit mit der Meinungsfreiheit etwa *v. Ungern-Sternberg*, in: Unger/dies. (Fn. 61), S. 17ff. Insgesamt zur Vereinbarkeit mit den kollidierenden Interessen siehe etwa Löber/Roßnagel (Fn. 29), S. 496. Unklar bleibt aber, wie sich die Betreiberpflicht etwa zu der von Facebook vorgenommenen Sperrung von Fake-Profilen auf Grundlage der Nutzungsbedingungen verhält.

sprechende Analysesoftware lieferte schon in der Vergangenheit falsch-positive Ergebnisse.[93] Wird aber ein Nutzer fälschlich als Bot qualifiziert und gekennzeichnet, hat das Einfluss auf die Rezeptionschance von Äußerungen und damit wiederum auf die Meinungsäußerungsfreiheit des Art. 5 Abs. 1 S. 1 GG.[94] Auch hier besteht tendenziell die Gefahr eines Over-Blockings, worauf der MStV-E überhaupt nicht eingeht. Sinnvoller wäre es gewesen, dem bereits gesetzlich vorzubeugen.[95] So könnte eine gewisse Abstufung vorgenommen werden, die nach Grad der wahrscheinlichen Automatisierung unterscheidet und unterschiedlich intensive Rechtsfolgen vorsieht. So lässt sich zwischen erneuter Verifizierung bis hin zur Kennzeichnung variieren. Daneben ist aber auch eine verfahrensrechtliche Absicherung der betroffenen Nutzerrechte nicht gewährleistet. Vergleichbare Probleme stellten sich schon beim NetzDG, die durch den im Änderungsentwurf vorgesehenen Gegenvorstellungsverfahren (§ 3b NetzDG) aber beseitigt werden sollen.[96]

Insoweit ergibt sich mit Blick auf den MStV-E ein gemischtes Ergebnis. Zwar kommt der Gesetzgeber hier dem Schutzauftrag (endlich) nach, verkennt dabei aber die abwehrrechtlichen Grenzen, sodass verfassungsrechtliche Bedenken gegen den Entwurf bestehen.

4. Ergänzende Maßnahmen de lege ferenda

De lege ferenda könnte das Schutzkonzept auch anderweitig abgesichert und ergänzt werden. Ob es hierfür ratsam ist, einen Straftatbestand für Fake News zu schaffen, ist aber zweifelhaft.[97] In Betracht käme zwar eine

---

93 Vgl. *Neudert*, Ausschuss Drs. 19(23)046, S. 3f.

94 Ähnlich auch *Löber/Roßnagel* (Fn. 29), S. 498. Zumal die AGB ja auch den gänzlichen Ausschluss aus dem Netzwerk in solchen Fällen vorsehen, also noch über die gesetzliche Wirkung hinausgehen.

95 Europäische Rechtsakte verpflichten die Betreiber dazu, die betroffenen Grundrechte und ihre Bedeutung zu berücksichtigen, siehe hierzu etwa den Kommissionsentwurf KOM(2018) 640 final, Art. 3 Abs. 1, 6 Abs. 1.

96 BT-Drs. 19/18792, S. 9.

97 Ausführlicher zu einem solchen Ansatz *Hoven*, Zur Strafbarkeit von Fake News – de lege lata und de lege ferenda, ZStW 2017, 718 (737ff.). Eine ähnliche Diskussion wurde bereits in Italien geführt, vgl. Wissenschaftlicher Dienst d. Bundestages, WD 10-3000-27/19. Eine Änderung des dortigen Strafrechts ist bisher aber nicht erfolgt. Und da bspw. Facebook bereits den Kampf gegen Fake News mit Hilfe externer Factchecker aufgenommen hat, lässt sich zumindest fragen, ob eine solche Regelung überhaupt notwendig wäre.

Erweiterung des § 130 oder der §§ 108 ff. StGB, sodass mit dem NetzDG dann auch die wirksame Durchsetzung gesichert werden kann.[98] Mit Blick auf die Meinungsfreiheit dürfte das in aller Regel aber nur bei bewusst oder erwiesen unwahren Tatsachenbehauptungen oder dort in Betracht kommen, wo Sorgfaltspflichten evident verletzt worden sind. Eine isolierte Tatsachenbehauptung wird aber nur selten vorliegen, sodass das Schutzniveau höher ist.[99] Eine verfassungsmäßige Grenze zu ziehen – etwa bei einer erheblichen Vergiftung des Meinungsklimas – gestaltet sich schwer, wäre aber notwendig, weil ein Schutz nicht vor jeder Lüge geboten ist[100]. Vielmehr ist die Ermittlung der Wahrheit und Enttarnung der Lüge zuvörderst Aufgabe des Meinungskampfes. Hinzu kommen Wertungsfragen um die Bedeutung der Unwahrheit ähnlich wie auch bei § 186 StGB.[101] Und einmal mehr besteht die Gefahr des Over-Blockings.

In jedem Fall ratsam ist es aber auch die Medienkompetenz der Nutzer zu stärken. Hierfür wäre die Anpassung von Lehrplänen im Rahmen der Schulaufsicht der Länder möglich, um eine deutlich stärkere Fokussierung auf den Umgang mit (digitalen) Medien zu erreichen. Und auch staatliche Informationskampagnen sind denkbar, um ältere Nutzerschichten zu erreichen.

Daneben wäre es ratsam, dass der Gesetzgeber weiterhin die Forschung finanziell unterstützt und die Ergebnisse sorgsam auswertet, um bei Bedarf nachzujustieren. Insoweit wäre es gar hilfreich, wenn man einen Forschungszugang zu den Netzwerken zunächst auf freiwilliger Basis, ggf. aber auch mit gesetzlichem Zwang, schaffen würde, um das Einflusspotential bestimmter Phänomene besser beurteilen zu können.[102]

Ebenso wäre es auch denkbar, dass die Betreiber generell stärker in die Pflicht genommen werden, ihre Algorithmen darauf zu trainieren bestimmte Manipulationen zu erkennen und entsprechende Inhalte jeden-

98 Hierzu *Mafi-Gudarzi* (Fn. 18), S. 68. Kritisch hierzu *Drexl* (Fn. 2), S. 540f.

99 St. Rspr. seit BVerfGE 85, 1 (15) – *Bayer-Aktionäre*.

100 *Milker* (Fn. 29), S. 220.

101 Statt vieler *Regge/Pegel*, in: MüKo StGB, Bd. IV, § 186 Rn. 24ff. m.w.N. Etwaige strafrechtsdogmatische und rechtspolitische Fragen stellt in diesem Zusammenhang auch *Mafi-Gudarzi* (Fn. 18), S. 68.

102 Twitter gewährleistet einen solchen Zugang jedenfalls, weshalb auch die meisten Studien hierzu veröffentlicht werden. Facebook ist hier zurückhaltender. Die berechtigten Interessen der Betreiber sind dann allerdings zu berücksichtigen und abzusichern. Datenschutzrechtlich wäre aber eine Analyse der Netzwerkdaten grundsätzlich möglich, siehe u.a. Artt. 5 lit b.), 85 DS-GVO, § 27 BDSG.

falls nicht priorisiert weiterzuleiten.[103] Der MStV-E enthält „nur" Vorschriften zur Transparenz und zum diskriminierungsfreien Angebot von redaktionell-journalistischen Inhalten (§§ 93, 94 MStV-E). Und allgemein lässt sich sicherlich auch über eine europäische verbindliche Lösung nachdenken, um ein einheitliches Schutzniveau im Binnenmarkt zu gewährleisten.[104]

IV. Fazit

Von Meinungsrobotern geht eine potentielle Gefahr für den Willensbildungsprozess aus, die staatliche Schutzpflichten aktiviert und durch die im MStV-E vorgesehene Pflichten vorerst erfüllt werden. Aus abwehrrechtlicher Sicht werden aber wesentliche Schutzvorkehrungen für die Meinungsfreiheit in dem Vorschlag nicht getroffen. Insoweit besteht ggf. Nachbesserungsbedarf. Inwieweit sich die Norm in der Praxis schlägt, bleibt abzuwarten. In jedem Fall ist der Gesetzgeber aber dazu verpflichtet, die bestehende Lage zu beobachten. Hierfür böte es sich an, nicht nur die empirische Forschung finanziell zu unterstützen, sondern auch einen Zugang zu den Netzwerkdaten zu schaffen. Nur so lässt sich die Überprüfung bisheriger Einschätzungen ermöglichen. Abhängig von diesen Ergebnissen, kann der Gesetzgeber zu einer Nachbesserung oder Aufhebung der Regelungen verpflichtet sein. [105]

---

103 Hierzu *Drexl* (Fn. 2), S. 541. Das wird aber auch wieder Spannungen mit Art. 15 Abs. 1 der E-Commerce-Richtlinie hervorrufen, weshalb auch über eine europäische Lösung nachzudenken wäre.

104 Abgrenzungsprobleme ergeben sich insoweit nur hinsichtlich der allein den Mitgliedstaaten vorbehaltenen Medienpolitik und der wirtschaftlich ausgerichteten EU-Kompetenz. Wegen des Doppelcharakters der Medien als Kultur- und Wirtschaftsgut, kann aber auch ein europäischer Zugriff, insbesondere über Art. 114 AEUV erfolgen, um Beeinträchtigungen des Binnenmarktes zu verhindern.

105 Zur Nachbesserungspflicht vgl. BVerfGE 56, 54 (78) – *Fluglärm* m.w.N. Die abwehrrechtliche Seite der betroffenen Grundrechte kann den Gesetzgeber aber dazu veranlassen, die Regelungen aufheben zu müssen, sobald erkennbar wird, dass Meinungsroboter überhaupt keine Relevanz im Meinungsbildungsprozess besitzen.