Der Einsatz von Social Bots im Raum digitaler demokratischer Öffentlichkeit

A. Zugang

I. Ist die Demokratie in Gefahr?

On the internet, nobody knows you're a bot. So könnte die im *New Yorker* erschienene berühmte Karikatur des Zeichners *Peter Steiner* aus dem Jahre 1993, in der zwei Hunde vor einem Computer sitzen und welche mit „On the internet, nobody knows you're a dog." untertitelt ist, umgestaltet werden, um der hier zu behandelnden Thematik gerecht zu werden.[1] Doch dies ist noch weiter zu pointieren. Die dort veranschaulichten Problematiken, die sich um die Anonymität im Internet ranken, haben nicht an ihrer Aktualität verloren, sondern Ausmaße angenommen, welche im Jahre 1993 nicht vorhersehbar waren. Darauf abzielend titelte das *Verge Magazine* nahezu 30 Jahre später treffend: „On the internet, nobody knows you're a human."[2]

Vor über 75 Jahren trat der Parlamentarische Rat in Bonn zusammen und anlässlich dieses Jubiläums sprach der ehemalige Bundespräsident Joachim Gauck von einer damaligen durch das Grundgesetz begründeten Daseinsgewissheit, die es nur theoretisch geben könne, „solange sie nicht praktisch immer wieder bewahrt, geschützt, neu erfunden und mit Leben gefüllt wird".[3] Eine Herausforderung ist der digitale Wandel, der sich in den vergangenen zwei Jahrzehnten in verschiedenen Lebensdomänen Bahn brach: auf dem Arbeitsmarkt, im Konsum, in der Kommunikation. Vernetzung und Digitalisierung waren und sind weiterhin Grundlage, Antrieb und Medium von gesellschaftlichen sowie wirtschaftlichen fließenden Veränderungen und kaskadenartigen Umbrüchen. Dabei sind diese Entwicklungen so ubiquitär, dass darin nicht bloß von einem Fortschreiten der Industrialisierung gesprochen werden kann, sondern vielmehr eine dritte Umwälzung der Menschheitsgeschichte, nach den Übergängen vom Jäger und Sammler zum Ackerbau sowie vom Ackerbau zur Industrialisierung, zu erblicken ist.[4] Teil dieses neuen Zeitalters ist die digitale Manifestierung des Individuums in sozialen Netzwerken, die im „Internet of Everything" mündet.[5] Zunächst beschränkt auf singuläre Lebensbereiche eines bestimmten Adressatenkreises, den einzelne Anbieter abdeckten, setzte sich schließlich eine zielgruppenunabhängige Universalität weniger Intermediäre durch.
Mit der Etablierung der sozialen Netzwerke verlagerte sich der gesellschaftliche Meinungsaustausch zunehmend in das World Wide Web (WWW). Dabei werden sowohl bestehende Kommunikationswege vereinfacht als auch die Grenzen des Kommunikationsumfeldes verschoben. Die Transformation der sozialen Netzwerke von reinen Freizeitportalen zu wirtschaftlichen und gesellschaftlichen Faktoren, bei gleichzeitiger hoher Verbreitung in der Bevölkerung, hat zur Folge, dass eine Dominanz der Intermediäre, wie Facebook, X oder Instagram bei der Verbreitung von Botschaften entstanden ist.

Das Feld des politischen Diskurses stellt ein weiteres Einfallstor digitaler Phänomene dar. Und so wird die politische Kommunikation, sei es inner- oder außerhalb des Wahl-

1 Vgl. Garton Ash, Redefreiheit, 476.
2 Lindsay, On the internet, nobody knows you're a human.
3 Altenbockum, von, Frankfurter Allgemeine Zeitung 2023, 1.
4 Dreier, in: Bizer/Lutterbeck/Rieß, Umbruch von Regelungssystemen in der Informationsgesellschaft: Freundesgabe für Alfred Büllesbach, 65 (65).
5 Hoffmann-Riem, AöR 2017, 1 (5).

kampfes, von digitaler Präsenz geprägt. Die politischen Akteure haben die Vorzüge von unmittelbarer Reaktion und schnellem Agieren, bei gleichzeitiger Ausnutzung von Multiplikatoreffekten, längst erkannt. Dabei führt das Umgehen klassischer Medien als Gatekeeper des öffentlichen Diskurses zu einer ungefilterten Übermittlung der Botschaft.[6] Reichweiten und digitaler Widerhall stellen analoge Medien in den Schatten. Diese Dynamik beeinflusst Meinungsäußerung gleichermaßen wie Meinungsrezeption.

Dieses neue Kommunikationsumfeld, samt den dort vorherrschenden Bedingungen, machen sich Social Bots zunutze, um als „digitale Claquere" „trending Topics" in sozialen Netzwerken zu erzeugen.[7]
Social Bots sind automatisierte Accounts in sozialen Netzwerken. Gesteuert werden diese durch Algorithmen, die vorgeben, unter welchen Voraussetzungen der ferngesteuerte Account in Erscheinung zu treten und in welcher Weise er zu agieren hat. Dabei ist diese Automatisierung nicht nur auf den einzelnen Account bezogen, sondern der Verwender kann beliebig viele Accounts marionettenartig fernsteuern. Bei der 94. Frühjahrskonferenz der Justizministerinnen und Justizminister 2023 wurde die sich aus der Verbreitung von Fakenews unter Verwendung von Social Bots ergebende Bedrohung der Demokratie durch eine Verfälschung des Diskurses besonders thematisiert.[8] Mit dem Hinzutreten dieser digitalen Meinungsroboter ist ein Schritt vollzogen, welcher sich nicht bloß in der Auswechslung des Übertragungsmediums erschöpft, sondern auch die Bedingungen, Akteure und Kräfteverhältnisse neu auslotet. Grundlage jedes demokratischen Prozesses ist der kommunikative Austausch. Die Evolution von Kommunikation setzte in der Vergangenheit mit jedem Entwicklungsschritt bei dem Medium des Diskurses an. Das Konzept von Social Bots macht sich die strukturellen Bedingungen der Digitalisierung zu Nutze, setzt jedoch bei dem Adressanten an und ersetzt den menschlichen Nutzer durch einen automatisierten Account. Diese Substitution kombiniert den geringen Aufwand, in sozialen Netzwerken Reichweiten zu erzielen, mit einem Multiplikatoreffekt auf der Adressatenseite.

In der Gemengelage aus Rechts-, Politik-, Sozialwissenschaften und Informatik sind die Folgen und die etwaigen Gefahren durch die Digitalisierung in den Fokus wissenschaftlicher und gesellschaftlicher Debatten geraten. Typischerweise treten Social Bots bei öffentlichkeitsrelevanten Ereignissen von größerer Bedeutsamkeit in Erscheinung. Dabei werden sie zur Etablierung von Randmeinungen genutzt. Gerade im Kontext des politischen Wahlkampfes stoßen digitale Meinungsmultiplikatoren auf ein empfängliches Umfeld. Erstmals gerieten sie mit der amerikanischen Präsidentschaftswahl im Jahre 2016 in die öffentliche Diskussion und beschäftigen seitdem die Rechtswissenschaft. Es ist schwer vorstellbar, wie Bits und Bytes eine Bedrohung für das über Jahrhunderte gewachsene System der Demokratie, geformt durch Philosophen sowie Rechtsgelehrte und gefestigt durch Verfassungen, darstellen können. Das Phänomen war neu, die Studiendichte gering und in der Öffentlichkeit, den Medien, der Politik und der Wissenschaft erfolgte eine kritische Betrachtung und Bewertung. Seitdem ist die Diskussion nicht abgeflacht, erste Maßnahmen gegen Social Bots wurden getroffen und es bietet sich mit zeitlichem Abstand an, die Lage neu zu sondieren. Der ehemalige Ministerpräsident von Nordrhein-Westfalen, Armin Laschet, warnte in seiner Neujahrsansprache 2020 vor den Gefahren der sog. Filterblasen.[9] Filterblasen sind eine Problematik, die besonders durch das Hinzu-

6 Magen, in: Fragmentierungen, 67 (73); Neuberger, ZUM 2022, 157 (160).
7 Golz, K&R 2017, 30 (30); Dankert, in: Hoffmann-Riem, Big Data – Regulative Herausforderungen, 157 (158).
8 Konferenz der Justizministerinnen und Justizminister, Frühjahrskonferenz am 25. Mai und 26. Mai 2023 – Beschluss TOP II.2, 1.
9 Staatskanzlei Nordrhein-Westfalen, Neujahrsansprache 2020 von Ministerpräsident Armin Laschet | Das Landesportal Wir in NRW.

treten von Social Bots ein noch drastischeres Gefährdungspotential darstellt. Dies wurde besonders im Zusammenhang mit der Coronapandemie deutlich. Dort erlangten Social Bots als digitale Superspreader über COVID-19 zuletzt mediale Aufmerksamkeit.[10] In diesem Kontext wird die Gefährdungslage deutlich. Der analoge zwischenmenschliche Austausch wird durch Kontaktbeschränkungen eingeschränkt. Als Tor zur Teilhabe fungiert das Internet. Gerade dieses Zusammentreffen birgt besondere Brisanz für die hier zu untersuchenden Fragen. Die digitale Isolation und das World Wide Web als eine der primären Informationsquellen bereiten einen fruchtbaren Nährboden, der durch Einflussnahme auf die Meinungsbildung und den Diskurs zur Gefahr für die Demokratie werden kann. Schließlich wurden bei der 94. Frühjahrskonferenz der Justizministerinnen und Justizminister 2023 die sich aus dem Einsatz von Social Bots ergebende Bedrohung der Demokratie durch eine Verfälschung von Diskursgrundlagen hervorgehoben.[11]

II. Herangehensweise

Die rechtlichen Problemfelder bei der Verwendung von Social Bots liegen in der automatisierten und amplifizierten Adressierung einer digitalen Öffentlichkeit. Daher gilt es, vor rechtlichen Überlegungen das Phänomen Social Bots näher zu betrachten und den Kommunikationsraum der digitalen Öffentlichkeit zu beleuchten.
Zunächst ist dazu unter B. eine Definition von Social Bots aufzustellen und zu erörtern, welcher Meinungsstand in der Wissenschaft hinsichtlich der einzelnen Merkmale besteht.
Zur Darstellung, dass es sich nicht um ein rein theoretisches Problem handelt, sind bisherige bedeutsame Einsatzzusammenhänge und ihre Folgen unter C. aufzuzeigen.
Um festzustellen, welche Auswirkungen Social Bots auf den Diskurs und schließlich auf den dort verorteten politischen Wahlkampf haben, sind zunächst ihre Funktions- und Wirkungsweise unter D. herauszuarbeiten. Dafür werden die technischen Grundlagen sowie die Wirkungsweisen von Social Bots in der digitalen Kommunikation erläutert und aufgeführt, welche Möglichkeiten es zu einer Identifizierung von Social Bots nach dem Stand der Technik gibt. Aufgrund der zunehmenden Diskussion um Künstliche Intelligenz wird eine Einordnung vorgenommen und erörtert, welche verschiedenen technischen Prozesse im Rahmen einer Automatisierung zusammenwirken. Dabei ist besonders das Verhältnis und die Abgrenzung von Algorithmen zu Künstlicher Intelligenz von Bedeutung.
Anschließend wird unter E. das Wirkfeld von Social Bots unter rechtlicher, philosophischer und kommunikationswissenschaftlicher Perspektive betrachtet. Dabei werden insbesondere die Zusammenhänge von Demokratie, Öffentlichkeit und Diskurs beleuchtet. Mit der Heranziehung einer deliberativen Demokratietheorie rücken formale staatsorganisatorische Teilhabeprozesse in den Hintergrund, während der Diskurs eine exponierte Stellung einnimmt.[12] Daher kommt eine Beleuchtung dieser Zusammenhänge nicht umhin, im Rahmen der kommunikationswissenschaftlichen Annäherung auf die Phänomene der Schweigespirale, Filterblase und Echokammer einzugehen.
Bevor auf die Besonderheiten der Nutzung durch politische Parteien eingegangen wird, sind die grundrechtlichen Rahmenbedingungen für die Nutzung von Social Bots im Allgemeinen unter F. zu erörtern. Es ist zu prüfen, ob und in welcher Weise die Verwendung von der Meinungsfreiheit nach Art. 5 I 1 Hs. 1 GG erfasst ist und inwieweit im bejahenden Falle eine Verwendung beschränkt werden kann. Dazu wird untersucht, wel-

10 Vgl. Allyn, Researchers; Kanski, A snapshot of social COVID-19 conversations found bots, anti-vaxxers and concerns about medication access.
11 Konferenz der Justizministerinnen und Justizminister, Frühjahrskonferenz am 25. Mai und 26. Mai 2023 – Beschluss TOP II.2, 1.
12 Volkmann, in: Unger/Ungern-Sternberg, Demokratie und künstlicheIntelligenz., 51 (60).

che Einschränkungen von Social Bots auf Grund der aktuellen Gesetzeslage möglich und nötig sind, welche gesetzgeberischen Maßnahmen in der Vergangenheit korrespondierend mit der Thematik getroffen wurden und welche gesetzlichen Initiativen kumulativ sinnvoll erscheinen. Dabei wird insbesondere auf den Zusammenhang zur Rundfunkfreiheit eingegangen.
Schließlich folgt unter G. die Untersuchung zur Nutzung von Social Bots durch politische Parteien im Allgemeinen und im Speziellen in Zeiten des Wahlkampfes. Dabei wird zunächst der Parteienbegriff untersucht und die grundsätzliche Grundrechtsfähigkeit der Parteien dargestellt. Dabei sind die Besonderheiten der Nutzung von Social Bots im Spannungsfeld des Status der Freiheit und des Status der Öffentlichkeit von besonderer Relevanz. Letztlich ist die besondere Situation im Wahlkampf zu betrachten und zu erörtern, ob weitere Anpassungen hinsichtlich der zuvor getroffenen Feststellungen auf Grund der Wahlrechtsgrundsätze des Art. 38 I GG vorzunehmen sind.

III. Rechtliche Problemfelder

Das Wirken von Social Bots im Bereich der öffentlichen Meinungsbildung und damit im „Vorhof des parlamentarischen Komplexes“[13] erschöpft sich nicht bloß in algorithmischen Besonderheiten, sondern wirkt weit hinein in grundrechtliche und staatsorganisatorische Fragestellungen, namentlich insbesondere in die Kommunikationsfreiheiten und die demokratischen Prozesse. Eine besondere Bedeutung erlangt die plebiszitärekommunikative Ebene dieser demokratischen Prozesse. Auf dieser Ebene erhalten Social Bots Zugriff, sodass ihre Folgen auf den kommunikativen Prozess herauszuarbeiten sind. Als Folgen des Einwirkens von Social Bots auf die öffentliche Meinungsbildung werden die Verzerrung des Meinungsbildes, insbesondere im Zusammenhang mit Wahlen, das einseitige Vermitteln von Themen und Fakten, die Fragmentierung der Gesellschaft sowie die Isolation und Polarisierung in sozialen Netzwerken diskutiert.[14]
Rechtlicher Ausgangspunkt ist die rechtstheoretische Frage um das Verhältnis von Verfassung und Verfassungswirklichkeit.
Anschließend ist der Schutzbereich der Meinungsfreiheit zu bestimmen und die Besonderheiten, die sich aus einer Verwendung von Social Bots ergeben, sind herauszuarbeiten und zu problematisieren. Social Bots könnten selbst der Meinungsfreiheit zu unterstellen sein. Damit würde hinsichtlich des personalen Schutzbereichs nicht der jeweilige Verwender der Social Bots, sondern die Social Bots als solche geschützt sein. Dieses geht Hand in Hand mit der Frage, wer Träger von Grundrechten sein kann und ob eine *E-Person* zu etablieren ist, beziehungsweise eines rechtlichen Schutzes bedarf. Daraus erwächst die Folgefrage, welche digitalen Äußerungsformen, beispielsweise das Folgen, das Liken und das Abonnieren, von denen Social Bots Gebrauch machen können, vom Schutzbereich der Meinungsfreiheit erfasst sind. Fraglich ist des Weiteren, ob die unmittelbare Äußerung, die ihre Grundlage in einem Algorithmus hat, auf einen Menschen zurückgeführt werden kann. Dabei ist der Anknüpfungspunkt einer solchen Rückführung zu bestimmen und das Delta zwischen Programmierung und Äußerung zu bewerten. Mit dem Auseinanderfallen von Verwender und Social Bot geht die Frage einher, wie die möglicherweise vorliegende Täuschung über den tatsächlichen Charakter des von Social Bots zugegriffenen Profils zu bewerten ist und ob dieses dem Schutzbereich des Art. 5 I 1 Hs. 1 GG unterfällt. Denn für die Rezipienten solcher automatisierter Kommunikate entsteht der Eindruck, dass ein Mensch dieses unmittelbar erzeugt hat. In diesem Zusammenhang wird ein Vergleich zu unwahren Tatsachenbehauptungen im Lichte der Meinungsfreiheit

13 Habermas, Faktizität und Geltung, 533.
14 Eisenegger, in: Eisenegger/Prinzing/Ettinger/Blum, Digitaler Strukturwandel der Öffentlichkeit: Historische Verortung, Modelle und Konsequenzen, 1 (2 f.).

heranzuziehen und zu bewerten sein, ob durch Social Bots ein Irrtum hervorgerufen werden kann. Des Weiteren ist problematisch, ob die Meinungsfreiheit die Freiheit zu der anonymisierten und pseudonymisierten Meinungsäußerung in sozialen Netzwerken einschließt und welcher Anspruch an die formale Teilhabe in einem öffentlichen Diskurs zu stellen ist. Schließlich ist im Zusammenhang mit dem Schutzbereich der Meinungsfreiheit zu betrachten, ob die durch Social Bots erfolgende quantitative Überhöhung von Meinungen durch die Täuschung von Mehrheitsverhältnissen rechtmäßig ist.
Sollte die Verwendung von Social Bots vom Schutzbereich des Art. 5 I 1 Hs. 1 GG erfasst sein, ist die Rechtfertigung von Eingriffen unter Heranziehung der Schranken des Art. 5 II GG zu beleuchten. Relevant sind in dem zu betrachtenden Zusammenhang insbesondere die Schranke der allgemeinen Gesetze und das kollidierende Verfassungsrecht. Die zuvor im Schutzbereich angeführten Besonderheiten der Verwendung von Social Bots, der mutmaßliche Täuschungscharakter, die Pseudonymität und schließlich der Multiplizierungseffekt, sind im Rahmen der Schranken-Schranken einer neuerlichen Prüfung zu unterziehen, die nun einer Abwägung zugänglich ist.
Diesen rechtlichen Bewertungen folgt im Spannungsfeld von technischem Fortschritt und Regulierung die Betrachtung der bestehenden Rechtslage. Dabei ist zu überprüfen, ob diese Rechtslage die Verwendung von Social Bots im Sinne der Demokratie hinreichend adressiert oder ob eine weitergehende staatliche Handlungspflicht besteht. In diesem Zusammenhang sind insbesondere die sich aus dem Medienstaatsvertrag (MStV) ergebende Kennzeichnungspflicht von Social Bots und das Netzwerkdurchsuchungsgesetz (NetzDG) zu betrachten. Hier lassen sich bei § 18 III MStV rechtliche Lücken identifizieren, die im Zusammenhang mit dem Grad von Automatisierungen und dem Zugriff auf vorgefertigte Texte sowie dem Adressatenkreis der Norm stehen. Hinsichtlich des NetzDG sind insbesondere ein etwaiges *Overblocking*, vermutete *Chilling Effects* und eine *privatisierte* Rechtsdurchsetzung zu thematisieren.
Letztlich münden diese rechtlichen Fragestellungen in der Betrachtung einer Verwendung von Social Bots durch politische Parteien innerhalb und außerhalb des Wahlkampfes unter besonderer Beachtung des Demokratieprinzips und der auf dieses wirkende Meinungsfreiheit. Dabei können die staatsorganisatorischen Besonderheiten nicht außer Acht gelassen werden, die insbesondere aus dem Verfassungsauftrag der Parteien nach Art. 21 I 1 GG und ihrer Staatsnähe hervorgehen. In diesem Zusammenhang ist der dreifältige Status der Parteien nach *Konrad Hesse* darzustellen, um mit dessen Ratio die Rechtmäßigkeit der Verwendung von Social Bots durch Parteien zu überprüfen. Dabei ist fraglich, ob sich aus dem sichernden Aspekt der Freiheit der Parteien eine Rechtfertigung des Einsatzes von Social Bots herleiten lässt. Gleichzeitig ist dieser freiheitliche Aspekt in Einklang mit dem Grundsatz der Gleichheit der Parteien zu bringen. Letztlich müssen die vorangegangenen Überlegungen dem Status der Öffentlichkeit entsprechen, wonach Parteien die Verantwortung für ihr öffentliches Handeln obliegt, diese Verpflichtung jedoch die Rolle als Grundrechtsträger wahrt.
Diese allgemeinen Erwägungen erfahren eine besondere demokratische Relevanz, wenn die Verwendung von Social Bots im Wahlkampf in Rede steht. Eine unrechtmäßige Beeinträchtigung des Wahlvorganges könnte sowohl aus strafrechtlicher als auch aus verfassungsrechtlicher Perspektive zu betrachten sein. In den Blick zu nehmen ist dabei nicht der Wahlakt als solcher, sondern der diesem vorausgehende Prozess der Meinungsbildung. Dort sind insbesondere die §§ 108, 108a StGB und der Art. 38 I GG zu problematisieren, dabei jedoch der unterschiedliche Regelungsrahmen unter Berücksichtigung der verfassungsrechtlichen Judikate zu berücksichtigen. Schließlich sind die etwaigen Anforderungen an die Transparenz unter Berücksichtigung der Abweichungen zu *gewöhnlicher* Kommunikation in sozialen Netzwerken – die Automatisierung, die Multiplizierung und die Pseudonymisierung – herauszuarbeiten.

B. Definition von Social Bots

Die technische und phänotypische Vielfältigkeit von Social Bots geht Hand in Hand mit der Heterogenität der in der Literatur vertretenen Definitionsansätze. Während überwiegend ein Konsens dahingehend besteht, dass jedenfalls soziale Netzwerke adressierende automatisierte Kommunikationsprozesse durch Algorithmen vorliegen, unterscheiden sich die Auffassungen in den darauf aufbauenden zusätzlichen Kriterien. Die in der Literatur vertretenen Definitionen werden also verschiedentlich durch hinzukommende Merkmale feiner untergliedert. Alle Definitionen verbindet der automatisierte Kommunikationsprozess. Dieser wird teilweise kumulativ durch die Kriterien eines menschenäquivalenten Handelns und einem Manipulationswillen erweitert. Die engsten Definitionen sind mithin – in Ihren Kriterien aufeinander aufbauend und – fünfstufig.

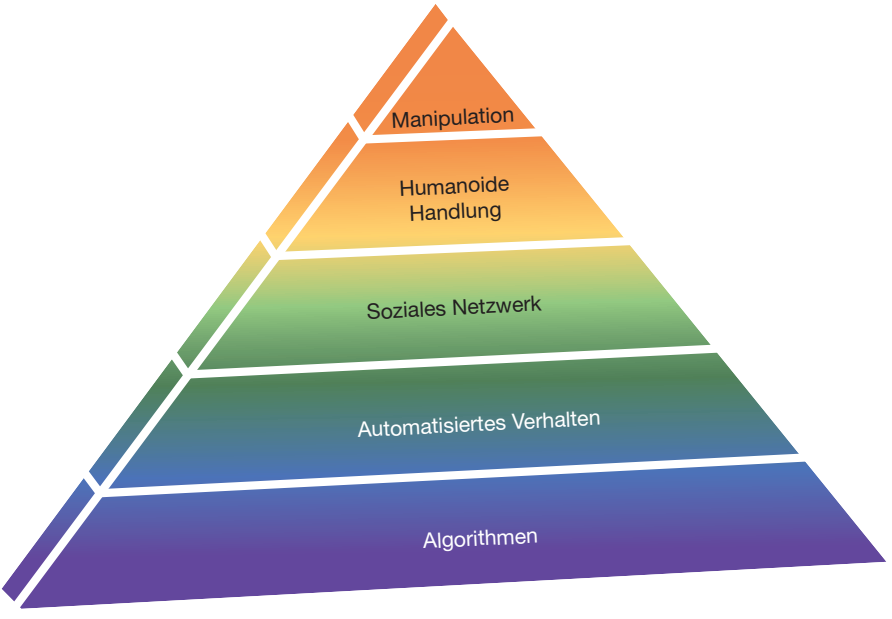

Abbildung 1: Kumulative Definitionselemente von Social Bots

Nach hier vertreten Auffassung sind ***Social Bots*** *von Personen- oder Personengruppen in Verkehr gebrachte Programmcodes, welche nach Inverkehrbringen selbsttätig Social-Media-Accounts und die dazugehörigen Profile kontrollieren, um sich nach determinierten Programmierungsmustern auf der jeweiligen korrespondierenden Plattform wie ein menschlicher Nutzer kommunikativ interagierend zu gerieren*.

I. Automatisierter Programmcode in sozialen Netzwerken

Das Definitionsmerkmal „durch Personen oder Personengruppen in Verkehr gebracht" beschreibt, dass Social Bots auf eine menschliche Schöpfung zurückgehen und nicht aus sich selbst entstanden sind oder bereits ohne menschliches Zutun existent sind. Durch das Befolgen von „determinierten Programmierungsmustern" wird auf die algorithmische Basis von Social Bots rekurriert und die Abgrenzung zur Künstlichen Intelli-

genz (KI) verdeutlicht. Denn insbesondere der bestimmbare und vorhersehbare Ablauf ist für einen Algorithmus wesentlich.[15] So beinhaltet die ganz überwiegende Anzahl aller Definitionsansätze als Grundbausteine eine algorithmusbasierte automatisierte Handlung in der Wirkungswelt eines sozialen Netzwerks; statt vieler[16] *Murthy* et al.: „computer programs or algorithms controlling accounts on social media".[17]
Die Bezeichnung als „Programmcode" wurde aus zweierlei Gründen gewählt: zum einen dient sie einer Versachlichung der Diskussion um Social Bots und soll so einer Vermenschlichung bereits auf Definitionsebene entgegenwirken.[18] Zum anderen ist jedoch wichtig, zwischen dem inverkehrgebrachten Programmcode als zugreifende Entität und dem angesteuerten Account des jeweiligen Intermediärs als Zugriffsobjekt zu differenzieren. Ein Algorithmus kann zahlreiche Accounts fernsteuern. Strenggenommen sind, wenn regelmäßig von Social Bots gesprochen wird, durch Social Bots kontrollierte Accounts oder die dazugehörigen Profile gemeint. Dabei besteht der Account im Verhältnis zwischen Nutzer und Plattformbetreiber und meint das dort befindliche Nutzerkonto, während das Profil die jeweilige Entität und die dazugehörige Seite des Nutzers ist, die den anderen Netzwerkteilnehmern gegenüber sichtbar ist.[19] Daher wird mit der hier genutzten Definition der Programmcode des Bots und die gesteuerten Subjekte voneinander unterschieden.

Vereinzelt finden sich Literaturstimmen, die bei diesen fundamentalen Definitionskriterien abweichen. So definiert *Hostacna* beispielsweise, dass Social Bots „kleine Softwareprogramme [sind], welche ein Gespräch mit einem Menschen auf Social Media simulieren".[20] Diese Definition greift zu kurz. Das automatisierte Verhalten, welches in dem jeweiligen Netzwerk erfolgt, ist nicht zu eng zu fassen. Einem Gespräch wohnt ein Dialog mit wechselseitiger Rede und Gegenrede inne. Ein solches wird in den seltensten Fällen durch Social Bots entstehen oder aufrechterhalten werden (können) und betrifft nur einen Teilbereich der automatisierten Aufgaben. Vielmehr passt diese Eigenschaft zu der Sonderform der Chat Bots. Auch werden dadurch weitere Handlungsformen ausgeklammert. So ist ebenfalls die Definition von *Leistert* zu eng, der auf eine Kommunikation mittels Sprache abstellt.[21] Social Bots können sich jedoch bloß non-verbal – je nach Programmierung – auf eine Followereigenschaft oder das Liken beschränken.

Über das Merkmal der Wirkungswelt einer Social-Media-Plattform findet überwiegend die Abgrenzung und Spezialisierung von und zu sonstigen Botkategorien statt. Überge-

15 Siehe dazu unter D IV.

16 Paal/Hennemann, ZRP 2017, 76 (77); Janal/Isikay, GRUR-Prax 2018, 393 (393); Schröder, in: Schröder/Schwanebeck, Big Data – In den Fängen der Datenkraken: Die (un-)heimliche Macht der Algorithmen, 73 (79 f.); Röttgen/Juelicher, DSRITB 2017, 227 (227); Decker, Parteiendemokratie im Wandel, 265; Schünemann/Marg, in: Schünemann/Kneuer, E-Government und Netzpolitik im europäischen Vergleich, 381 (389); Prier, SSQ 2017, 50 (54); differenzierend Volkmann, MMR 2018, 58 (58 f.); Gasser/Kraatz, Social Bots: Wegbereiter der Maschinokratie abstellend auf fiktive Identität und nicht auf täuschenden Charakter und mithin eher diesem Meinungsspektrum zuzuordnen; Howard/Kollanyi, SSRN 2016, 1 (1); und in der Tendenz auch Thieltges/Hegelich, in: Behnke/Blätte/Schnapp/Wagemann, Computational Social Science: Die Analyse von Big Data, 357 (359) mit der Ergänzung, dass der Bot vorgibt, ein menschlicher User zu sein; vgl. Hoffmann-Riem, AöR 2017, 1 (14); FAQ unter Botometer, Botometer Startseite; Oertel u. a., Algorithmen in digitalen Medien und ihr Einfluss auf die Meinungsbildung, 37; Davis u. a., WWW '16 Companion 2016, 273 (273); unter Verzicht auf das Merkmal des Algorithmus John, Social Bots im Parteienwettbewerb, 27 f.

17 Murthy u. a., IJC 2016, 4952 (4955).

18 Vgl. beispielsweise Amann u. a., Wie digitale Dreckschleudern Meinung machen.

19 Vgl. Laude, Automatisierte Meinungsbeeinflussung, 32.

20 Hostacna, AL 2018, 1 (1) [Klammerzusatz durch den Verfasser]; so auch Froitzheim/Köbrich, WRP 2017, 1188 (1188); besser Wolf, der breiter auf die Interaktion eines Programms mit Menschen abstellt Wolf, WRP 2019, 440 (441).

21 Leistert, in: Seyfert/Roberge, Algorithmuskulturen: Über die rechnerische Konstruktion der Wirklichkeit, 215 (215).

ordnet liegt als allgemeinere Kategorie ein Algorithmus in Form eines Web Bots vor. Vereinzelt wird Social Bots nur ein Tätigwerden bei Facebook zugeschrieben.[22]
Eine weitere Verständnismöglichkeit ist, dass sich die Verwendung des Wortes *Social* lediglich aus der gesellschaftlich kommunikativen Partizipation ergibt und nicht auf den Einsatzzweck in sozialen Netzwerken Bezug nimmt.[23] Einer solchen Deutung des Wortlautes ist entgegenzuhalten, dass per se Aufgabe eines jeden Bots die Ausführung eines auferlegten menschlichen Handlungsäquivalentes ist und sich die Voranstellung „Social" somit auf die Einsatzumgebung in den sozialen Netzwerken bezieht.

II. Humanoides Handlungsäquivalent

Dem *Wesen* von Bots ist immanent, von Menschen ausführbare Tätigkeiten, die zur bloßen Vereinfachung auf einen Algorithmus übertragen wurden, selbsttätig auszuführen. Da die spezifische Aufgabe von Social Bots die Übernahme menschlicher Interaktion in sozialen Netzwerken ist, kommt es gerade darauf an, durch die Steuerung des jeweiligen Profils, wie ein menschlicher Nutzer zu interagieren. Dabei erschöpft sich diese Interaktion nicht in einer spezifischen Handlungsform.[24] In der Literatur wird ebenfalls ein solches *humanoides Handlungsäquivalent* gefordert.[25] Dabei wird unterschieden zwischen dem Imitieren von menschlichen Handlungen einerseits,[26] so auch der Duden, wonach der Social Bot ein „Computerprogramm [ist], das in einem sozialen Netzwerk vorgibt, ein Mitglied oder ein Nutzer, eine Nutzerin zu sein, und die Aktivitäten natürlicher Personen imitiert."[27]
Andererseits ist nach einer größeren Meinungsgruppe[28] Voraussetzung von Social Bots, dass vorgetäuscht wird, ein realer Mensch zu sein: „These are computer programs designed to use social networks by simulating how humans communicate and interact with

22 Flint, Fake News im Wahlkampf, 56.

23 Vgl. Boshmaf u. a., Proceedings of the 27th Annual Computer Security Applications Conference on – ACSAC '11 2011, 1 (1); Roos, in: Chibanguza/Kuß/Steege, Künstliche Intelligenz: Recht und Praxis automatisierter und autonomer Systeme Rn. 1.

24 John, Social Bots im Parteienwettbewerb, 28.

25 Anders hingegen Gerecke/Stark, GRUR 2021, 816 (819), welche gänzlich auf menschliches Handlungsäquivalent verzichten und auf die faktische Handlung des Social Bots als solche abstellen.

26 Vgl. Wagner u. a., CEUR 2012, 41 (1); Fuchs, Warum Social Bots unsere Demokratie gefährden; Skupin, in: Waechter/Marhold, Europe – Against the Tide, 81 (84); Preuß u. a., in: Deutscher Dialogmarketing Verband e.V., Dialogmarketing Perspektiven 2018/2019, 151 (153); Schatto-Eckrodt u. a., Politikum 2018, 42 (44); Oertel u. a., Algorithmen in digitalen Medien und ihr Einfluss auf die Meinungsbildung, 37; Büttel, AnwZert ITR 1/2021 Anm. 3 2021, 1 (1); Gerecke, GRUR-Prax 2023, 381 (383); Lent, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, MStV § 18 Rn. 13; Schemmel, Der Staat 2018, 501 (509), nach welchem die Bots sogar als natürliche Person agieren. Marechal, IJC 2016, 5022 (5022); Stieglitz u. a., Australasian Conference on Information Systems 2017, 1 (6); John, Social Bots im Parteienwettbewerb, 26 f.

27 DUDEN, Social Bot: Rechtschreibung, Bedeutung, Definition, Herkunft [Klammerzusatz durch den Verfasser].

28 Vgl. Andresen, HRN 2017, 9 (9); Drucksache 518/18: Entschließung des Bundesrates zu Transparenz und klaren Regeln auf digitalen Märkten, 9; Künast, ZRP 2019, 62 (63); Krüper, in: Unger/von Ungern-Sternberg, Demokratie und künstliche Intelligenz, 67 (70); Ungern-Sternberg, von, in: Unger/von Ungern-Sternberg, Demokratie und künstliche Intelligenz, 3 (4, 12); Graber/Lindemann, in: Sachs-Hombach/Zywietz, Fake news, hashtags and social bots: neue Methoden populistischer Propaganda, 51 (57); Meyer, Zwischen Partizipation und Plattformisierung, 76; Hegelich, Analysen & Argumente 2016, 1 (2) wonach die Beeinflussung erst auf Handlungsebene herausgearbeitet wird; Milker, ZUM 2017, 216 (216) welcher von als „realer Nutzer […] ausgeben" schreibt und die Manipulationsmöglichkeit erst auf eine mögliche Handlungsebene verlagert; Klaas, MMR 2019, 84 (87); Thieltges/Hegelich, in: Behnke/Blätte/Schnapp/Wagemann, Computational Social Science: Die Analyse von Big Data, 357 (359) wobei diese Auffassung auch unter der Imitation eines Menschen kategorisiert werden könnte, da sich die Verfasser Boshmaf beziehen und „simulating" mit „vorgeben" übersetzen; Boshmaf u. a., Computer Networks 2013, 556 (556 f.)„mimicking" und „simultating" wird hier eher im Sinne von imitieren oder nachahmen ohne die Wertung des Täuschens zu verstehen sein, aber

each other, and are becoming pervasive in OSNs[29], being highly effective in convincing users that they are actually humans."[30]. Über dieses Kriterium wird teilweise die Abgrenzung zu Spam Bots vorgenommen.[31] Wenn die Zuordnung zu einem *realen* Menschen vorgenommen wird, kann dies nur unmittelbar – bezogen auf den jeweiligen Aktionsmoment im sozialen Netzwerk – verstanden werden, schließlich geht der Social Bot notwendigerweise mittelbar auf einen Menschen sowie seine determinierte Programmierung und Verwendung zurück. Vermittelnd wird darauf abgestellt, dass Social Bots wie natürliche Personen erscheinen.[32]

Auf den ersten Blick scheint die Differenzierung zwischen dem Täuschen und dem Imitieren unerheblich zu sein, sowie auf bloße unterschiedliche Wortwahl zurückzugehen. Jedoch liegt dieser Unterscheidung eine Wertung zu Grunde. Trotz möglicher Kongruenz beider Kriterien, wohnt dem Imitieren eine objektive Komponente inne, während die Täuschung eine subjektive Komponente beinhaltet. Aufgrund der Funktion von Automatisierungen – menschliches Verhalten rationalisiert nachzuahmen – ist das Imitieren Folge dieses Automatisierungsprozesses. Das Kriterium des Vortäuschens verlässt unnötigerweise diese objektive Ebene und stellt auf das Motiv und den Rezipienten ab. Eine Identitätstäuschung kann durch Social Bots erfolgen, ist aber diesen nicht zwingend immanent und sollte nicht als Definitionsmerkmal herangezogen werden.[33] Dies ergibt sich schon aus dem Telos der Kennzeichnungspflicht von Social Bots, wonach Verwender von Social-Bot-Accounts sich als solche auszuweisen haben.[34] Wenn Social-Bot-Accounts als solche zu kennzeichnen sind, können diese nicht gleichzeitig vorgeben, ein menschlicher Nutzer zu sein. Bei gegenteiliger Auffassung würde dies nämlich bedeuten, dass ein Social Bot ab dem Kennzeichnungsmoment kein Social Bot mehr wäre.[35] Dann wäre wiederum eine Kennzeichnung nicht mehr erforderlich. Dieser Zirkelschluss belegt die Untauglichkeit des Abstellens auf das Kriterium des Vortäuschens des Menschseins.[36]

---

aufgrund des „pass itself off as a human being" eher der Meinung mit Täuschungsabsicht zuzuschreiben; Deutscher Bundestag – 19. Wahlperiode, Bericht der Enquete-Kommission Künstliche Intelligenz, 464; Semizoglu, in: Hetmank/Rechenberg, Kommunikation, Kreation und Innovation – Recht im Umbruch?, (82); Libertus, ZUM 2018, 20 (20); Hufen, Staatsrecht II, 413, Rn. 3; Stöcker/Lischka, in: Mohabbat Kar/Parycek/Thapa, (Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft, 364 (380); Liesem, in: Litschka/Krainer, Der Mensch Im Digitalen Zeitalter: Zum Zusammenhang Von Ökonomisierung, Digitalisierung und Mediatisierung, 183 (184); Beck, DVBl. 2020, 253 (257); Peifer, CR 2017, 809 (809); einschränkend Siara, MMR 2020, 370, wonach sich Social Bots „oft als Menschen" ausgeben.

29 Abkürzung für Online Social Networks.

30 Freitas u. a., SNAM 2016, 1 (1); vgl. Löber/Roßnagel, MMR 2019, 493 (493).

31 So z. B. Boshmaf u. a., Proceedings of the 27th Annual Computer Security Applications Conference on – ACSAC '11 2011, 1 (1); Murthy u. a., IJC 2016, 4952 (4955); Boshmaf u. a., Computer Networks 2013, 556 (556 f.).

32 Drexl, ZUM 2017, 529 (530), nach dessen Definition Beiträge jedoch „ohne Unterlass" verbreitet werden. Die zeitliche Streuung ist jedoch von der Programmierung und dem sich aus diesem ergebenden Zusammenfallen von Suchparamtern und Suchtreffern abhängig, so dass eine zeitliche Komponente nicht aufgenommen werden sollte. Martini, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, MStV § 2 Rn. 124, wonach die Äußerungen von Social Bots suggerieren, von menschlichen Nutzern erstellt worden zu sein. Holznagel, ZRP 2021, 229 (231); Rotermund, Künstliche Intelligenz aus staatlicher Perspektive, 38; Laude, Automatisierte Meinungsbeeinflussung, 38; Buchholtz, DÖV 2017, 1009 (1013 f.); Hepp, in: Eisenegger/Prinzing/Ettinger/Blum, Digitaler Strukturwandel der Öffentlichkeit: Historische Verortung, Modelle und Konsequenzen, 471 (476); Oberer u. a., in: Stumpf, Digitalisierung und Kommunikation, 311 (311).

33 Vgl. Wolf, WRP 2019, 440 (443); Schünemann, ComSoc 2019, 159 (162), welcher enefalls gänzlich auf Imitation, Täuschung oder Manipulation verzichtet.

34 Siehe unter F. I. 1.

35 So auch John, Social Bots im Parteienwettbewerb, 28.

36 Anders Boshmaf u. a., Proceedings of the 27th Annual Computer Security Applications Conference on – ACSAC '11 2011, 1 (1), welcher gerade darauf verweist, dass der Social Bot „stealthy" agiert.

Aus selbigem Grund sind die Auffassungen abzulehnen, die auf eine „Tarnung als menschlicher User“ abstellen.[37] Der Social Bot gibt nicht unmittelbar vor, ein Mensch zu sein, vielmehr beruht dieses Vorgeben tatsächlich auf der Schlussfolgerung des Empfängers. Es bedarf nämlich eines gedanklichen Zwischenschrittes. Der Schlüssel zur Partizipation an einem sozialen Netzwerk ist nicht die menschliche Eigenschaft, sondern das Vorliegen eines nutzungsbedingungskonformen Accounts und des darauf beruhenden Profils.[38] Welchen Eindruck der Verwender bei anderen Netzwerkteilnehmern hervorzurufen beabsichtigt, ist erst auf zweiter Ebene zu prüfen. Genau daran knüpfen die Meinungen an, welche definieren, dass Social Bots „mit scheinbar echten Nutzerprofilen wie gewöhnliche Teilnehmer des Netzwerks aussehen“[39]. Zwar wird damit richtigerweise auf Profile abgestellt, jedoch müsste dann konsequenterweise die Unterscheidung zwischen echten und unechten Profilen aufgegeben werden. Diese setzt nämlich voraus, dass botgesteuerte Profile keine echten Profile sind und führt somit zwingend zu der Frage, wann ein Profil als echt gilt. Die Einschränkung auf ein scheinbar echtes Nutzerprofil greift zu kurz und engt die Definition eines Social Bots zu sehr ein. Es ist bei einer Abgrenzung nicht zielführend, die Möglichkeit eines Rückschlusses auf eine echte Person zu fordern, denn de facto betreiben eine Vielzahl von realen Nutzern Profile mit Vor-, Spitz- oder Fantasienamen. Ein Abstellen auf die Nutzungsrichtlinien von X[40] (ehemals Twitter) zeigt, dass Automatisierungsaccounts aufgrund des *application programming interfaces* (APIs) von X möglich, zulässig und ordnungsgemäß sind.[41] Sinnvollerweise sollte von einem den Nutzungsbedingungen konformen Profil gesprochen werden.
Sowohl bei der Variante des Täuschens als auch des Imitierens ist die Existenz von botgesteuerten Profilen ohne Nutzerbild sowie Nutzernamen mit zufälligen Reihungen von Buchstaben zu berücksichtigen. Aus der Perspektive der adressierten Nutzer dürften diese Profile, falls diese einer näheren Betrachtung unterzogen würden, nur schwerlich für gewöhnliche Accounts gehalten werden. Gerade bei offensichtlich generierten Profileigenschaften dürfte es dem Ersteller vorrangig nicht darum gehen, über eine unmittelbare menschliche Betreibereigenschaft zu täuschen. Ohnehin sind mit der Verbreitung automatisierter Accounts, Fakeaccounts und Zweitaccounts[42] die Grenzen fließend und bei der regulären, nicht automatisierten Nutzung, längst nicht mehr davon auszugehen, dass tatsächlich, im Sinne von *Ein Mensch = Ein User*, ausschließlich ein singulärer, digitaler Avatar eines existierenden Menschens gegeben ist.

Damit zeigen sich sowohl das Imitieren als auch das Täuschen als Definitionsmerkmal nicht geeignet. Gleichwohl bedarf es eines humanoiden Handlungsäquivalentes mit einem, da sich eine algorithmische Automatisierung auch in einem bloßen im Hintergrund ablaufenden Rechenprozessen erschöpfen könnte und damit nicht bei jedem automatisierten Prozess von einem Social Bot zu sprechen ist. Um dem gerecht zu werden, aber dennoch auf der objektiv-deskriptiven Ebene gerecht zu werden, sollte die Vergleichbarkeit zu einem menschlichen Nutzer durch „wie ein menschlicher Nutzer gerieren“ hergestellt werden.

37 Künast, ZRP 2019, 62 (63); vgl. auch Milker, ZUM 2017, 216 (216); anders Klaas, MMR 2019, 84 (87), welcher auf „die Existenz eines realen, hinter dem Netwerkprofil stehenden Menschen“ abstellt.
38 Thieltges/Hegelich, in: Behnke/Blätte/Schnapp/Wagemann, Computational Social Science: Die Analyse von Big Data, 357 (359).
39 Andresen, HRN 2017, 9 (9).
40 In dieser Arbeit wird der Übersichtlichkeit halber, wenn Studien und Quellen zitiert werden, die auf X vor der Umbenennung von Twitter Bezug nehmen, weiterhin Twitter geschrieben.
41 X, X Hilfebereich: Regeln zur Automatisierungsentwicklung.
42 Die Aufteilung von geschäftlichen und privaten Accounts, sowie die Einstellung anonymer Zweitaccounts führt beispielsweise zum Innehaben verschiedener Accounts.