PAUL DÜRR

Social Bots

Internet und Gesellschaft
32

Mohr Siebeck

Internet und Gesellschaft

Schriften des Alexander von Humboldt Institut für Internet und Gesellschaft

Herausgegeben von

Jeanette Hofmann, Matthias C. Kettemann,
Björn Scheuermann, Thomas Schildhauer
und Wolfgang Schulz

32

Paul Dürr

Social Bots

Digitale Manipulation und Verfassungsrecht

Mohr Siebeck

Paul Dürr, geboren 1990; Studium der Rechtswissenschaften an der Universität Münster und der Universidad Autónoma de Madrid; Wissenschaftliche Mitarbeit am Weizenbaum Institut für die vernetzte Gesellschaft in Berlin und Forschungsaufenthalt an der Universität Haifa; Rechtsreferendariat am Kammergericht Berlin; Rechtsanwalt in Berlin.
orcid.org/0000-0003-4008-1856

D 6

Open Access gefördert durch den Fachinformationsdienst (FID) interdisziplinäre Rechtsforschung in Berlin.

ISBN 978-3-16-163385-0 / eISBN 978-3-16-163386-7
DOI 10.1628/978-3-16-163386-7

ISSN 2199-0344 / eISSN 2569-4081 (Internet und Gesellschaft)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über *https://dnb.dnb.de* abrufbar.

Publiziert von Mohr Siebeck Tübingen 2024. www.mohrsiebeck.com

Das Buch wurde von Beltz Grafische Betriebe in Bad Langensalza auf alterungsbeständiges Werkdruckpapier gedruckt und dort gebunden.

Printed in Germany.

Für meine Großeltern

Vorwort

Diese Arbeit wurde im Sommersemester 2023 von der Rechtswissenschaftlichen Fakultät der Universität Münster als Dissertation angenommen. Die digitale Manipulation des öffentlichen Meinungsbildungsprozesses ist ein Themenfeld, das sich in technologischer, politischer und (rechts-)wissenschaftlicher Hinsicht sehr dynamisch entwickelt. Die Arbeit berücksichtigt Literatur und Regulierungsvorhaben bis zum Herbst 2023. Jedoch hoffe ich, dass die verfassungsrechtlichen Überlegungen auch für zukünftige Manipulationsphänomene und regulatorische Konzepte fruchtbar gemacht werden können.

Mein Dank gilt zunächst Herrn Prof. Dr. Fabian Wittreck, der mein Promotionsvorhaben von der Konzeption bis zur mündlichen Prüfung betreut hat. Er hat im Studium mein Interesse am Verfassungsrecht geweckt und verkörpert für mich bis heute höchstes Engagement für Forschung und Lehre.

Herrn Prof. Dr. Herbert Zech danke ich für die Erstellung des Zweitgutachtens. Vor allem aber bedanke ich mich für die kontinuierliche Unterstützung meines Dissertationsprojekts, geistreiche Denkanstöße und die Leidenschaft, die er für Wissenschaft vermittelt.

Ich hatte das Privileg, dass mein Forschungsvorhaben durch öffentliche Mittel gefördert wurde. Bedanken möchte ich mich dafür bei der Studienstiftung des deutschen Volkes und dem Weizenbaum Institut für die vernetzte Gesellschaft. Am Weizenbaum Institut sind große Teile der Arbeit entstanden. Dort zu arbeiten und zu forschen, war ein großes Glück: Das Institut bot mir nicht nur ideale Voraussetzungen zum Nachdenken und Schreiben. Es brachte mich auch mit vielen Menschen zusammen, bei denen ich mich für akademische Diskussionen, kulinarische Freuden und jede Menge heiterer Momente bedanken möchte. Das gilt natürlich in besonderem Maße für meine Weggefährten der FG 16: Simon Schrör, Jana Pinheiro, Ferdinand Müller, Pablo Schumacher und Alexandra Keiner.

Bei meinen Eltern Tatjana und Frank bedanke ich mich für bedingungslose Unterstützung und das uneingeschränkte Vertrauen, das sie mir entgegenbringen. Jürgen und Sabine danke ich für unermüdliches Korrekturlesen. Dir, liebe Charlotte, danke ich für deine Zuneigung, Aufmunterung, Fußnotenkorrekturen und vieles mehr.

Berlin, im Februar 2024 Paul Dürr

Inhaltsübersicht

Vorwort VII

Inhaltsverzeichnis XI

Einleitung 1

A. Anlass der Untersuchung: Social Bots als Sinnbild kommunikativer Veränderungen 1

B. Zentrale Fragestellungen und Eingrenzung des Untersuchungsumfangs 4

C. Gang der Untersuchung 5

Teil 1: Untersuchungsgegenstand: Social Bots – ein neues Instrument digitaler Manipulation 7

A. Social Bots als pseudomenschliche Kommunikationsteilnehmer innerhalb sozialer Netzwerke 7

B. Social Bots und die digitale Manipulation politischer Prozesse 32

Teil 2: Verfassungsrechtlicher Schutz durch das Grundrecht auf Meinungsäußerungsfreiheit 55

A. Persönlicher Schutzbereich 55

B. Sachlicher Schutzbereich 78

Teil 3: Beeinträchtigte Interessen: Social Bots und die demokratische Öffentlichkeit 151

A. Öffentlichkeit und Manipulation im demokratischen System des Grundgesetzes 151

B. Auswirkungen auf den demokratischen Legitimationsmodus der Wahlen 168

C. Beeinträchtigung subjektiv-individueller Kommunikationsinteressen 199

D. Verzerrung des öffentlichen Meinungsbildungsprozesses 207
E. Besondere Restriktionen für staatliche Stellen und Parteien 255
F. Staatliche Schutzpflicht und legislativer Gestaltungsspielraum 297

Teil 4: Regulierung von Social Bots 311
A. Selbstregulierung der Plattformbetreiber 311
B. Regulierungskonzept de lege lata: Zur Kennzeichnungspflicht des Medienstaatsvertrags 324
C. Regulierungsperspektiven de lege ferenda 357
D. Zwischenergebnis, resilienzfördernde Maßnahmen und Restrisiko ... 378

Zusammenfassende Thesen 381

Literaturverzeichnis 387

Sachverzeichnis 411

Inhaltsverzeichnis

Vorwort VII

Inhaltsübersicht IX

Einleitung 1

A. Anlass der Untersuchung: Social Bots als Sinnbild kommunikativer Veränderungen 1

B. Zentrale Fragestellungen und Eingrenzung des Untersuchungsumfangs 4

C. Gang der Untersuchung 5

Teil 1: Untersuchungsgegenstand: Social Bots – ein neues Instrument digitaler Manipulation 7

A. Social Bots als pseudomenschliche Kommunikationsteilnehmer innerhalb sozialer Netzwerke 7

I. Begriffsklärung 7

1. Bot-Technologie und die Automatisierung digitaler Aufgaben 8

2. Arbeitsdefinition 10

3. Abgrenzung zu verwandten Internetphänomenen 11

a) Fake News und Desinformation 12

b) Trolle 13

c) Chatbots 14

d) Cyborgs 14

II. Technischer Hintergrund: Zur Erstellung und Vervielfältigung von Social Bots 16

III. Handlungsspektrum von Social Bots 19

1. Netzwerkspezifische Funktionen als absolute Grenze 19

2. Die Leistungsfähigkeit der Steuerungssoftware als relative Grenze 20

IV. Künstliche Authentizität durch Täuschung 24

V. Enttarnungsmöglichkeiten und ihre Grenzen 26

1. Mangelnde Medienkompetenz der Internetnutzer 26

2. Professionelle Enttarnung 27
VI. Einsatzmöglichkeiten und Missbrauchsgefahr 30

B. Social Bots und die digitale Manipulation politischer Prozesse 32
I. Einsatzbeispiele 33
1. Exemplarische Social Bot-Einsätze weltweit 33
2. Situation in Deutschland 35
II. Begriffsklärung: (Digitale) Manipulation als verdeckte Form der Beeinflussung 37
III. Manipulationsstrategien 39
1. Verzerrung des Kommunikationsprozesses durch das Erzeugen künstlicher Mehrheiten und die Simulation gesellschaftlichen Rückhalts 40
a) Strategien zur Erlangung quantitativer Meinungsmacht 40
b) Auswirkungen auf die Meinungsbildung: Zur „Schweigespirale“ und dem Prinzip sozialer Bewährtheit 42
2. Blockieren gegnerischer Meinungskanäle 44
3. Zukunftsszenario: Von einer quantitativen zu einer qualitativen Manipulation 45
IV. Zur tatsächlichen Relevanz: Der Effekt von Social Bots auf politische Entscheidungsprozesse 47
1. Methodische Schwierigkeiten und empirische Unschärfen 47
2. Kein unmittelbarer Einfluss auf das Ergebnis politischer Entscheidungen 48
3. Potenzielle Auswirkungen auf den Prozess der öffentlichen Meinungsbildung 49
4. Eine neue Qualität politischer Manipulation 51
5. Zwischenergebnis: Aktuelles Risiko und vorläufige Gefahrenprognose 52

Teil 2: Verfassungsrechtlicher Schutz durch das Grundrecht auf Meinungsäußerungsfreiheit 55

A. Persönlicher Schutzbereich 55
I. Grundrechtsberechtigung *de lege lata* 56
1. Natürliche Personen als „originäre“ Grundrechtsträger 56
2. Grundrechtsberechtigung juristischer Personen 60
a) Begriff der „juristischen Personen“ i.S.d. Art. 19 Abs. 3 GG 61
b) Restriktion auf „inländische“ juristische Personen 62
c) Wesensvorbehalt 63
II. Grundrechtsberechtigung *de lege ferenda*: Ausweitung auf technische Systeme 65
1. Mögliche Ausgestaltung einer Grundrechtserstreckungsnorm für „maschinelle Personen“ 67

2. Vereinbarkeit einer Verfassungsänderung mit Art. 79 Abs. 3 GG 69
3. Rechtspolitische Bewertung ... 73
a) Verfassungsrechtliches Schutzvakuum ... 73
b) Argumente gegen eine Ausweitung der Grundrechtsberechtigung ... 76
c) Schrittweise Statuserweiterung ... 77
III. Zwischenergebnis ... 78

B. Sachlicher Schutzbereich ... 78
I. Grundrechtsdogmatische Vorüberlegung: Vorzüge einer weiten Schutzbereichsinterpretation ... 79
1. Grundrechtsdogmatischer Dreischritt: Schutzbereich, Eingriff, Rechtfertigung ... 81
2. Liberales Grundrechtsverständnis: Konfliktlösung primär auf Rechtfertigungsebene ... 82
3. Restriktionsansatz: Enger Gewährleistungsinhalt statt weiter Schutzbereich ... 82
4. Weiter Schutzbereich als Basis einer rationalen Grundrechtsargumentation ... 84
5. Abstrakte Voraussetzungen für die Annahme einer Schutzbereichsausnahme ... 87
6. Zwischenergebnis ... 90
II. Inhaltsfrage: Digitale Desinformation als „Meinung" im Sinne von Art. 5 Abs. 1 S. 1 Var. 1 GG ... 90
1. Ausgangspunkt: Weites verfassungsrechtliches Begriffsverständnis ... 91
2. Schutzbereichsausnahme für (bewusst) unwahre Tatsachenbehauptungen ... 94
a) Dogmatische Rechtfertigung der Schutzbereichsausnahme 94
b) Fake News und Desinformation als bewusst unwahre Tatsachenbehauptungen ... 98
c) Einsatz von Social Bots als bewusst unwahre Tatsachenbehauptung ... 99
3. Schutz von Schmähkritik, Formalbeleidigungen und Hassrede 100
III. Modalitätsfrage: Social Bots als geschütztes Äußerungsmedium ... 103
1. Schutzbereichsrelevante Besonderheiten von Social Media-Kommunikation ... 104
a) Die Meinungsfreiheit als „technikoffenes Grundrecht": Schutz digitaler Kommunikation ... 104
b) Einzelne Social Media-Funktionen und ihr kommunikativer Gehalt ... 105
2. Absolute Grenze der Modalitätsfreiheit: Verhaltenssteuerung durch Zwang ... 108

a) Physische Gewalt als Ausgangspunkt 109
b) Vorsichtige Erweiterung der Restriktion: psychischer Zwang durch Drohungen 111
c) Verortung von Social Bots: Blockieren von Meinungskanälen als digitaler Zwang 113
3. Automatisierung als legitime Form moderner Individualkommunikation 115
a) Kein Schutz von intermaschinellem Datenaustausch 115
b) Programmierung eines Algorithmus als antizipierte Meinungsäußerung 117
c) Mindesterfordernis: Zurechnungszusammenhang zwischen Mensch und Maschine 119
aa) Zivilrechtliche Zurechnungsgrundsätze zur automatisierten Willenserklärung 121
bb) Zurechnung automatisierter Meinungsäußerungen durch Social Bots 124
cc) Konkretisierung des Zurechnungssubjekts 127
4. Fiktive Profilgestaltung als geschützte Anonymität 128
a) Begriffsklärung: Pseudonymität und Anonymität 128
b) Verfassungsrechtlicher Schutzumfang 129
aa) Wortlaut des Art. 5 Abs. 1 S. 1 Var. 1 GG 131
bb) Systematischer Zusammenhang 131
cc) Telos 132
(1) Einwände gegen den Anonymitätsschutz 133
(2) Der Schutz vor Selbstzensur als maßgebliches Argument für den Anonymitätsschutz 136
c) Zwischenergebnis 138
5. Rechtsdogmatisches Neuland: Schutzbereichsausnahme für „bewusst unwahre Meinungsäußerungsmodalitäten“ 138
a) Präzisierung des Täuschungselements: Verbindung von Automatisierung und Identitätstäuschung 139
b) Begründungsansätze für eine neue Schutzbereichsausnahme 140
aa) Unterschiede zu bisherigen Formen der Anonymisierung 141
(1) Qualitative Unterschiede 141
(2) Quantitative Unterschiede 144
bb) Parallele zur Schutzbereichsausnahme für bewusst unwahre Tatsachenbehauptungen 145
c) Zwischenergebnis: Plädoyer für eine Berücksichtigung des Täuschungselements auf Rechtfertigungsebene 148

Teil 3: Beeinträchtigte Interessen: Social Bots und die demokratische Öffentlichkeit 151

A. Öffentlichkeit und Manipulation im demokratischen System des Grundgesetzes 151
I. Öffentlichkeit: Begriff, Struktur(wandel) und Funktionen im demokratischen System 152
1. Begriff der Öffentlichkeit 152
2. Struktur von Öffentlichkeit: Ebenen, Foren, Akteure 154
3. Digitaler Strukturwandel der Öffentlichkeit 156
4. Funktionen von Öffentlichkeit im demokratischen System 159
II. Demokratische Öffentlichkeit als verfassungsrechtliches Leitbild ... 162
III. Normative Leitplanken des Grundgesetzes 163
IV. Demokratische Öffentlichkeit zwischen Partizipation und Manipulation 166

B. Auswirkungen auf den demokratischen Legitimationsmodus der Wahlen 168
I. Wahlen als zentraler Modus demokratischer Legitimation 168
II. Freiheit der Wahl 169
1. Absoluter Schutz vor externer Beeinflussung beim Akt der Stimmabgabe 170
2. Wahlbeeinflussungen im Vorfeldstadium: Zwischen zulässigem Wahlkampf und unzulässiger Beeinträchtigung der Entscheidungsfreiheit 173
a) Mindesterfordernis: Funktionaler Kontext zu einer Wahl ... 173
b) Verstoß gegen Freiheit der Wahl nur bei hinreichender Intensität der Beeinflussungshandlung 176
aa) Inkompatibilität von Freiheit (der Wahl) und Zwang ... 177
bb) Graubereich zwischen Zwang und argumentativer Überzeugung 179
c) Manipulation und Täuschung im Kontext der Freiheit der Wahl 182
aa) Manipulation und Freiheit der Wahl in der Rechtsprechung 182
bb) Grundsatz: Restriktive Anwendung des Art. 38 Abs. 1 S. 1 GG bei Manipulationen des Willensbildungsprozesses 186
cc) Ausnahme: Marginalisierung des individuellen Entscheidungsspielraums 188
dd) Wählerautonomie und digitale Manipulation durch Social Bots 191
III. Gleichheit der Wahl 193
IV. Öffentlichkeit der Wahl 197

V. Zwischenergebnis ... 199

C. Beeinträchtigung subjektiv-individueller Kommunikationsinteressen 199
I. Meinungsfreiheit ... 199
II. Informationsfreiheit ... 202
1. Kein subjektives Recht auf wahrheitsgemäße Information ... 202
2. Negative Dimension der Informationsfreiheit: Schutz vor aufgedrängter Information und das Recht auf selbstbestimmte Rezeption ... 203
III. Zwischenergebnis ... 207

D. Verzerrung des öffentlichen Meinungsbildungsprozesses ... 207
I. Verfassungsrechtlicher Maßstab: Die objektive Dimension von Art. 5 Abs. 1 GG ... 209
1. Objektive Dimension und überindividueller Inhalt der Grundrechte ... 209
2. Objektiv-rechtliche Grundrechtsgehalte im System der Kommunikationsfreiheiten ... 212
a) Gemeinsames Ziel: Freiheit individueller und öffentlicher Meinungsbildung ... 212
b) Unterschiede in inhaltlicher und dogmatischer Ausrichtung ... 214
c) Präzisierung des normativen Anknüpfungspunkts ... 216
3. Der Kommunikationsprozess als objektiv-rechtliches Schutzgut der Meinungsfreiheit ... 216
a) Die demokratiekonstituierende Funktion der Meinungsfreiheit als Basis eines überindividuellen Freiheitschutzes ... 217
b) (Unzureichende) verfassungsdogmatische Konkretisierung des Schutzguts ... 219
4. Zwischenergebnis ... 221
II. Das Konzept kommunikativer Chancengleichheit als Konkretisierungsansatz ... 221
1. Übergeordneter Kontext: Demokratischer Wettbewerb und das Prinzip der Chancengleichheit ... 222
2. Verfassungsrechtliche Verankerung und Funktion ... 224
3. Normativer Gehalt: Kommunikative Chancengleichheit als privilegienkritischer Analysemaßstab ... 226
4. Bisherige Anwendungsfelder ... 228
a) Chancengleicher Zugang zum Kommunikationsprozess ... 228
b) Verhinderung vorherrschender Meinungsmacht im Bereich der Massenmedien ... 230
5. Zwischenergebnis ... 233
III. Social Bots im Kontext kommunikativer Chancengleichheit ... 233

1. Der Einsatz von Social Bots als Machtfaktor im Meinungsbildungsprozess 234
2. Zur Legitimierung kommunikativer Machtungleichgewichte 236
a) Verfassungsrechtliches Ideal: Geistiger Meinungskampf und kommunikativ begründete Machtstellungen 237
b) Die Ausübung von Zwang als Inbegriff illegitimer Meinungsmacht 239
3. Verortung digitaler Manipulation durch Social Bots 241
a) Automatisierung als technisch vermittelte Macht 241
aa) Anwendungen der Kommunikationsautomatisierung als nicht-exklusive Hilfsmittel 243
bb) Zur kommunikativen Relevanz von Automatisierungsanwendungen 244
b) Das Täuschungselement und die Macht digitaler Claqueure 246
aa) Drei Täuschungsdimensionen 246
bb) Zur besonderen Qualität der erzeugten Meinungsmacht 247
cc) Normative Einordnung: Social Bots im Spannungsverhältnis mit den Zielwerten des Art. 5 Abs. 1 S. 1 GG 250
(1) Kommunikative Selbstbestimmung 250
(2) Demokratische Öffentlichkeit und das Prinzip „one man, one voice“ 252
4. Zwischenergebnis 254

E. Besondere Restriktionen für staatliche Stellen und Parteien 255
I. Social Bots als Instrument staatlicher Kommunikationstätigkeit ... 256
1. Der Staat als Faktor der öffentlichen Meinungsbildung 256
2. Zurechnungskriterien: Inanspruchnahme amtlicher Autorität oder staatlicher Ressourcen 258
3. Verfassungsrechtlicher Kontext staatlicher Kommunikationstätigkeit 261
4. Richtigkeit, Sachlichkeit und Neutralität als etablierte, aber unzureichende Maßstäbe 262
a) Richtigkeitsgebot 263
b) Sachlichkeitsgebot 263
c) Neutralitätsgebot 265
aa) Verfassungsrechtliche Verankerung 265
bb) Normativer Gehalt: Verbot zielgerichteter Wettbewerbsverzerrungen 265
cc) Digitaler Kontext und Konfliktpotenzial beim Einsatz von Social Bots 267

5. Keine Unsichtbarkeit des Staates: Social Bots als Verstoß gegen das Gebot der Kommunikatorklarheit 269
a) Verfassungsrechtliche Verankerung 269
b) Normativer Gehalt und Anwendung auf das Phänomen der Social Bots 271
aa) Mindestvorgabe: Erkennbarkeit des Staates und Ausschluss von Identitätstäuschungen 272
bb) Erweiterung: Transparenz bei Kommunikationsautomatisierung 273
6. Zwischenergebnis 276
II. Social Bots und die verfassungsrechtliche Sonderstellung politischer Parteien 277
1. Zwischen Staat und Gesellschaft: Zur Rolle der Parteien in der Kommunikationsordnung des Grundgesetzes 278
2. Status der Freiheit: Keine Übertragbarkeit der für den Staat geltenden Kommunikationsgebote 281
3. Status der Gleichheit: Implikationen für den Wettbewerb der Parteien 284
4. Status der Öffentlichkeit: Besondere Verantwortung für den Kommunikationsprozess und verfassungsrechtliche Transparenzerwartung 286
a) Status der Öffentlichkeit als verantwortungsbegründendes Element 287
b) Verfassungsrechtliche Verankerung und inhaltliche Konkretisierung 287
c) Social Bots im Spannungsfeld zwischen verfassungsrechtlicher Transparenzerwartung und kommunikativer Freiheit 290
aa) Zur freiheitslimitierenden Wirkung von Art. 21 Abs. 1 S. 1 GG 290
bb) Identifizierbarkeit der Partei als demokratisches Anliegen 292
cc) Täuschung über den Automatisierungsumstand und der Gedanke der Ressourcentransparenz 294
5. Zwischenergebnis 296

F. Staatliche Schutzpflicht und legislativer Gestaltungsspielraum 297
I. Social Bots im mehrpoligen Verfassungsrechtsverhältnis 298
1. Grenzen von Abwehrdimension und (mittelbarer) Drittwirkung der Grundrechte 298
2. Staatliche Schutzpflicht als dogmatischer Hebel zur Effektuierung grundrechtlicher Wertungen 299
II. Tatbestand der staatlichen Schutzpflicht 301

1. Social Bots als Instrument der Grundrechtsbeeinträchtigung 301
2. Gefahrenschwelle: Staatliche Schutzpflicht trotz empirischer Unschärfen 303
a) Polizeirechtlicher Gefahrenbegriff als Orientierungspunkt 303
b) Wahrscheinlichkeit des Schadenseintritts und empirische Unschärfen 304
c) Besondere Qualität der Grundrechtsbeeinträchtigung 305
III. Rechtsfolge: Weiter Gestaltungsspielraum des Gesetzgebers 306

Teil 4: Regulierung von Social Bots 311

A. Selbstregulierung der Plattformbetreiber 311
I. Keine grundrechtlich determinierte Schutzpflicht der Plattformbetreiber 312
II. Wirtschaftliche Rationalitäten als Basis der Selbstregulierung 312
III. Mobilisierung durch Soft Law: EU-Verhaltenskodex zur Bekämpfung von Desinformation 313
IV. Normative Struktur der Selbstregulierung: Social Bot-Manipulation als Verstoß gegen die Plattform-Regeln 315
1. Facebook 316
2. Twitter 318
V. Vorteile und Grenzen der Selbstregulierungsmaßnahmen 319
1. Vorteile: Technische Kapazitäten und normative Reichweite 320
2. Grenzen: Effektivitäts- und Transparenzdefizite im Kontext des grundrechtlichen Freiheitsanspruchs 321
VI. Zwischenergebnis 323

B. Regulierungskonzept de lege lata: Zur Kennzeichnungspflicht des Medienstaatsvertrags 324
I. Kennzeichnungspflicht für Nutzer sozialer Netzwerke (§ 18 Abs. 3 MStV) 325
1. Adressaten: Inländische Nutzer sozialer Netzwerke 326
2. Tatbestandsmäßiges Verhalten: Kommunikationsautomatisierung mit Täuschungspotenzial 327
a) Automatisiert erstellte Inhalte oder Mitteilungen 327
b) Authentische Ausgestaltung des Nutzerkontos 330
3. Rechtsfolge: Kennzeichnungspflicht und Sanktionsmöglichkeiten 331
4. Bewertung: Risikoadäquates Instrument mit Durchsetzungsproblemen 332
a) Verhältnismäßigkeit der Kennzeichnungspflicht 332
aa) Legitimer Zweck 332
bb) Geeignetheit 333
cc) Erforderlichkeit 334

dd) Angemessenheit ... 335
(1) Geringe Schutzwürdigkeit bei Täuschung über Automatisierungsumstand ... 335
(2) Manipulationspotenzial als Abwägungsfaktor ... 337
(3) Abwägungsergebnis: Praktische Konkordanz durch Transparenz ... 339
b) Zu den Problemen bei der Rechtsdurchsetzung und der (nicht nur) symbolischen Wirkung der Kennzeichnungspflicht ... 339
II. Effektuierung der Kennzeichnungspflicht durch vorsichtige Einbindung der Plattformbetreiber (§ 93 Abs. 4 MStV) ... 341
1. Adressaten: Betreiber sozialer Netzwerke ... 342
2. Konkretisierung des Verantwortungstatbestands ... 342
a) Der weite Wortlaut als Ausgangspunkt ... 342
b) Haftungsprivilegierungen als systematisches Argument gegen aktive Überwachungspflicht ... 343
c) Telos: Effektiver Grundrechtsschutz und weiter Handlungsspielraum der Plattformbetreiber ... 345
3. Satzung i.S.v. § 96 MStV als Konkretisierungsinstrument ... 347
4. Mögliche Umsetzungsmaßnahmen ... 348
a) Minimalanforderung: Implementierung einer Kennzeichnungsfunktion ... 348
b) Eigene Kennzeichnungspflicht ab Kenntnis (Notice-and-disclosure) ... 349
c) Fakultative Maßnahmen ... 350
5. Bewertung: Sinnvoller Regulierungsansatz mit Konkretisierungsbedarf ... 351
a) Verhältnismäßigkeit der Plattformverantwortlichkeit ... 351
b) Kein falscher Anreiz zum „Overblocking“ ... 353
c) Konkretisierungsauftrag der Landesmedienanstalten und Grenzen des Regulierungsansatzes ... 354
III. Zwischenergebnis ... 356

C. Regulierungsperspektiven de lege ferenda ... 357
I. Vermeidung von eingriffsintensiven Verboten ... 357
1. Verbot automatisierter Kommunikation in sozialen Netzwerken ... 358
2. Einschränkung anonymer Kommunikation durch Klarnamen- oder Identifizierungspflicht ... 359
a) Klarnamenpflicht ... 360
b) Identifizierungspflicht ... 361
II. Politische Parteien als potenzielle Regulierungsadressaten ... 365
III. Erweiterte Transparenzpflichten für die Betreiber sozialer Netzwerke ... 367

IV. Regulierungsbestrebungen auf EU-Ebene 369
1. Digital Services Act: Compliance-Mechanismus zum Schutz vor „systemischen Risiken“ 370
a) Adressaten: Sehr große Online-Plattformen 371
b) Der Einsatz von Social Bots als systemisches Risiko 371
c) Die einzelnen Pflichten: Risikobewertung, Risikominderung, Prüfung, Transparenz 372
d) Bewertung und Vergleich mit dem Regulierungskonzept des Medienstaatsvertrags 374
2. Artificial Intelligence Act: Kennzeichnungspflicht für „intelligente“ Kommunikationssysteme 376
D. Zwischenergebnis, resilienzfördernde Maßnahmen und Restrisiko ... 378

Zusammenfassende Thesen 381

Literaturverzeichnis 387

Sachverzeichnis 411

Einleitung

A. Anlass der Untersuchung: Social Bots als Sinnbild kommunikativer Veränderungen

Das Grundrecht auf freie Meinungsäußerung ist als unmittelbarster Ausdruck der menschlichen Persönlichkeit in der Gesellschaft eines der vornehmsten Menschenrechte überhaupt […]. Für eine freiheitlich-demokratische Staatsordnung ist es schlechthin konstituierend, denn es ermöglicht erst die ständige geistige Auseinandersetzung, den Kampf der Meinungen, der ihr Lebenselement ist.[1]

Dieser prägnante Ausspruch zum Verhältnis von Meinungsfreiheit und Demokratie besitzt über 60 Jahre nach der wegweisenden Lüth-Entscheidung des Bundesverfassungsgerichts vom 15. Januar 1958 nach wie vor Gültigkeit. Ein demokratisches System ist auf die kommunikative Partizipation der Bürgerinnen und Bürger angewiesen.[2] Allerdings bekommt das Bild des demokratiefördernden Diskurses gerade in jüngerer Vergangenheit immer mehr Risse. Insbesondere in digitalen Kontexten zeigt sich: Kommunikative Freiheiten eröffnen auch Raum für missbräuchliche Verhaltensweisen, die eine freiheitlich-demokratische Staatsordnung nicht fördern, sondern ihre Funktionsbedingungen schleichend untergraben.

Dass die Digitalisierung einen tiefgreifenden gesellschaftlichen Wandel angestoßen hat, ist inzwischen kaum mehr als eine Plattitüde.[3] Digitale Technologie durchdringt beinahe jeden Lebensbereich und rekonfiguriert das wirtschaftliche, politische und soziale Zusammenleben auf vielfältige Weise. Besonders deutlich offenbart sich dieser Veränderungsprozess im Kontext zwischenmenschlicher Kommunikation. Die informationstechnologischen Innovationspotenziale schlagen sich in einem „digitalen Strukturwandel der Öffentlichkeit" nieder.[4]

---

[1] BVerfGE 7, 198 (208).

[2] Allein aus Gründen der besseren Lesbarkeit wird im Folgenden das generische Maskulinum verwendet und auf geschlechtsspezifische Formulierungen verzichtet. Alle personenbezogenen Bezeichnungen beziehen sich auf beide Geschlechter gleichermaßen.

[3] Exemplarisch zum Begriff der Digitalisierung *Peuker*, Verfassungswandel durch Digitalisierung, S. 17: „Digitalisierung dient […] als Chiffre für einen umfassenden gesellschaftlichen und kulturellen Wandel, der durch die Entwicklung neuer digitaler informations- und kommunikationstechnischer Systeme angestoßen wurde und der sich im Bedeutungszuwachs dieser Systeme für die private und die öffentliche Kommunikation manifestiert."

[4] Mit dieser Formulierung etwa *Thiel*, in: Heinrich-Böll-Stiftung (Hrsg.), Stichworte zur

Während die klassischen Massenmedien ihre Monopolstellung als Gatekeeper der öffentlichen Meinungsbildung verlieren, gewinnen neue Kommunikations- und Informationsformen zunehmend an Bedeutung.[5] Eine zentrale Rolle spielen in diesem Zusammenhang die sozialen Netzwerke. Die durch sie eröffneten Interaktions- und Vernetzungsmöglichkeiten wirken sich in erheblicher Weise auf das kommunikative Ökosystem der demokratischen Gesellschaft aus.

Dabei handelt es sich um einen ambivalenten Vorgang. Auf der einen Seite erweitern die niedrigen Zugangshürden und der Optionenreichtum digitaler Kommunikation die Partizipationschancen: Jede Person, die Zugang zum Internet hat, kann nicht nur auf eine Fülle an Informationen zugreifen, sondern als Kommunikator einen großen Adressatenkreis erreichen und so zum Faktor der öffentlichen Meinungsbildung werden. Auf der anderen Seite entstehen neue Missbrauchs- und Eskalationpotenziale:[6] Die sozialen Netzwerke werden zum Forum von Desinformations- und Manipulationskampagnen. Illegale Inhalte, Hassbotschaften und Falschnachrichten verbreiten sich in rasantem Tempo. Und neue Beeinflussungsinstrumente führen zu Machtungleichgewichten im kommunikativen Wettstreit. Die Risiken digitaler Kommunikationsformen manifestieren sich in Autonomie- und Persönlichkeitsrechtsverletzungen des Individuums. Zugleich besitzen sie jedoch auch eine überindividuelle, gesellschaftliche Dimension: Durch sie wird die Integrität des Kommunikationsprozesses als Strukturelement des demokratischen Systems zunehmend auf die Probe gestellt.[7]

Paradigmatisch für die kommunikativen Veränderungen und die damit einhergehenden Risiken steht das Phänomen der Social Bots. Dabei handelt es sich um automatisierte Profile in sozialen Netzwerken, die unter Vortäuschung einer menschlichen Identität am digitalen Kommunikationsprozess teilnehmen.[8] Diesen pseudomenschlichen Kommunikationsteilnehmern wird nachgesagt, dass sie die öffentliche Meinungsbildung verzerren und so den politischen Wettbewerb sabotieren können. Sie sollen etwa im Rahmen des Präsidentschaftswahlkampfs in den Vereinigten Staaten im Jahr 2016 sowie vor dem Brexit-Referendum im Vereinigten Königreich zu Manipulationszwecken eingesetzt worden sein.[9] Spä-

---

Zeit, S. 197 (197); *Schliesky*, NVwZ 2019, S. 693 (696); *Hoffmann-Riem*, AöR 137 (2012), S. 509 (517); *Fehling/Leymann*, AfP 2020, S. 110 (110). Angelehnt ist diese Beschreibung an den von *Habermas* postulierten „Strukturwandel der Öffentlichkeit", siehe *Habermas*, Strukturwandel der Öffentlichkeit. Näher zum digitalen Strukturwandel der Öffentlichkeit siehe unter Teil 3.A.I.3.

[5] Siehe nur *Lobigs/Neuberger*, Meinungsmacht im Internet, S. 88.

[6] So *Ingold*, Der Staat 56 (2017), S. 491 (515 ff.).

[7] Zur „diskursiven Integrität" als Voraussetzung demokratischer Herrschaft siehe *Schimmele*, Staatliche Verantwortung für diskursive Integrität in öffentlichen Räumen, S. 170 ff.

[8] Zur Definition von Social Bots siehe unter Teil 1.A.I.2.

[9] Zum Einsatz von Social Bots im US-Wahlkampf 2016 siehe etwa *Bessi/Ferrara*, First Monday 21 (2016), Ausg. 11; *Kollanyi* u.a., Bots and Automation over Twitter during the U.S. Election, COMPROP Data Memo 2016.4, abrufbar unter: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/89/2016/11/Data-Memo-US-Election.pdf (4.11.2023), S. 2 ff.;

testens seit diesen prominenten Beeinflussungsversuchen steht das Kommunikationsinstrument der Social Bots immer wieder im Fokus der öffentlichen Aufmerksamkeit. Die Risiken automatisierter Manipulationskampagnen werden nicht nur medial kontrovers diskutiert, sondern sie sind Gegenstand der politischen Debatte und zunehmend auch von Regulierungsvorhaben.[10] In Deutschland gilt seit Inkrafttreten des Medienstaatsvertrags[11] eine Kennzeichnungspflicht für Social Bots (§§ 18 Abs. 3, 93 Abs. 4 MStV).

Aus (rechts-)wissenschaftlicher Perspektive ist das Phänomen der Social Bots von besonderem Interesse, weil sich in ihm wesentliche Konfliktlinien des digitalen Strukturwandels der Öffentlichkeit spiegeln. Social Bots heben sich durch ihr spezifisches Manipulationspotenzial von anderen Formen der Meinungsbeeinflussung ab. Charakteristisch ist dabei das Zusammenspiel von Automatisierung und Täuschung: Eine manipulative Qualität gewinnt das Kommunikationsinstrument durch das eingesetzte Täuschungselement. Social Bots operieren unter gefälschten Profilen und verschleiern die Tatsache, dass die Kommunikation automatisiert abläuft. Sie werden von anderen Nutzern sozialer Netzwerke also nicht als computergesteuerte Anwendung, sondern als menschliche Kommunikationspartner wahrgenommen. Auf Grund dieser täuschungsbasierten Authentizität sind Social Bots geradezu prädestiniert, um als Manipulationsinstrument eingesetzt zu werden und die öffentliche Meinung in eine bestimmte

---

Woolley/*Guilbeault*, Computational Propaganda in the United States of America: Manufacturing Consensus Online, abrufbar unter: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2017/06/Comprop-USA.pdf (4.11.2023), S. 14 ff.; *Badawy* u.a., Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, S. 258 (259 ff.). Zum Brexit-Referendum siehe *Howard*/*Kollanyi*, Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum, COMPROP Research Note 2016.1, abrufbar unter: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2016/06/COMPROP-2016-1.pdf (4.11.2023), S. 3 f.; *Bastos*/*Mercea*, Social Science Computer Review 37 (2019), Ausg. 1, S. 38 (44 ff.).

[10] Exemplarisch zu der mitunter hitzigen medialen Debatte siehe nur *Gallwitz*/*Kreil*, Die Mär von „Social Bots", abrufbar unter: https://background.tagesspiegel.de/digitalisierung/die-maer-von-social-bots (4.11.2023) sowie die Replik von *Klinger*, Social Bots: Realität digitaler Öffentlichkeit, abrufbar unter: https://background.tagesspiegel.de/digitalisierung/social-bots-realitaet-digitaler-oeffentlichkeit (4.11.2023). Zu den politischen Initiativen in Deutschland siehe etwa der Antrag der Bundestagsfraktion Bündnis 90/Die Grünen vom 4.4.2017, Transparenz und Recht im Netz – Maßnahmen gegen Hasskommentare, „Fake News" und Missbrauch von „Social Bots", BT-Drs. 18/11856; Bericht der Länderarbeitsgruppe „Social Bots", September 2017, abrufbar unter: https://fragdenstaat.de/anfrage/abschlussbericht-der-landerarbeitsgruppe-zu-social-bots (4.11.2023), S. 5 ff.; Antrag des Landes Hessen vom 16.10.2018, Entschließung des Bundesrates zu Transparenz und klaren Regeln auf digitalen Märkten, BR-Drs. 519/18. Zur Regulierung von Social Bots im US-Bundesstaat Kalifornien siehe Senate Bill 1001, Chapter 892, abrufbar unter: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001 (4.11.2023) sowie die Analyse von *Stricke*, Vanderbilt Journal of Entertainment and Technology Law 22 (2020), S. 841 (845 ff.).

[11] Staatsvertrag zur Modernisierung der Medienordnung in Deutschland vom 28.4.2020 (in Kraft getreten am 7.11.2020).

Richtung zu lenken. Durch die Automatisierung kommunikativer Abläufe lassen sich erhebliche Quantitätssteigerungen erreichen. Digitale Inhalte können anhand bestimmter Parameter massenweise erstellt und in beliebiger Frequenz verbreitet werden. So sind Social Bots in der Lage, künstliche Mehrheiten zu erzeugen, gesellschaftlichen Rückhalt zu simulieren oder fremde Kommunikationskanäle zu blockieren.

Angesichts der neuartigen Risiken, die mit dem Einsatz digitaler Manipulationsinstrumente einhergehen, müssen die normativen Grundlagen demokratischer Öffentlichkeit neu vermessen werden. Die Verfassungsordnung steht dabei vor der Herausforderung, kommunikative Freiheit und Innovationsoffenheit zu gewährleisten, ohne dass die „geistige Auseinandersetzung, [der] Kampf der Meinungen", zur Farce verkommt.

B. Zentrale Fragestellungen und Eingrenzung des Untersuchungsumfangs

Das Phänomen der Social Bots wirft viele Fragen auf, von denen im Rahmen dieser Untersuchung nur ein Ausschnitt behandelt werden kann. Ziel ist es, das Kommunikationsinstrument aus einer verfassungsrechtlichen Perspektive einzuordnen.[12] Im Mittelpunkt stehen dabei drei übergeordnete Fragestellungen. Erstens: Genießt der Einsatz von Social Bots verfassungsrechtlichen Schutz? Zweitens: Mit welchen verfassungsrechtlich relevanten Interessen steht der Einsatz von Social Bots im Konflikt? Drittens: Durch welche Regulierungsinstrumente lässt sich das verfassungsrechtliche Spannungsverhältnis (bestmöglich) auflösen?

Es wird also ein (verfassungs-)normativer Zugriff gewählt. Mit dieser Weichenstellung ist bereits die erste Einschränkung des Untersuchungsumfangs vorgezeichnet: Zu den – komplexen und bei weitem nicht abschließend geklärten – deskriptiven Fragen, die das Kommunikationsinstrument der Social Bots aufwirft, kann und will diese Untersuchung keinen eigenen Beitrag leisten. Die Klä-

[12] Zum verfassungsrechtlichen Kontext von Social Bots siehe auch die Beiträge von *Laude*, Automatisierte Meinungsbeeinflussung, S. 141 ff.; *Iben*, Staatlicher Schutz vor Meinungsrobotern, S. 121 ff., 166 ff.; *Krüper*, in: Unger/v. Ungern-Sternberg (Hrsg.), Demokratie und Künstliche Intelligenz, S. 67 (72 ff.); *v. Ungern-Sternberg*, in: Unger/v. Ungern-Sternberg (Hrsg.), Demokratie und Künstliche Intelligenz, S. 3 (14 ff.); *Iben*, in: Greve u.a. (Hrsg.), Der digitalisierte Staat, S. 155 (159 ff.); *Semizoglu*, in: Hetmank/Rechenberg (Hrsg.), Recht im Umbruch?, S. 79 (84 ff.); *Milker*, ZUM 2017, S. 216 (217 ff.); *Dankert/Dreyer*, K&R 2017, S. 73 (74 ff.); *Schröder*, DVBl. 2018, S. 465 (466 ff.); *Steinbach*, ZRP 2017, S. 101 (102 ff.); *Liesem*, in: Litschka/Krainer (Hrsg.), Der Mensch im digitalen Zeitalter, S. 183 (188 ff.); *Löber/Roßnagel*, MMR 2019, S. 493 (496 f.); *Brings-Wiesen*, Meinungskampf mit allen Mitteln und ohne Regeln?, abrufbar unter: https://www.juwiss.de/93-2016 (4.11.2023); *Zumkeller-Quast*, Die Nutzung von Social Bots als Identitätstäuschung, abrufbar unter: https://www.juwiss.de/2-2017 (4.11.2023).

rung, in welchem Umfang Social Bots tatsächlich eingesetzt werden, wie sie sich konkret auf die individuelle und öffentliche Meinungsbildung auswirken und welche Effekte ihr Einsatz auf politische Ergebnisse hat, muss anderen Disziplinen vorbehalten bleiben. Gleichwohl werden die empirischen Ergebnisse, die insbesondere die Informatik-, Kommunikations- und Politikwissenschaften in diesem Kontext bereithalten, herangezogen, um die verfassungsrechtlichen Wertungen auf ein möglichst solides Tatsachenfundament zu stellen.

Eine weitere Eingrenzung ergibt sich aus dem zugrundegelegten normativen Rahmen. Analysemaßstab dieser Untersuchung ist das Grundgesetz der Bundesrepublik Deutschland. Auf andere Verfassungsordnungen und Grundrechtskataloge – wie etwa die Charta der Grundrechte der Europäischen Union, die Europäische Menschenrechtskonvention oder die Allgemeine Erklärung der Menschenrechte – wird nur am Rande eingegangen. Gleichwohl lassen sich viele der in dieser Arbeit entwickelten Gedanken und Ergebnisse abstrahieren und auf andere Rechtsordnungen übertragen.

Schließlich erfolgt auch in inhaltlicher bzw. thematischer Hinsicht eine Eingrenzung des Untersuchungsumfangs. Der Fokus liegt auf den Implikationen, die der Einsatz von Social Bots für den politischen Prozess mit sich bringt. Untersucht werden also normative Konflikte, die sich dem übergeordneten Kontext der demokratischen Meinungsbildung zuordnen lassen. Andere verfassungsrechtlich relevante Interessenlagen, auf die sich das Manipulationspotenzial (mittelbar) auswirken kann, sind dagegen nicht Gegenstand dieser Untersuchung.[13] Gänzlich ausgeklammert wird außerdem der Fragenkomplex, wie Manipulationsversuche einzuordnen sind, die von ausländischen Hoheitsträgern ausgehen.[14]

C. Gang der Untersuchung

Die Arbeit gliedert sich in vier Teile. Im *ersten Teil* wird – unter Berücksichtigung der relevanten Nachbarwissenschaften – der Untersuchungsgegenstand präzisiert. Nach einer Darstellung des in dieser Arbeit zugrundegelegten Begriffsverständnisses wird insbesondere auf den technischen Hintergrund und die Funktionsweise von Social Bots eingegangen. Anschließend soll es darum gehen, wie Social Bots politische Prozesse beeinflussen. Dafür werden konkrete Einsatzbeispiele aufgeführt. Vor allem aber sollen die verwendeten Manipulationsstrategien

[13] Man denke etwa an die durch Art. 12 Abs. 1 GG geschützten wirtschaftlichen Interessen, die berührt sein können, wenn Social Bots eingesetzt werden, um Wettbewerbsvorteile zu erlangen. Auch mit Blick auf das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) kann es zu verfassungsrechtlichen Spannungen kommen, wenn z.B. ehrverletzende Inhalte durch das Kommunikationsinstrument der Social Bots verbreitet werden.

[14] Siehe dazu etwa *Steinbach*, ZRP 2017, S. 101 (104), der auf eine mögliche Verletzung des völkerrechtlichen Einmischungsverbots hinweist.

beschrieben und systematisiert werden. Abgerundet wird der erste Teil der Arbeit mit einer Einordnung der tatsächlichen Relevanz: Die Effekte, die Social Bots auf das demokratische System haben, sind zwar schwer messbar und mit empirischen Unschärfen verbunden. Trotzdem steht das Kommunikationsphänomen für eine neue Qualität politischer Manipulation.

Der *zweite Teil* der Arbeit widmet sich der Frage, ob der Einsatz von Social Bots durch die Meinungsäußerungsfreiheit (Art. 5 Abs. 1 S. 1 Var. 1 GG) geschützt ist. Angesichts der Autonomiezuwächse technischer Systeme wird im Rahmen des persönlichen Schutzbereichs erörtert, ob eine Ausweitung der Grundrechtsberechtigung auf „maschinelle Personen" verfassungsrechtlich zulässig und rechtspolitisch zu begrüßen wäre. Der Fokus liegt jedoch auf der Untersuchung des sachlichen Schutzbereichs. Dabei sind drei Fragen von besonderem Interesse: Unter welchen Voraussetzungen genießen automatisierte Kommunikationsakte verfassungsrechtlichen Schutz? Greift die Meinungsfreiheit auch bei anonymen Äußerungen? Und wie wirkt sich das für Social Bots charakteristische Täuschungselement auf den grundrechtlichen Schutz aus?

Der *dritte Teil* beleuchtet die verfassungsrechtlichen Interessen, die durch den Einsatz von Social Bots beeinträchtigt werden. Das Konfliktpotenzial schlägt sich in unterschiedlichen Normenkomplexen nieder. Zunächst wird auf die Wahlrechtsgrundsätze (Art. 38 Abs. 1 S. 1 GG) sowie subjektiv-individuelle Grundrechtspositionen eingegangen. Von zentraler Bedeutung ist sodann die objektive Dimension der Meinungsfreiheit: Sie schützt den öffentlichen Meinungsbildungsprozess als kollektives Unterfangen der demokratischen Gemeinschaft. Ihr lässt sich auch der Grundsatz der kommunikativen Chancengleichheit entnehmen, der beim Einsatz illegitimer Manipulationsmittel verletzt wird. Schließlich werden die normativen Rahmenbedingungen präzisiert, die für staatliche Stellen und politische Parteien gelten, wenn sie sich kommunikativ betätigen. In beiden Akteurskonstellationen greifen besondere Restriktionen, die es bei einer verfassungsrechtlichen Einordnung des Social Bot-Phänomens zu berücksichtigen gilt.

Der *vierte Teil* der Arbeit befasst sich mit der Regulierung von Social Bots. Die Untersuchung erfolgt in drei Schritten: Zuerst wird ein Blick auf die Selbstregulierung der Plattformbetreiber geworfen. Daraufhin wird der in Deutschland geltende rechtliche Rahmen näher beleuchtet. Bei der Kombination aus Kennzeichnungspflicht (§ 18 Abs. 3 MStV) und Plattformverantwortlichkeit (§ 93 Abs. 4 MStV) handelt es sich zwar grundsätzlich um einen risikoadäquaten Regulierungsansatz. Es bleibt jedoch Nachbesserungspotenzial. Abschließend wird deshalb auf Regulierungsperspektiven eingegangen, die *de lege ferenda* eine Rolle spielen könnten.

Teil 1

Untersuchungsgegenstand: Social Bots – ein neues Instrument digitaler Manipulation

Um die Grundlage für die spätere verfassungsrechtliche Analyse zu legen, gilt es zunächst, den Untersuchungsgegenstand zu präzisieren. Im Folgenden wird deshalb ein Blick auf die Eigenschaften und Funktionsmechanismen von Social Bots geworfen. Insbesondere soll dargestellt werden, wie sie im politischen Kontext eingesetzt werden können, um die öffentliche Meinungsbildung zu manipulieren. Ziel ist es, das Missbrauchspotenzial sichtbar zu machen und den Blick für die normativen Konfliktlinien zu schärfen.

A. Social Bots als pseudomenschliche Kommunikationsteilnehmer innerhalb sozialer Netzwerke

Mit dem Phänomen der Social Bots hat sich eine neue Gattung pseudomenschlicher Kommunikationsteilnehmer entwickelt. Es handelt sich dabei um automatisierte Profile in sozialen Netzwerken, die unter Vortäuschung einer menschlichen Identität am öffentlichen Diskurs im Internet teilnehmen. Moderne Social Bots sind nicht nur in der Lage, innerhalb der sozialen Netzwerke menschenähnlich zu kommunizieren, sondern sie sind durch die Ausgestaltung ihrer Profile und Handlungsmuster auch kaum noch von menschlichen Akteuren zu unterscheiden. Mit ihren spezifischen Eigenschaften stellen Social Bots ein Medium dar, durch das Inhalte effektiv in der öffentlichen Debatte positioniert und verbreitet werden können. Das Einsatzspektrum von Social Bots ist vielfältig und reicht von positiven Verwendungsmöglichkeiten bis hin zu evident missbräuchlichen und schädlichen Nutzungsformen.

I. Begriffsklärung

Die wissenschaftliche Untersuchung von Social Bots befindet sich noch in einem Anfangsstadium und ist dementsprechend mit vielen Unsicherheiten behaftet. Schon zu der grundsätzlichen Frage, was unter dem Begriff überhaupt zu verstehen ist, herrscht keine Einigkeit. Vielmehr wird er in der aktuellen Debatte – je

nach Kontext und individuellem Begriffsverständnis – für unterschiedliche Phänomene verwendet.[1] Um Social Bots einer verfassungsrechtlichen Untersuchung unterziehen zu können, ist daher eine terminologische Eingrenzung und Präzisierung des Untersuchungsgegenstandes unerlässlich.

1. Bot-Technologie und die Automatisierung digitaler Aufgaben

Social Bots sind eine bestimmte Form von Software-Robotern. Solche digitalen Helfer werden inzwischen in den unterschiedlichsten Lebensbereichen zur Automatisierung von Routineaufgaben verwendet. Die Entwicklung von Bots ist im Zeitalter der Digitalisierung ein zentrales Innovationsfeld und profitiert insbesondere von technologischen Fortschritten im Bereich der künstlichen Intelligenz.

Bei der Bezeichnung „Bot" handelt es sich um eine Abkürzung des englischen Begriffs robot (deutsch: Roboter).[2] Im Bereich der Robotik wird grundsätzlich zwischen Hardware- und Software-Robotern differenziert – die Kurzform Bot steht dabei für letztere Gruppe.[3] Dieser Einteilung entsprechend versteht man in der Informationstechnologie unter einem Bot ein (weitgehend) autonom[4] agierendes Computerprogramm, das zur automatisierten Durchführung vordefinierter Aufgaben eingesetzt wird.[5] Dabei steht der Bot mit seiner Umwelt und anderen Software-Agenten in Verbindung und ist in der Lage, mit ihnen zu interagieren.[6]

---

[1] Vgl. *Grimme* u.a., Social Bots: Human-Like by Means of Human Control?, abrufbar unter: https://arxiv.org/pdf/1706.07624.pdf (4.11.2023), S. 2, 5.

[2] *Ferrara* u.a., Communications of the ACM 59 (2016), S. 96 (96); *Kind* u.a., Social Bots, S. 11.

[3] Vgl. *Ferrara* u.a., Communications of the ACM 59 (2016), S. 96 (96); *Howard* u.a., Journal of Information Technology & Politics 15 (2018), S. 81 (82 f.). Mitunter werden auch die Begriffe Softbot oder Software-Agent synonym verwendet, vgl. *Russell/Norvig*, Artificial Intelligence, S. 41; *Röttgen/Juelicher*, in: Taeger (Hrsg.), Recht 4.0, S. 227 (228).

[4] Der Begriff der Autonomie wird in dieser Arbeit nicht in einem absoluten Sinn verwendet, sondern vielmehr als eine „graduelle Eigenschaft" aufgefasst, so auch *Zech*, in: Gless/Seelmann (Hrsg.), Intelligente Agenten und das Recht, S. 163 (171). Auch durch einen Algorithmus gesteuerte Computerprogramme mit einem gewissen Komplexitätsgrad werden deshalb als (teil-)autonom bezeichnet.

[5] Siehe insbesondere die technischen Standards ISO/IEC-Norm 27032:2012(en), Information technology – Security techniques – Guidelines for cybersecurity, unter 4.12: „Automated software program used to carry out specific tasks"; ISO-Norm 19731:2017(en), Digital analytics and web analyses for purposes of market, opinion and social research, unter 3.7: „Autonomous software that operates as an agent for a user or a program or simulates a human activity". Aus der Literatur siehe etwa *Graeff*, What We Should Do Before the Social Bots Take Over: Online Privacy Protection and the Political Economy of Our Near Future, abrufbar unter: https://dspace.mit.edu/handle/1721.1/123463 (4.11.2023), S. 2; *Röttgen/Juelicher*, in: Taeger (Hrsg.), Recht 4.0, S. 227 (228); *Abokhodair* u.a., The 18th ACM conference on CSCW (2015), S. 839 (840).

[6] Richtlinie VDI/VDE 2653, Blatt 1; *Röttgen/Juelicher*, in: Taeger (Hrsg.), Recht 4.0, S. 227 (228); *Kirn/Müller-Hengstenberg*, MMR 2014, S. 225 (227).

Die Entwicklung von Bots dient der Automatisierung und damit der Vereinfachung digitaler Aufgaben. Ursprünglich wurde die Bot-Technologie vor allem von Anbietern digitaler Plattformen zur Optimierung der eigenen Dienstleistungen eingesetzt. Beispiele sind Web Crawler-Bots, die von Suchmaschinen verwendet werden, um das Internet anhand bestimmter Kriterien nach digitalen Inhalten zu durchsuchen,[7] oder sogenannte Wikipedia-Bots, die zu Wartungszwecken und teilweise sogar zur Editierung von Inhalten der Online-Enzyklopädie eingesetzt werden.[8] Während solche Softwareanwendungen zumeist im Hintergrund agieren, treten moderne Bots zunehmend in eine direkte Interaktion mit dem Benutzer. Sie sind mit einer Sprachverarbeitungssoftware ausgestattet und können mit Menschen in Dialogform kommunizieren.[9]

Inzwischen kommt die Bot-Technologie in den unterschiedlichsten Bereichen zum Einsatz.[10] Chatbots automatisieren in vielen Bereich den Kundenservice und versprechen nicht nur Effizienzgewinne, sondern gewährleisten auch eine ständige Erreichbarkeit. Andere Programme assistieren bei Übersetzungen[11] oder versorgen den Benutzer mit aktuellen Wettervorhersagen.[12] Die technischen Möglichkeiten, die mit der Automatisierungstechnologie einhergehen, eröffnen jedoch auch Missbrauchspotenzial.[13] Beispiele für Bots mit einer schädlichen Zweckrichtung sind sogenannte Cheatbots, die im Rahmen von Computerspielen zur Manipulation des Spielgeschehens eingesetzt werden, oder Spambots, mit deren Hilfe große Mengen unerwünschter Nachrichten verbreitet werden können.[14]

Unabhängig von dem jeweils verfolgten Einsatzzweck ist die Bot-Technologie ein sehr dynamisches Entwicklungsfeld und wird von führenden Technologieunternehmen als Trend ausgerufen.[15] Dies liegt zum einen daran, dass die fort-

---

[7] *Graeff*, What We Should Do Before the Social Bots Take Over: Online Privacy Protection and the Political Economy of Our Near Future, abrufbar unter: https://dspace.mit.edu/handle/1721.1/123463 (4.11.2023), S. 2.

[8] *Leistert*, in: Seyfert/Roberge (Hrsg.), Algorithmuskulturen, S. 215 (222 ff.). Eine Liste der auf Wikipedia eingesetzten Bots findet sich unter: https://de.wikipedia.org/wiki/Wikipedia:Bots/Liste_der_Bots (4.11.2023).

[9] *Röttgen/Juelicher*, in: Taeger (Hrsg.), Recht 4.0, S. 227 (227).

[10] Mit einer Auflistung unterschiedlicher Anwendungsbeispiele *Harringer*, Information – Wissenschaft & Praxis 69 (2018), S. 257 (260).

[11] So etwa der Discord Translator bot, siehe unter: https://nvu.io/en/bots/discord-translator (4.11.2023).

[12] Vgl. *Edwards* u.a., Computers in Human Behavior 33 (2014), S. 372 (372).

[13] Eine Differenzierung zwischen gut- und bösartigen *Bots* kritisiert etwa *Leistert*, in: Seyfert/Roberge (Hrsg.), Algorithmuskulturen, S. 215 (220 f.).

[14] *Röttgen/Juelicher*, in: Taeger (Hrsg.), Recht 4.0, S. 227 (232 ff.).

[15] So hat etwa der CEO von Microsoft Satya Nadella bereits im Jahr 2016 angekündigt, dass „Bots die neuen Apps" seien, siehe dazu *della Cava*, Microsoft CEO Nadella: „Bots are the new apps", abrufbar unter: https://eu.usatoday.com/story/tech/news/2016/03/30/microsof-ceo-nadella-bots-new-apps/82431672 (4.11.2023). Siehe auch *Leistert*, in: Seyfert/Roberge (Hrsg.), Algorithmuskulturen, S. 215 (220); *Hegelich*, Analysen & Argumente 2016, Ausg. 221, S. 2.

schreitende Digitalisierung immer mehr Anwendungsfelder für diesen Technologiezweig erschließt.[16] Denn je mehr Lebensbereiche digitalisiert werden, desto größer ist der Bedarf an Automatisierungsprozessen. Zum anderen führen die Fortschritte der Software- und Hardware-Technologie dazu, dass sich die Leistungsfähigkeit automatisierter Anwendungen kontinuierlich steigert. Insbesondere durch die Implementierung von technischen Innovationen aus dem Bereich der künstlichen Intelligenz erlebt die Bot-Technologie erhebliche Entwicklungssprünge.[17] Durch die Programmierung von Bots können daher immer mehr und vor allem komplexere Aufgaben bewältigt werden.

2. Arbeitsdefinition

Als Ausprägung der skizzierten Automatisierungsentwicklung handelt es sich bei Social Bots also um (teil-)autonom agierende Computerprogramme. In einem nächsten Schritt stellt sich die Frage, durch welche spezifischen Eigenschaften sich Social Bots definieren und von anderen Software-Agenten unterscheiden. Diesbezüglich existiert mittlerweile eine breite Variation an Definitionsansätzen, die sich teilweise erheblich voneinander unterscheiden.[18] Bei dem Ausdruck Social Bot handelt es sich derzeit somit eher um „eine Mischung aus empirischem Befund und politischer Interpretation“[19] als um einen feststehenden wissenschaftlichen Terminus. Im Rahmen dieser Arbeit werden zwei Definitionsmerkmale zugrundegelegt, die sich in den meisten der bisherigen Begriffsklärungen wiederfinden: Erstens nehmen Social Bots am Kommunikationsprozess im Internet teil und zweitens verschleiern sie dabei ihre Identität als automatisierte Anwendung.

Nähert man sich dem Begriff auf sprachlicher Ebene, wird deutlich, dass er anfällig für Fehlinterpretationen ist. Denn das Adjektiv „social“ (deutsch: sozial) hat entsprechend seines lateinischen Ursprungs (*socialis*) im allgemeinen Sprachgebrauch unterschiedliche Bedeutungen.[20] Unter anderem dient es dazu, ein Individuum als gesellig und kommunikationsfreudig zu beschreiben. Dieser Bedeutung entsprechend zeichnen sich Social Bots in erster Linie dadurch aus, dass sie aktiv an kommunikativen Prozessen im Internet teilnehmen. Darüber hinaus lässt sich der Begriff Social Bot auch als Referenz zu ihrem primären Einsatzort

---

[16] Den Zusammenhang zwischen Digitalisierung und Bot-Technologie benennen auch *Hwang* u.a., Interactions 19 (2012), Ausg. 2, S. 38 (40); *Guilbeault*, International Journal of Communication 10 (2016), S. 5003 (5007).

[17] *Kind* u.a., Social Bots, S. 16.

[18] Zu den unterschiedlichen Definitionsansätzen und den bestehenden Mehrdeutigkeiten *Grimme* u.a., Social Bots: Human-Like by Means of Human Control?, abrufbar unter: https://arxiv.org/pdf/1706.07624.pdf (4.11.2023), S. 5 ff.

[19] So *Hegelich*, Die politische Meinung 2017, Ausg. 543, S. 32 (33).

[20] Zur Bedeutungsvielfalt des lateinischen *socialis* siehe etwa *Dänzer*, in: Baier (Hrsg.), Der neue Georges, Band II, Sp. 4425 f.; zum englischen *social* siehe Oxford English Dictionary online, Stichwort: Social (4.11.2023).

Sachverzeichnis

Algorithmus 28, 117
Amtsträger 259 ff., 266
Anonymität 51 f., 251, 270, 293, 358 ff.
– Begriffsklärung 128
– grundrechtlicher Schutz 129 ff.
API 16
Artificial Intelligence Act 376 ff.
Automatisierung 4, 8 ff., 39
– als technisch vermittelte Macht 241 ff.
– grundrechtlicher Schutz 115 ff.
– Meinungsäußerung 124 ff.
– Verwaltungsakt 274
– Willenserklärung 121 ff.
Autonomie 2, 8, 38, 66, 74, 77, 123, 208
– Wählerautonomie 170 ff., 191 ff.

Berufsfreiheit 351 ff.
Bot 8 ff.

Chancengleichheit *siehe* Kommunikative Chancengleichheit
Chat GPT 23
Chatbots 9, 14, 23
Chilling effect 137
Claqueur 246, 249
Cyborgs 14

Deep Fakes 378
Definition 10
Demokratieprinzip 163 ff., 168, 187, 196
Demokratische Öffentlichkeit *siehe* Öffentlichkeit
Demokratischer Wettbewerb 222 ff.
Desinformation 12 f., 98, 313
Digital Services Act 370 ff.
Digitale Manipulation 37 ff.
Digitaler Zwang *siehe* Meinungsfreiheit
Drittwirkung *siehe* Mittelbare Drittwirkung

E-Commerce-Richtlinie 343, 370
Einsatzbeispiele 33
Empirische Unschärfen 47 f., 304, 338 f.
Enttarnung 26 ff., 48, 379
EU-Verhaltenskodex Desinformation *siehe* Selbstregulierung
Ewigkeitsgarantie 69

Facebook 17, 19 f., 316 ff.
Fake News *siehe* Desinformation
Falschnachrichten *siehe* Desinformation
Filterblase 50, 192
Freiheit der Wahl 169 ff.

Gleichheit der Wahl 193 ff.
Grundrechtsberechtigung
– Ausweitung auf technische Systeme 65
– juristische Personen 60 ff.
– natürliche Personen 56 ff.

Haftungsprivilegierung 343 ff., 370
Handlungsspektrum 19
Hate Speech *siehe* Meinungsfreiheit

Identifizierungspflicht 361 ff.
Identitätstäuschung 24 ff., 99 f., 139 ff., 246 ff., 272
Illegitime Meinungsmacht 239 ff.
Informationsfreiheit 202 f.

Kennzeichnungspflicht 325 ff.
Klarnamenpflicht 316 ff., 360

Kommunikative Chancengleichheit 208, 221 ff., 233 ff.
Kommunikatorklarheit 269 ff.
Künstliche Intelligenz 10, 23, 45 f., 67, 72, 120

Legislativer Gestaltungsspielraum 306 ff.

Manipulationsstrategien 39 ff.
Maschinelle Person 67 ff.
Massenmedien 49, 155 ff., 214 f., 230 ff.
Medienfreiheiten 214
Medienkompetenz 26, 380
Medienstaatsvertrag 324 ff.
Meinung 91 ff.
Meinungsbildungsprozess, *siehe* Öffentlichkeit
Meinungsfreiheit
– antizipierte Meinungsäußerung 117 ff.
– demokratiekonstituierende Funktion 217 ff.
– Desinformation als Meinung 90 ff.
– digitaler Zwang 113 ff.
– Formalbeleidigung 100
– Hassrede 100
– objektive Dimension 209 ff.
– persönlicher Schutzbereich 55 ff.
– sachlicher Schutzbereich 78 ff.
– Schmähkritik 100
– Schutzbereichsausnahme bei Social Bots 138 ff.
– technikoffenes Grundrecht 104 f.
– unwahre Tatsachenbehauptungen 94
Meinungskampf 112, 163, 227 ff., 237 ff.
Mikrotargeting 46, 206
Mittelbare Drittwirkung 298 f.

NetzDG 322, 362
Netzneutralität 229
Notice-and-disclosure 349 ff.
Nudging 31

Objektive Dimension der Meinungsfreiheit, *siehe* Meinungsfreiheit
Öffentlichkeit
– Begriff 152
– digitaler Strukturwandel 156
– Funktionen 159
– verfassungsrechtliche Leitplanken 163 ff.
Öffentlichkeit der Wahl 197
One man, one voice 252 ff.

Parteien
– als Regulierungsadressaten 365
– Status der Freiheit 281 ff.
– Status der Gleichheit 284 ff.
– Status der Öffentlichkeit 286 ff.
Partizipation 2, 166 f.
Political Bots 32
Pseudonymität 128 f., 141 f., 246 ff., 292 f.

Recht auf selbstbestimmte Rezeption 203 ff.
Regulierung
– Deutschland 324
– EU 369 ff.
– USA 3, 325
Ressourcentransparenz 294 ff.

Sachlichkeitsgebot 263 ff.
Schutzlücke 67, 73 f., 186
Schutzpflicht des Staates 297
Schweigespirale 42 ff.
Selbstregulierung
– EU-Verhaltenskodex Desinformation 313
– Facebook 316 ff.
– Twitter 318 ff.
Selbstzensur 136 ff., 251, 270, 361
Social Media *siehe auch* Facebook, Twitter
– Funktionen 19 ff.
– Grundrechtlicher Schutz 104
Soft Law 313 f.
Staatliche Kommunikationstätigkeit 256 ff.
Systemische Risiken 370 ff.

Technischer Hintergrund 16
Trolle 13
Twitter 17, 19 f., 106, 318 ff.

Verfassungsrechtliches Leitbild 162 f.
Versammlungsfreiheit 84, 89

Wahlbeeinflussung 173 ff.

Zugang zum Kommunikationsprozess 228 ff.
Zurechnungszusammenhang 67 f., 76, 119 ff., 258 ff.