Unsocial Bots – Eine Gefahr für die Autonomie des Gesellschaftssystems

Benjamin Heurich

1. Einleitung

Der Einsatz künstlich erzeugter Identitäten, die von automatisierten Softwareprogrammen (Bots) gesteuert und mittlerweile massenhaft in Social Networking Services (SNSs), wie Twitter, Facebook oder Instagram eingebunden sind, gewann in den letzten Jahren vor dem Hintergrund weltgesellschaftlicher Ereignisse immer mehr an Brisanz.[1] Ausgereifte Bot-Technologien generieren automatisch Kommunikationsinhalte und interagieren mit menschlichen Nutzer/innen – aber auch anderen Bots – in den öffentlichen Kommentarspalten, Chats und Newsfeeds der SNSs. Aufgrund deren beobachteten Wirkung auf die Sozialität der digitalen Gesellschaft hat sich der Begriff *Social Bot* etabliert, der in der folgenden gesellschaftstheoretischen Abhandlung beibehalten werden soll und die Problematik der Arbeit transportiert. Mithilfe der soziologischen Systemtheorie von Niklas Luhmann werden die empirischen Befunde im Zusammenhang mit aktuellen Einflüssen von Social Bots auf einer abstrakten Ebene zusammengeführt, um das gesamtgesellschaftliche Gefahrenpotential der Technologie aufzuzeigen. Durch eine funktionsanalytische Einführung des Begriffs der *Systemautonomie* in den Problembereich wird der neutrale Standpunkt aus der Privatheitsforschung akzentuiert, der Privatheit im Zuge der Digitalisierung zunehmend als ein gemeinschaftliches und öffentliches Gut markiert, das es zur Integrität sozialer Kontexte

1 Politische Ereignisse in jüngster Vergangenheit, die globale Auswirkungen nach sich gezogen haben und in denen Social Bots eine signifikante Rolle zugewiesen wird, sind beispielsweise der Austritt Großbritanniens aus der EU (*Brexit*), der sogenannte *Arabische Frühling* und die Präsidentschaftswahlen in den USA im Jahr 2016 (vgl. Stieglitz u.a. 2017: S. 397). Es wird zudem spekuliert, dass der sogenannte *Flash Crash* des US-amerikanischen Aktienindexes S&P 500 im Jahr 2010 – neben dem mittlerweile offensichtlichen Einsatz von Algorithmen – auch auf den Einsatz von Social Bots auf Twitter zurückzuführen sei (vgl. Ferrara u.a. 2016: S. 99). Das populärwissenschaftliche Buch *LikeWar – The Weaponization of Social Media* beschreibt diese und weitere Ereignisse aus politisch-strategischer Sicht und verweist ebenfalls auf den Einsatz von Social Bots in SNSs (siehe Singer/Brooking 2018).

und für das Funktionieren einer demokratischen Gesellschaftsstruktur zu schützen gilt.[2] Die eingangs skizzierte Problematik spitzt sich vor diesem Hintergrund auf den folgenden Untersuchungsgegenstand zu, bei dem sich letztendlich zwei Verantwortungsebenen für besagten Schutz enthüllen werden: In dem Bestreben, die demokratische Meinungs- und Willensbildung der Gesellschaftsmitglieder zu beeinflussen, werden Social Bots im SNS Twitter zur Konstruktion und Manipulation öffentlich verhandelter Themen eingesetzt. Getarnt hinter künstlich erzeugten Identitäten nutzen sie die technosoziale Beschaffenheit des Netzwerks, um bestimmte Themen auf die öffentliche Agenda zu setzen oder den Informationsfluss zu bereits bestehenden Themen zu kontrollieren. Der systemtheoretische Zugang eröffnet sich hierbei in der Beschreibung und der Analyse der (digitalen) Öffentlichkeit, in der sich ein komplexes Geflecht gesellschaftlicher Themen etabliert, an dem sich alle Teilsysteme der Gesellschaft zur Aufrechterhaltung von Kommunikation orientieren.[3] Speziell in der Beobachtung der öffentlichen Meinung, die Luhmann als das »Medium der Selbst- und Weltbeschreibung der modernen Gesellschaft«[4] beschreibt, lassen sich funktionsanalytische Annahmen aus der Privatheitsforschung mit systemtheoretischen Erkenntnissen verbinden.[5] Die These lautet, dass gesellschaftliche Gefahren, die mit dem Einsatz von Social Bots einhergehen, sowohl gegenwärtig als auch zukünftig nicht direkt und in vollem Umfang von den Funktionssystemen selbst erkannt und in Risiken umgewandelt werden können, weil etwaige Umweltereignisse stets nur anhand des systemspezifischen Codes geprüft und verarbeitet werden.[6] Durch den Einsatz von Social Bots werden daher zwar innersystemische Komplexitäten gesteigert, deren risikominimierende Wirkungen jedoch durch die neu entstandenen digitalisierten Kopplungen ein stetig ansteigendes Gefahrenpotential durch nicht

2 Helen Nissenbaum legt in diesem Zusammenhang ausführlich dar, warum Privatheit nicht an einzelnen Daten oder individuellen Zugangskontrollen, sondern an die Unversehrtheit (*contextual integrity*) jeweils verschiedener Kontexte gebunden ist (vgl. Nissenbaum 2010: S. 127-157). Weitere theoretische Konzeptionen beschreiben Privatheit als ein Gemeinschaftsgut (»public value of privacy«, Regan 2015: S. 60), das vor allem innerhalb von Sozialität einen Wert erhält (ausführlich dazu Regan 2015: S. 55-65 und Gavison 1980). Auch Beate Rössler weist bei der Verortung eines Wertes von Privatheit darauf hin, dass digitale Daten und Kommunikation stets der »Problematik des Kontextes« unterworfen sind (Rössler 2001: S. 225).

3 Vgl. Luhmann 2005: S. 166f.

4 Luhmann 2015: S. 1107.

5 Diese neutrale Konzeption transportiert einen Wert von Privatheit innerhalb der theoretischen Aushandlung als ein gesellschaftliches Gut, das jeweils sowohl von den sozialen Systemen als auch von den Menschen individuell bestimmbar und verhandelbar ist (vgl. Gavison 1980: S. 423).

6 Es sind dann Beobachtungen von Beobachtungen (Beobachtungen zweiter Ordnung), wie beispielsweise mit dieser Arbeit aus dem Wissenschaftssystem heraus, die spezielle *Wie*-Fragen stellen und dadurch Problemlösekompetenzen erhöhen und erweiterte gesellschaftliche Zusammenhänge kenntlich machen können.

handhabbare Umweltabhängigkeiten entwickeln und damit die Autonomie von Gesellschaftssystemen beinträchtigen. Zum besseren Verständnis werden im folgenden Kapitel zunächst die methodische Eignung und der wissenschaftliche Mehrwert des angewandten Analyserepertoires der soziologischen Systemtheorie für den dort entsprechend skizzierten Problembereich dargelegt. Um die rein technologischen Komponenten des Untersuchungsgegentandes adäquat in einen gesamtgesellschaftlichen Kontext einpassen zu können, erfolgt ein Umriss der sozialen und funktionalen Eingebundenheit von Social Bots anhand der soziologischen Unterscheidung zwischen Risiko und Gefahr. Kapitel 3 widmet sich in mehreren Schritten der von Luhmann selbst eingeleiteten, »radikal ansetzenden Rekonstruktion« des Begriffs der öffentlichen Meinung, der auf diese Weise »den Empiriebezug und die Genauigkeitsansprüche der heutigen Sozialwissenschaften zur Geltung bringen«[7] soll. Der empirische Teil folgt in Kapitel 4 und wird mit einer Unterteilung des Analysegegenstandes in *back-end* und *front-end* eingeleitet. Hier werden zunächst strukturelle Gründe für die Fremdsteuerung der digitalen Themenagenda im Microblogging-Netzwerk Twitter aufgezeigt, bevor abschließend auf zusätzliche Herausforderungen in der zwischenmenschlichen Digitalkommunikation eingegangen wird, die es bei dem Vorhaben, Bot-Technologien nachhaltig in der Öffentlichkeit zu verankern, zu überwinden gilt.

2. Social Bots als formgebende Elemente gesellschaftlicher Funktionssysteme

Die wissenschaftliche Auseinandersetzung mit der angesprochenen Problematik befasst sich hauptsächlich mit der Frage, wie die allgegenwärtige Nutzung von Social Bots kontrolliert werden kann und welche Regularien an welche Verantwortungsbereiche zu knüpfen wären. Während in diesem Zusammenhang die Technikfolgenabschätzung im Vordergrund steht, befassen sich weitere Diskurse mit den vermuteten psychologischen Effekten eingesetzter Bots auf die individuelle Entscheidungsfindung der Menschen.[8] Hier wird die Frage nach den Ausmaßen der Manipulationsmöglichkeiten von Individuen in gesellschaftlich relevanten Entscheidungssituationen gestellt, die sich durch die Aggregation und Auswertung persönlicher Daten mittels einer kritischen Masse an Social Bots erzielen ließe. Im Hinblick auf die globale Vernetzung der digitalen Gesellschaft wird bereits von einer »Klimavergiftung [der] politische[n] Debattenkultur im Internet«

7 Luhmann 2005: S. 164.

8 Vgl. Stieglitz u.a. 2017: S. 381. Zum Stand der Technik und zum Einflussbereich von Social Bots vgl. Kind u.a. 2017; Ferrara u.a. 2016 und Varol u.a. 2017; zur Wirkung von Bot-Netzwerken in Wirtschaftszusammenhängen vgl. ANA/White Ops, Inc. 2017.

gesprochen, mit der das »Vertrauen in die Demokratie«[9] unterlaufen werde. Die Diskurse um Hate Speech und Fake News[10] befeuern die Technologiekritik und münden in dem Vorwurf einer einseitigen Manipulation der Bürger/innen durch den gezielten Einsatz von Social Bots in SNSs.[11] Die empirischen Untersuchungen stützen sich dabei jedoch lediglich auf »eine begrenzte Anzahl prominenter Ereignisse«[12], anhand derer sich etwaige privatheitssensible Thesen, die bei der Eindämmung von Social Bots behilflich sein sollen, nicht zur Genüge belegen lassen.[13] Die Annahme eines *direkten* Einflusses von Social Bots auf die persönliche und individuelle Meinungs- und Willensbildung der Internetnutzer/innen konnte bisher ebenso wenig belegt werden und wird mit Bezug zur theoretischen Fundierung dieser Arbeit auch generell angezweifelt.[14] Hier knüpft der einleitend erwähnte Genauigkeitsanspruch der heutigen Sozialwissenschaften an, dem Luhmann unter anderem mit einer radikalen Neuansetzung des Begriffs der öffentlichen Meinung begegnet, der »[i]m Verhältnis zur Tradition […] auf jede Rationalitätsimplikation, ebenso aber auch auf jede Herausstellung spezifischer Irrationalitäten der ›Massenpsychologie‹ [verzichtet]«[15]. Aufgrund der fortschreitenden Entwicklung digitaler Technologien und der wachsenden Elastizität digitaler Kontexte kann davon ausgegangen werden, dass sich eine robuste Grundlage für politische oder rechtliche Regulierungen von Social Bots auch in Zukunft nicht aus einzelnen empirischen Befunden legitimieren lassen. Nicht zuletzt macht es die heutige ubiquitäre Verwendung von Social Bots in allen Teilsystemen der Gesellschaft notwendig, eine Beobachter/innenposition einzunehmen, die gerade *entgegen* der Funktionalität ein gesamtgesellschaftliches Risikobewusstsein stärkt und auf Gefahren *innerhalb* einer sozialen Ordnung verweist. Wie sich zeigen wird, hilft die systemtheoretische Unterscheidung zwischen *Risiko* und *Gefahr* dabei, diese

9 Kind u.a. 2017: S. 40.

10 Eine Oxford-Studie zu Online-Propaganda bringt das weltweite Aufkommen von Fake News und Hate Speech mit dem Einsatz von Social Bots in Verbindung (vgl. Woolley/Howard 2017).

11 Zur Thematik online Hate Speech, Fake News und weiteren sozialen Implikationen von Social Bots vgl. Bollmer/Rodley 2017; Matsakis 2017; Schneiderman 2017; für eine Übersicht über die breit geführte Privatheitsdebatte um die Zusammenarbeit von Facebook und der Datenanalysefirma Cambridge Analytica vgl. Dachwitz u.a. 2018; Grigonis 2018.

12 Kind u.a. 2017: S. 30.

13 Bei einer funktionalen Analyse sind empirische Daten als vorläufige Gegenwartsaufnahmen zu betrachten. Gavison verweist hier im Besonderen auch auf die Bestimmung eines Wertes von Privatheit: »[…] the empirical data is not only scant, it is often double-edged. The evaluation of links between privacy and other values must therefore be extremely tentative« (Gavison 1980: S. 442).

14 Vgl. Kind u.a. 2017: S. 7. Zur operativen Schließung psychischer Systeme vgl. Luhmann 1993: S. 346-375.

15 Luhmann 2005: S. 167.

Diskrepanzen aufzulösen. Zunächst ist jedoch eine – wenn auch stark verkürzte – systemtheoretische Gesellschaftsbeschreibung notwendig, die den Zugang zu einigen zentralen Begrifflichkeiten der vorliegenden Arbeit legt: Die soziologische Systemtheorie von Niklas Luhmann beschreibt eine funktional ausdifferenzierte Gesellschaft, in der sich einzelne Funktionssysteme, wie Recht, Politik und Wissenschaft, für die Erfüllung jeweils spezifischer Aufgabenbereiche gebildet haben. Das diese Systeme umfassende Metasystem *Gesellschaft* besteht aus jeweils temporär realisierter Kommunikation, die durch *strukturelle Kopplungen* zwischen den Bewusstseinssystemen der Menschen zustande kommt.[16] Damit integrieren sich Menschen eigenständig als Personen in die Gesellschaft und ordnen sich, beispielsweise als Konsument/in oder Wähler/in, einem Funktionssystem zu. Die Funktionssysteme setzen sich innerhalb der Gesellschaft in der Regel über einen spezifischen, zweiwertigen Code (bspw. Recht/Unrecht im Rechtssystem oder Zahlung/Nichtzahlung im Wirtschaftssystem) in eine Differenz zu ihrer Systemumwelt, um dadurch die Überkomplexität aller für sie erreichbaren Kommunikationen zu reduzieren und die Funktionserfüllung und Leistungserbringung überhaupt erst zu ermöglichen.[17] Von zentraler Bedeutung ist dabei, dass sich der systemtheoretische Funktionsbegriff nicht allein auf ein System, sondern immer auf das Verhältnis eines Systems zu seiner Umwelt bezieht.[18] Ohne eine Grenzziehung zur Umwelt können Systeme nicht existieren, da es keine Identität ohne eine Unterscheidung geben kann.[19] Auf diese Weise erzeugen Systeme durch eigene Operationen und Entscheidungen, wie beispielsweise die Implementierung neuer technologischer Elemente, für sich selbst stets mehr oder weniger kalkulierbare *Risiken*, die durch strukturelle Neuordnungen minimiert oder absorbiert werden können. In der Systemumwelt werden im Gegensatz dazu *Gefahren* als Ereignisse erlebt, die anderen Systemen zugeschrieben werden und daher nicht durch eigene Operationen gehandhabt werden können.[20] Durch die Erhöhung innersyste-

16 Vgl. Luhmann 1993: S. 555f. Diese Form der Gesellschaftsbeschreibung geht auf den von Luhmann eingeleiteten Paradigmenwechsel zurück, durch den die Sozialwissenschaften einen adäquaten Zugang zu dem abstrakten theoretischen Begriffsrepertoire der Systemtheorie und der Kybernetik erhielten. Nur indem die Menschen und deren Gedanken der Umwelt des Metasystems Gesellschaft zugewiesen werden und das Ganzes-Teil-Schema neu geordnet wird, ist es möglich, soziale Gesetzmäßigkeiten über Generationen hinweg zu beschreiben und der Komplexität der Gesellschaft Rechnung zu tragen (ausführlich dazu Luhmann 1993: S. 15-29).

17 Soziale Systeme erfüllen nach der soziologischen Systemtheorie eine *Funktion* für die Gesellschaft und erbringen eine *Leistung* für andere Teilsysteme (vgl. Luhmann 2015: S. 748-758).

18 Vgl. Luhmann 1993: S. 242-245.

19 Die Differenz von Identität und Differenz, die demnach letztbegründend immer auf eine Differenz (und nicht auf eine Einheit) hinausläuft, bildet das zentrale Paradigma der Theorie selbstreferentieller Systeme (vgl. Luhmann 1993: S. 26).

20 Vgl. Luhmann 2015: S. 140.

mischer Komplexität und die Implementierung neuer Elemente kann ein System die Beherrschbarkeit von Umweltgefahren herbeiführen und diese stückweise in Risiken umwandeln.[21] Veränderung in der Umwelt, wie beispielsweise eine Erfindung oder Marktreife einer neuen Technologie, lässt wiederum neue Gefahrenbezüge entstehen, die bei Beobachtung ereignishafte Irritationen nach sich ziehen.[22] Systeme erhalten vor diesem Hintergrund ihre Autonomie dadurch aufrecht, dass sie *gleichzeitig* die Abhängigkeit und Unabhängigkeit von Umweltereignissen regulieren und, der gesellschaftlichen Abwicklung dieser Ereignisse entsprechend, laufend aktualisieren. Ist also von gesamtgesellschaftlichen Gefahren die Rede, hat das umfassende Metasystem Gesellschaft den Anspruch an die jeweiligen Funktionssysteme, das Gefahrenpotential systemspezifisch zu erkennen, aufzugliedern und durch wirtschaftliche, politische oder erzieherische Maßnahmen in kalkulierbare Risiken umzuwandeln. Die These, dass sich gerade diese Form der Gefahrenabwicklung aufgrund der strukturellen Verfestigung von Social Bots aktuell als wenig zielführend erweist, begleitet die beiden folgenden Abschnitte.

2.1 Social Bots als gesellschaftliches Risiko

Die innere Komplexität eines Systems gibt vor, wie effektiv und flexibel es auf beobachtete Umweltereignisse reagieren kann.[23] Systemeigene Elemente dienen im Angesicht ereignishafter Umweltgefahren der Funktionserfüllung und Leistungserbringung und legitimieren sich in einer selbstreflexiven Beobachtung der Systeme selbst.[24] Diese Selbstbezogenheit und die Fähigkeit der Systeme, »die Elemente, aus denen sie bestehen, durch die Elemente, aus denen sie bestehen,

21 Vgl. Luhmann 1998: S. 661f.

22 Vgl. Luhmann 1993: S. 243. Ein komprimiertes Beispiel: Die Erfindung des iPhones durch das nordamerikanische Unternehmen Apple, zu beschreiben als ein zentrales Ereignis schnell fortschreitender Digitalisierung, hatte für wenig bis keine Irritationen im (deutschen) Erziehungssystem gesorgt. Es entstand keine Absicht, die Heranwachsenden auf den (systemspezifischen) Umgang mit dem iPhone vorzubereiten und die technologisierten Sozialisationsprozesse erzieherisch zu begleiten. Lehrende sahen sich zeitnah der Gefahr ausgeliefert, im Unterricht von den Lernenden einen Wikipedia-Artikel auf einem iPhone entgegengehalten zu bekommen, wodurch sowohl die Erziehungsautorität als auch die Geschlossenheit des Klassenraums unterminiert wurde. Auf der Makroebene entstand die Gefahr, dass Heranwachsende keine ausreichende – von den anderen Funktionssystemen eingeforderte – digitale Bildung vorweisen können. Diesem Umstand kann das Erziehungssystem nun durch neue Elemente, wie digitale Klassenzimmer, Umprogrammierung von Curricula oder Weiterbildung, entgegenwirken. Da dafür jedoch zunächst wirtschaftliche Investitionen und bildungspolitische Entscheidungen notwendig sind, ist das Erziehungssystem in diesem Vorhaben nicht autonom.

23 Vgl. Luhmann 1993: S. 296-298.

24 Vgl. Luhmann 1993: S. 58-60.

selbst produzieren und reproduzieren«[25] zu können, nennt Luhmann *Autopoiesis*[26]. Jede Operation, die einem autopoietischen System bei der Konstruktion von Anschlusskommunikation dienlich ist und dem Metasystem Gesellschaft letztendlich seine Form gibt, wird immer wieder von neuem auf ihre Wirksamkeit geprüft.[27] Diese Prüfung hat nun bereits in umfangreicher Form bei Social Bots stattgefunden. Die algorithmisierten Programme von Social Bots versprechen neue Formen operationalisierter Problemlösungen und eine verstärkte Unsicherheitsabsorption. Sie verändern beispielsweise durch das massenhafte Erstellen und Adressieren von Meinungsumfragen die kommunikativ erzeugte Form der öffentlichen Meinung; sie legen mit gezielten Werbemaßnahmen entsprechend der Analyse persönlicher Zahlungsbereitschaften der Menschen die Partizipationsvoraussetzungen für den Markt über das Medium Geld neu fest; und sie erweitern durch das Speichern, Ordnen und Verbreiten digitaler Wissensbestände die Möglichkeiten der Überprüfbarkeit von Theorien durch die Kommunikation wissenschaftlicher Wahrheit. Aufgrund dieser Popularität und den zahlreichen Einsatzmöglichkeiten kann – unter der weiteren Berücksichtigung des systemtheoretischen Abstraktionsgrades – die kommunikative Leistung jeglicher Bot-Technologien innerhalb der Funktionssysteme als eine maßgebliche soziale Bedingung der Umweltbeobachtung beschrieben werden.[28] In dieser dargelegten Form ist der Einsatz von Social Bots als Risiko auszuweisen, da die Funktionssysteme sich eigenständig zum Einsatz der Technologie aus spezifischen Gründen und unter vorgefundenen Bedingungen entschieden haben. Diesen Umgang mit neuen Technologien weist Luhmann dem Bereich gesellschaftlicher Errungenschaften zu, die dazu führen, dass auch die Systemautonomien mitunter neu austangiert werden müssen und keine Normierung stattfindet. Hier entstehe »ein gewisses Maß der systemeigenen Kontrolle über die Außenbeziehungen […] mit der Umformung von Risiken der Ausdifferenzierung in Risiken der Technik«[29]. Neben dieser funktionsbedingten Zurechenbarkeit und innersystemischen Legitimation hat die Menge an Social Bots, die mittlerweile in SNSs zu finden sind,[30]

25 Luhmann 1995: S. 56.

26 Der Begriff wurde von den beiden Biologen und Neurowissenschaftlern Humberto Maturana und Francisco Varela geprägt, auf die sich Luhmann in seiner Theorie bezieht (ausführlich dazu Luhmann 1993: S. 34-70).

27 Vgl. Luhmann 1993: S. 78-80.

28 Vgl. Luhmann 1998: S. 75.

29 Luhmann 2015: S. 528.

30 Einer Studie aus den USA zur Identifikation von Social Bots im SNS Twitter zufolge beläuft sich der Bestand an Accounts, die einem Bot zugeordnet werden können, bereits auf 9-15 %. Der signifikante Unterschied in den Prozentzahlen sei auf die bereits sehr ausgereifte Bot-Technologie und der Fehleranfälligkeit der menschlichen Kontrollpersonen zurückzuführen (vgl. Varol u.a. 2017: S. 285).

in den letzten Jahren aber auch aus anderen Gründen stark zugenommen; eine Entwicklung, die vor allem das gestiegene Gefahrenpotential aufzeigt.

2.2 Social Bots als gesellschaftliche Gefahr

Der einfache Zugang zu den notwendigen Softwareprogrammen befähigt mittlerweile einzelne Personen dazu, ganze Bot-Armeen zu konstruieren, die bei Bedarf in SNSs eingesetzt werden können.[31] Die anhaltende Veröffentlichung personenbezogener Daten, gepaart mit der Offenheit und Flexibilität digitaler Programmierschnittstellen (engl.: *application programming interface* (API)) in SNSs und der fortschreitenden Entwicklung von künstlicher Intelligenz tragen ebenfalls kontinuierlich zu der Verbreitung von Social Bots bei. Im Hinblick auf deren Einsatzgebiete sowie die intendierte Zielsetzung wird in aktuellen Diskursen mitunter zwischen *gutartigen* und *schadhaften* Social Bots unterschieden.[32] In den überkomplexen Zusammenhängen der digitalen Strukturen von SNSs, Webseiten oder Videospielen werden demnach gutartige Social Bots dazu eingesetzt, Inhalte nach bestimmten Vorgaben auszuwerten und für die Nutzer/innen aufzubereiten. Sie verbreiten im Namen von Unternehmen und Nachrichtenportalen aktuelle und journalistisch aufbereitete Informationen,[33] administrieren die Gespräche in Chaträumen und Foren oder sorgen als *non-player character* (NPC) für einen anhaltenden Spielfluss in Computerspielen. Diesen Kontexten ist gemeinsam, dass Social Bots stets auch als solche erkennbar sind und – was von zentraler Bedeutung ist – dort zu erwarten sind. Das Schadhafte der Social Bots lässt sich vor diesem Hintergrund in einem entsprechend breiten Rahmen dagegen so fixieren, dass sich deren Konstruktion und Programmierung der effektiven Vermeidung einer Identifikation als Bots verschrieben hat, weil durch die Imitation realer Personen die manipulative Wirksamkeit der Kommunikationen erhöht werden soll.[34] Diese Annahme kann mittels einer systemtheoretischen Abstraktion präzisiert werden: Als künstliche digitale Identitäten können Social Bots vorgeben, sich in der Umwelt der Gesellschaft aufzuhalten, um in der Form von Personen für Irritationen in Funktionssystemen zu sorgen. Diese Gefahr erweitert sich dabei

31 Vgl. Kind u.a. 2017: S. 36. Der Umfang und die Detailliertheit der Inhalte auf der Webseite www.botwiki.org stehen stellvertretend für die ubiquitäre und simplifizierte Nutzbarkeit von Social Bots im Internet. Auf der Seite finden sich neben zahlreichen ausführlichen Tutorials zur Erstellung von Bots auch Workarounds zu aktuellen Kontrollmechanismen und Zugangsbarrieren von SNSs sowie Links und Dokumente der aktiven Blogger/innen und Entwickler/innen-Community.

32 Vgl. Rosenbach/Traufetter 2017.

33 Im öffentlich-rechtlichen Rundfunk in Deutschland wird etwa der *newsbot Novi* zur Nachrichtendistribution eingesetzt (vgl. Tagesschau 2018).

34 Vgl. Angwin 2016.

parallel zum oben erwähnten Bestreben der Funktionssysteme und deren Teilsysteme, Risiken durch algorithmische Berechnungen zu minimieren, da dadurch immer mehr *feste Kopplungen* zu anderen Systemen hergestellt werden.[35] Social Bots sind hierbei eindeutig als Gefahr auszuweisen, da die Entscheidung zum Einsatz der Technologie in dieser Form aus der Umwelt der Gesellschaft heraus getroffen wird. Die Erwartungen, die einzelne Systeme aktuell an diese Art Gefahren richten können, erschöpfen sich in der Auswertung empirischer Daten mit Bezug zur netzkulturellen Kommunikationspraxis und in der Analyse etwaiger disruptiver Ereignisse, von denen eingangs einige Erwähnung fanden. Damit ein effektiver und zukunftsgerichteter Umgang mit diesen Gefahren überhaupt möglich wird, müssen neue Erwartungsstrukturen gebildet werden, die sich an soziale Gesetzmäßigkeiten der SNSs anpassen: »Unsicherheitsabsorption läuft über die Stabilisierung von Erwartungen«[36]. In diesem Bestreben entwickeln Systeme eine besonders sensible Umweltbezogenheit und sind umso mehr auf die Leistung eines bestimmten Funktionssystems angewiesen, das die thematische Grundstruktur gesellschaftlicher Kommunikation legt, in der Realitäten immer wieder neu verhandelt werden.

2.3 Sicherung des Gesellschaftsgedächtnisses im Medium der öffentlichen Meinung

Nach Luhmann übernimmt das System der Massenmedien in der beschriebenen, ausdifferenzierten Gesellschaftsform die Funktion, einzelne kommunizierte Meinungen von Personen zu jedweden verfügbaren *Themen* zu bündeln und der Öffentlichkeit über verschiedene Verbreitungsmedien zugänglich zu machen. Indem das System soziale Tatsachen aus Interaktionen selektiv aufgreift und in die Gesellschaft spiegelt, erbringt es für andere soziale Systeme die Leistung, die öffentliche Meinung zu produzieren und laufend in Form eines Gedächtnisses zu reproduzieren,[37] wodurch die Gesellschaft ihre kommunikative Struktur und Ordnung gewinnt: »Interaktionen sind Episoden des Gesellschaftsvollzugs.«[38] Die gekoppelten Meinungen bilden jeweils eigene Quantitäten und Sachzusammenhänge zu Themenkomplexen, mit denen sich zukünftig aktualisierte Gesellschaften und deren Teilsysteme – an vergangene Zustände erinnernd – immer wieder neu auseinanderzusetzen haben. Nach Luhmann ist diese Form der Beobachtung kontingent, da grundsätzlich das, was als *die* öffentliche Meinung zu bestimmten Themen wahrgenommen wird, auch von den personellen und sozialen Bedingun-

35 Vgl. Luhmann 2015: S. 525. Mehr dazu in Abschnitt 2.5.

36 Luhmann 1993: S. 158.

37 Vgl. Luhmann 2017: S. 9-11.

38 Luhmann 1993: S. 553.

gen der Beobachter/innen abhängig ist, die in den nicht einsehbaren Bewusstseinsprozessen sinnhaft wirken und die kommunikative Wirklichkeit konstituieren.[39] Eine Störung oder Manipulation dieser gesellschaftlichen Struktur kann daher zu erheblichen Problemen in der Funktionalität einzelner Systeme und der politischen Meinungs- und Willensbildung führen, da Gesellschaftsmitglieder in ihrer personellen Eingebundenheit in Systeme davon ausgehen, mit den realen Tatsachen politischer, wirtschaftlicher oder wissenschaftlicher Entscheidungen konfrontiert zu werden und daran ihre eigenen sinnhaften Handlungsmöglichkeiten ermessen. Zur effektiven Einflussnahme auf die öffentliche Meinung müssen Themen geformt und durch verschiedene Selektionskriterien dem System der Massenmedien angeboten werden.[40] Allgemeine Bedingungen dafür ergeben sich aus der zeitlichen Abarbeitung und Erneuerung aktueller Informationsgehalte, aus quantitativen Bezügen zur Lebenswelt, wie Statistiken und Relationierungen sowie in verschiedenen Bereichen der Sozialdimension, in der ein Thema beispielsweise durch neue Konflikte genährt wird.[41] Nun hat die Digitalisierung gerade bei der Formbarkeit und Bündelung einzelner Themen und Meinungen neue Möglichkeiten offenbart, die durch den Einsatz von Social Bots in besonderer Weise ausgenutzt werden können. Die Annahme von Luhmann, dass die Massenmedien »[i]n der Kontrolle ihrer eigenen Selektivität […] autonom«[42] seien, hält der Modernisierungsdynamik der Digitalisierung nicht mehr stand. Social Bots sind imstande, die genannten Differenzierbarkeiten und Dimensionen durch einen massenhaften und fokussierten Einsatz zu aktivieren. Die Effektivität von Social Bots ist und bleibt jedoch notwendigerweise an das Medium der öffentlichen Meinung und dessen thematische Verarbeitung von Gesellschaftskommunikation gebunden. Von dort aus kann sich letztendlich ein Einfluss auf die autonome Meinungs- und Willensbildung der Menschen entwickeln.

2.4 Menschliche Sinnverarbeitung im Medium der öffentlichen Meinung

In einer ausdifferenzierten Gesellschaft dienen Themen sowohl Bewusstseinssystemen als auch sozialen Systemen dazu, Kommunikationszusammenhänge in Episoden zu ordnen, damit sich einzelne Beiträge und Operationen darauf bezie-

39 Dies verweist vor allem auf den systemtheoretischen Konstruktivismus, der Beobachtung als Operation der Erkenntnis festlegt und die Beobachtung der öffentlichen Meinung als eine Beobachtung zweiter Ordnung beschreibt, in der immer auch das mitbeobachtet wird, was der/die Beobachtete beobachtet respektive nicht beobachtet (ausführlich dazu Luhmann 2005: S. 31-57 und Luhmann 2017: S. 108-113).

40 Vgl. Luhmann 2015: S. 1101.

41 Vgl. Luhmann 2005: S. 168; Luhmann 2015: S. 1105.

42 Luhmann 2017: S. 37.

hen können.[43] Dabei bilde die öffentliche Meinung, so Luhmann, »ein Kommunikationsnetz ohne Anschlusszwang«[44], das *nicht* »an dem, was wirkliche Menschen wirklich denken«[45] orientiert sei. Sie formuliere also »keinen Konsens darüber, was die Gesellschaft ist oder sein soll«[46], sondern nur ein vorübergehendes Resultat von Kommunikationen. In dieser Vorstellung wird in der Öffentlichkeit, im Zusammenspiel mit privaten Gedanken und Meinungen, »[d]ie öffentliche Meinung als Paradox stilisiert, als die unsichtbare Macht des Sichtbaren«[47], die jeder Mensch in jede Alltagssituation miteinbringt und in Entscheidungen präsent macht. Einmal vom System der Massenmedien produziert, dient die öffentliche Meinung der Formung von Differenzen und Erwartungsstrukturen, in denen sich die Gesellschaft selbst beschreibt. In der anhaltenden Verfügbarkeit von Themen und der kommunikativen Auseinandersetzung mit diesen, in der Differenz Konsens/Dissens, entsteht dann erst eine Form sozialer Ordnung, von der alle Funktionssysteme gleichermaßen profitieren, weil persönliche Meinungen als für alle Beobachter/innen voraussetzbar in Entscheidungen einfließen und zu Erwartungen umgeformt werden können. In der autopoietischen Verarbeitung thematischer Differenzen vergewissert sich das Metasystem Gesellschaft seiner Autonomie, die sich als ein sozialer Wert systemischer Privatheit konstituiert. Dieser Wert projiziert sich dann über den freien Zugang zu gesellschaftlichen Themen und Meinungen ins Zwischenmenschliche. Letztendlich kann hier der soziale Wert von Privatheit jeweils individuell an der selbstbestimmten Entscheidung zur Inklusion in die Gesellschaft sowie der erfolgreichen kommunikativen Teilnahme an gesellschaftlichen Themen gemessen werden: »Privacy is needed to enable the individual to deliberate and establish his opinions.«[48] Diese neutrale Konzeption von Privatheit lässt sich auch auf andere Intimitätsgrade zwischenmenschlicher Beziehungen übertragen, die beispielsweise durch Liebe, Vertrauen und Freundschaft aufrechterhalten werden.[49] Hier wird eine Funktion von Privatheit deutlich, die letztendlich nicht durch eine Kontrolle oder eine perfekte Balance zwischen etwas Privatem und Öffentlichem, sondern lediglich über die Fähigkeit,

43 Vgl. Luhmann 2017: S. 21f.

44 Luhmann 2005: S. 165.

45 Luhmann 2005: S. 164.

46 Luhmann 2015: S. 1098f.

47 Luhmann 2017: S. 163.

48 Vgl. Gavison 1980: S. 450. Bemerkenswert ist hierbei auch die zeitliche Dimension. Privatheit dient dazu, zu entscheiden, *ob* und *wann* eine Meinung geäußert wird. »By providing a refuge, privacy enables individuals to disobey in private and thus acquire the strength to obey in public« (Gavison 1980: S. 448).

49 Gavison 1980: S. 421.

diese Differenz überhaupt zu verarbeiten, einen sozialen Wert generiert.[50] Hier gelingt die Übertragung des funktionsanalytischen Privatheitskonzepts auf die Systemautonomie und das Management von Abhängigkeiten der Systeme von ihrer Umwelt. Am Einfluss von Social Bots und deren immanenter algorithmischer Programmstruktur auf eine spezifische Form der öffentlichen Meinung als die »politiksysteminterne Umwelt politischer Organisationen und Interaktionen«[51] kann beispielhaft gezeigt werden, wie Systeme durch Umweltbeobachtungen und Neustrukturierungen versuchen, die eigene Systemautonomie aufrechtzuerhalten.

2.5 Festigung der Systemautonomie durch Erneuerung von Erwartungsstrukturen

Luhmann beschreibt die politisch relevante öffentliche Meinung als einen Spiegel, in dem sich das Politiksystem »ein Bild von den Grenzen der eigenen Handlungsmöglichkeiten«[52] machen kann. Diese Metaphorik transportiert äußerst treffend das Bestreben sozialer Systeme, der Gesellschaft ein sorgfältig ausgehandeltes Abbild der eigenen Funktionstüchtigkeit zu übermitteln, das den Erwartungen der Umwelt (in der sich wohlgemerkt alle Menschen aufhalten) entspricht. Wie dieses Bestreben beim Politiksystem beobachtet werden kann, zeigen zwei unterschiedliche Beispiele: Eine politische Partei, als Organisation im Politiksystem, stellt fest, dass sich eine derart große Anzahl künstlicher Identitäten in einem SNS aufhält, dass ein erhaltenes Verkaufsversprechen nicht mehr eingehalten werden kann; nämlich exakte und persönlichkeitsgetreue Abbilder reeller Nutzer/innen für eine soziodemografisch geplante Parteiwerbung bereitzustellen. Social Bots gefährden damit eine weitere Zusammenarbeit zwischen dem Serviceunternehmen und dieser Partei, die mit dem Fortführen politischer Kommunikation im Netzwerk schließlich das Risiko einginge, keine repräsentative öffentliche Meinung im Netzwerk vorzufinden. Der SNS kann die genannte Gefahr durch die Erhöhung von Zugangsbarrieren für Bots innerhalb der technologischen Netzwerkstruktur in ein Risiko umwandeln, um damit die Erwartung der Partei wieder erfüllen zu können.[53] Ebenso wie in dieser skizzierten strukturellen Kopplung

50 Gavison betont, dass auch Privatheit vor allem in einem Verhältnis (Luhmann würde hier sagen *in der Einheit der Differenz*) zu Formbeschreibungen sozialer Beziehungen, wie beispielsweise Freundschaft, Vertrauen oder Liebe, an Aussagekraft und Wert gewinnt (vgl. Gavison 1980: S. 446).

51 Luhmann 2017: S. 126.

52 Luhmann 2005: S. 172.

53 Kapitel 3 geht darauf ein, welche Werkzeuge dazu zur Verfügung stehen und welche Schwierigkeiten sich bei dieser Maßnahme ergeben können.

zwischen dem Wirtschafts- und dem Politiksystem ziehen auch Beobachtungen der öffentlichen Meinung im innerpolitischen Zusammenhang Anpassungen von Erwartungen nach sich: Einige politische Parteien in Deutschland verkündeten, im Wahlkampf zukünftig auf den Einsatz von Social Bots verzichten zu wollen – und sprachen sich gleichsam für ein umfassendes Verbot aus.[54] Aus funktional-analytischer Sicht zeugte diese Entscheidung jedoch keinesfalls nur von einer selbstreflexiven Auseinandersetzung mit der systeminternen – und vermeintlich gesellschaftsschädigenden – Wirkung der Social Bots. Hier lässt sich vielmehr eine Reaktion auf die gewandelte soziale Anerkennung der Technologie erkennen, die in der politisch relevanten öffentlichen Meinung beobachtet werden konnte. Das nichtöffentliche Risikokalkül der Parteien, also eine autopoietische, systemerhaltende Entscheidung, ergibt sich auch hier entlang der Gefahr eines drohenden Verlustes legitimierter Macht, da beim Thema Social Bots in der öffentlichen Meinung zunehmend Misstrauen und Widerstände zu beobachten sind und ein Absehen von der Nutzung der Technologie von den Wähler/n/innen zunehmend erwartet wird. Gleichzeitig darf hier bezüglich des Aufrufs zu einem *allgemeinen* Verbot von Social Bots spekuliert werden, dass sich die Parteien der innersystemisch positiven Wirkung der Technologie bewusst bleiben und daher keiner anderen Partei diesen Vorteil gewähren wollen. Es wird deutlich, warum Luhmann betont, dass die öffentliche Meinung gerade für die Politik einer »der wichtigsten Sensoren [ist], dessen Beobachtung die direkte Beobachtung der Umwelt ersetzt«[55] – politische Macht also in einem direkten themenspezifischen Zusammenhang zu dieser steht. In gleicher Weise stellt die öffentliche Meinung aber auch für andere Funktionssysteme eine beobachtbare Öffentlichkeit dar, in der politische Gesellschaftskommunikation mit jeweils eigener, codegeführter Relevanz gespiegelt wird. In diesem Modus der Beobachtung ist jedoch kein gesellschaftliches Handeln erkennbar, sondern er stellt an sich lediglich eine Erweiterung systeminterner Komplexität dar, mit der auf Umweltereignisse reagiert wird. Ein weiteres Beispiel verdeutlicht dies: Es kann zu weltweiten Irritationen im Wirtschaftssystems kommen, wenn Social Bots Falschinformationen in dessen Umwelt verbreiten und über die Aktivierung von Themen innerhalb der öffentlichen Meinung die sensiblen und überkomplexen Zusammenhänge des Aktienhandels, als eine Öffentlichkeit des Wirtschaftssystems, manipulieren. Mittlerweile werden Interaktionen und Nachrichten in SNSs umfassend von algorithmisierten Programmen ausgelesen, um diese nach marktrelevanten Informationen zu durchsuchen, auf die dann in Sekunden mit Aktienkäufen oder -verkäufen reagiert wird.[56] So führ-

54 Vgl. Reinsch 2016.

55 Luhmann 2005: S. 171.

56 »Bots can amplify the visibility of misleading information, while automatic trading system lack fact-checking capabilities« (Ferrara u.a. 2016: S. 99).

te in der Vergangenheit eine Falschinformation über einen vermeintlichen Terrorangriff auf das Weiße Haus in den USA aufgrund ihrer Verbreitung durch Social Bots in SNSs unmittelbar zu Reaktionen auf dem weltweiten Aktienmarkt.[57] In dieser Kollision algorithmisierter Prozesse über die strukturelle Kopplung zweier Öffentlichkeiten – der öffentlichen Meinung und dem Aktienmarkt – wurde dem Wirtschaftssystem eine Grenze der Zuträglichkeit von Bot-Technologien und den neukonstruierten festen Kopplungen zwischen den Systemen offenbart. Grundsätzlich versprechen sich soziale Systeme vom Einsatz algorithmisierter Elemente eine exaktere und effektivere Form der Beobachtung öffentlich verhandelter Themen in der Umwelt. Indem implementierte Elemente aus vergangenen Ereignissen erwartbare Entscheidungen anderer Systeme mit Relevanz für das Wirtschaftssystem errechnen, beispielsweise wie sich Märkte und Preise – oder hier politische Entscheidungsträger/innen – bei einem vermeintlichen Terrorangriff verhalten *würden*, soll Unsicherheit absorbiert werden. Dies lässt sich auch als Beobachtung zweiter Ordnung des Wirtschaftssystems beschreiben. Das System hat gelernt, dass das Politiksystem die öffentliche Meinung als eine wichtige Orientierungshilfe bei der Verteilung politischer Macht verwendet und richtet demnach in dem Bestreben, die eigene Variabilität und Elastizität zu steigern, auch die eigenen Operationen – mit politischer Sensibilität – danach aus. Die Kenntnis des Wirtschaftssystems über diese Mehrsystemzugehörigkeit der Ereignisse entspringt dem Gesellschaftsgedächtnis und bezeichnet eine erhöhte interne Komplexität des Funktionssystems,[58] die durch Algorithmisierung noch weiter ausgebaut und hypersensibilisiert wurde. Die technologische Struktur der SNSs und die Kenntnis über die Neustrukturierung von Erwartungen des Wirtschaftssystems, die sich durch die mehrmalige Antizipation politischer Kommunikation vollzog, rief ein neues Gefahrenpotential durch den Einsatz von Social Bots hervor, das sich im nicht realisierbaren Versuch verbirgt, die Differenz zwischen Kommunikation und Handlung algorithmisch aufzulösen. Menschliches Handeln allein, hier in Form einer politischen Person, kann nicht algorithmisch vorberechnet werden. Die Orientierung an der öffentlichen Meinung als vermittelndes Element von Kommunikation und Handlung eröffnet zwar einen gewissen Berechnungsspielraum, aber dieser ist nun einem immer größer werdenden Umwelteinfluss unterworfen, weshalb es zu weitreichenden Fehlkalkulationen und unerwarteten Ereignissen kommen kann. Am Beispiel des SNS Twitter soll nun gezeigt werden, wie die technologischen Strukturbedingungen und die netzkulturelle Kommunikationspraxis den Einfluss von Social Bots fördern und welches Widerstandspotential dort jeweils zu finden ist.

57 Vgl. Ferrara u.a. 2016: S. 98.

58 Vgl. Luhmann 2015: S. 753f.

3. Themengenese und Meinungsformung im SNS Twitter

Twitter fällt in die Definition eines Mikroblogging-Netzwerks.[59] Über Hashtags und Likes sowie über eine Retweet- und Kommentarfunktion werden auf Twitter interessengeleitete Diskussionen geführt, die aufgrund ihrer einfachen Zugänglichkeit zur Teilhabe motivieren. In den Hashtags werden aktuelle Ereignisse, bestimmte Handlungsaufforderungen, Missstände oder Feierlichkeiten sowie Diskussionen zu prominenten Personen oder Institutionen verfestigt und mit universeller kommunikativer Anschlussfähigkeit versehen. Die *like-* und *share*-Funktion sorgen zusätzlich für die Verbreitung und Gewichtung der medialen Beiträge, Nennungen und Fragen sowie weiterer Kommentare von Nutzer/innen und Institutionen. Für die Beteiligung an Diskussionen zu aktuellen Themen wird den Nutzer/n/innen, im Vergleich zu eher textbasierten SNSs wie beispielsweise Reddit oder Facebook, nur relativ wenig zeitliches Engagement abverlangt.[60] Die Themen, die anhand der aufgezählten Mechanismen das größte Engagement in der Netzgemeinde nach sich ziehen, werden im *trending topic*-Bereich des Newsfeeds angezeigt.[61] Twitter operiert somit als Formgeber einer digitalen öffentlichen Meinung über die Darstellung und die algorithmische Bündelung zahlreicher loser Tweets und Hashtags. Die episodenhaften Interaktionen bilden sich in einer binär-kodierten Kommunikationsform aus wechselseitigen und aggregierbaren Zustimmungen und Ablehnungen ab, wodurch es den Algorithmen der Social Bots besonders effektiv möglich ist, diese auszulesen.[62] Sie werten Profile aus, analysieren Kommunikationsmuster und schließen sich Interessengruppen, Gefolgschaften und Fangemeinden an. Dadurch erhalten sie Zugriff auf weitere Personen- und Metadaten und binden sich in immer weitreichendere Netzwerke ein. Diese neuartige Explizitheit der öffentlichen Meinung

59 Vgl. Marwick/Boyd 2011: S. 16f.

60 Das Zeichenlimit für die Kurznachrichten auf Twitter wurde Ende 2017 von 140 auf 280 erhöht. Das Unternehmen begründete diese Maßnahme damit, dass es dadurch einfacher werden würde, am Netzwerk zu partizipieren. Die Beschränkung auf 140 Zeichen führte laut einer internen Datenauswertung dazu, dass die Nutzer/innen, um im vorgegebenen Limit auch ihre Meinung oder Einstellung adäquat kundzutun, sehr viel Zeit mit Umformulierungen, Satzbau und dem Einfügen von Abkürzungen verbrachten (vgl. Rosen 2017).

61 Die genaue Berechnung eines *trending topic* auf Twitter ist von zahlreichen Faktoren abhängig und auf die Nutzer/innen (der genaue Name des Bereichs heißt *Trends for you*) zugeschnitten (eine Übersicht liefert Needle 2016). Freilich vollziehen sich die unzähligen Interaktionen auf Twitter nicht zwangsweise in Gesellschaftszusammenhängen – sie sind aber dennoch Formen verschriftlichter oder verbildlichter Meinungsäußerungen, die Sozialität konstituieren. »Die Interaktion vollzieht somit Gesellschaft dadurch, daß sie von der Notwendigkeit, Gesellschaft zu sein, befreit ist.« (Luhmann 1993: S. 553).

62 Vgl. Bollmer/Rodley 2017: S. 148.

im SNS Twitter zieht bedeutsame Konsequenzen für die gesellschaftliche Themengenese nach sich. Aufgrund der langzeitlichen Speicherung und der Verbreitung mobiler Endgeräte wird zum einen das Aufmerksamkeitsdefizit einzelner Personen sowie die Diskrepanz zwischen der »Lebensrhythmik und Nachrichtenrhythmik«[63] ausgehebelt, an die sich Tageszeitungen und Fernsehnachrichten noch zu halten haben. Zum anderen werden sowohl die Themenselektion als auch Themendispersion an mehreren Stellen grundlegend modifiziert, sodass die »Thematisierungsschwellen«[64] und zeitlichen Begrenzungen aus der analogen Vergangenheit des Systems der Massenmedien ihre Geltung verlieren. Dies hat zur Folge, dass gesellschaftliche Teilsysteme und auch einzelne Organisationen eine zentrale Gatekeeper-Funktion der massenmedialen Berichterstattung umgehen können, die sich letztendlich direkt auf die *Akzeptanz* verbreiteter Themen bezieht. Während das System der Massenmedien nach der Bekanntmachung und Verbreitung von Themen davon ausgehen kann, dass diese auch tatsächlich bekannt sind, war es anderen Funktionssystemen vor der Digitalisierung nur schwer möglich, einen derartigen Verbreitungsgrad eigener Themen zu erreichen.[65] Über den Einsatz von Social Bots gelingt es den Funktionssystemen nun, eigenständig Themen sachgemäß zu konstruieren und über SNSs wie Twitter in die Digitalität einzuspeisen oder dort bereits behandelte Themen in Echtzeit zu modifizieren; ein Phänomen, dass in der Netzkultur auch mit den Begriffen *astroturfing*[66] oder *Twitter bomb*[67] beschrieben wird. Zusätzlich sind die Social Bots dazu imstande, die Mechanismen zu beeinflussen, mit denen die Menschen und andere Institutionen auf Twitter ihre Meinungen zu einem Thema ausdrücken. In diesen digitalen Komponenten des Mediums der öffentlichen Meinung entwickeln Social Bots ihr größtes Gefahrenpotential, da, wie im Folgenden anhand einer netzwerktechni-

63 Luhmann 2005: S. 168.

64 Zu diesen gehören nach Luhmann beispielsweise »Obszönitäten, religiöse Gefühle oder Bekenntnisse oder überhaupt Konfliktstoff« (Luhmann 1993: S. 214).

65 Vgl. Luhmann 2017: S. 22. Die Webseite Botswatch, die sich auf die Identifikation von Bot-Tätigkeiten spezialisiert hat, macht regelmäßig auf eine Methode aufmerksam, nach der während Politiktalkshows im Fernsehen gleichzeitig massenhaft Social Bots auf Twitter aktiv sind, um die geführten Fernsehdebatten in der Digitalität zu manipulieren. So werden beispielsweise abweichende Themen in den *trending topics* kreiert oder bestimmten Kommentaren durch positive Bewertungen zur Prominenz verholfen, wodurch kritische Beiträge marginalisiert und etwaige Diskussionen im Keim erstickt werden. Eine spezielle Form dieser politischen Propaganda ist auch unter dem Begriff »Whataboutism« bekannt (ausführlich dazu Kasparov 2015).

66 *Astroturfing* (dt. Kunstrasenbewegung) beschreibt, in Anlehnung an den Begriff *Graswurzelbewegung*, die Praktik, einzelne Meinungen, zumeist von Organisationen oder kleineren Gemeinschaften, künstlich einer großen Interessengemeinschaft zuzuweisen und damit den Schein zu erwecken, die öffentliche Meinung zu repräsentieren (vgl. Stieglitz u.a. 2017: S. 381-382 und Ferrara u.a. 2016: S. 98).

67 Vgl. Ratkiewicz u.a. 2011: S. 298.

schen Unterscheidung zwischen *back-end* und *front-end* punktuell dargelegt wird, etwaige Zugriffsbarrieren und die Möglichkeiten zur Eindämmung und Kontrolle eines derartigen Fremdeinflusses im SNS Twitter entweder nur begrenzt zur Verfügung stehen oder lediglich Symptome behandeln.

3.1 Strukturelle Diskriminierungen im *back-end*

Insgesamt sind die Möglichkeiten des technologischen Widerstandes gegen unerwünschte Bot-Technologien begrenzt. Social Bots erhalten grundsätzlich über das *back-end* eines SNS Zugang zum Netzwerk. Im *back-end* befindet sich die für die Nutzer/innen intransparente technologische Systemstruktur der Webseite. Hier werden Schnittstellen für Werbetreibende und andere Drittanbieter vom SNS zur Verfügung gestellt. Der SNS Twitter hat besonders »nutzerfreundliche und hürdenfrei zugängliche APIs«[68], weshalb viele Entwickler/innen von Social Bots den Fokus auf diese Plattform gelegt haben. Wenn man nun vor diesem Hintergrund auf den Lösungsvorschlag verweist, dass digitale soziale Kontexte so existenzfeindlich wie möglich für Social Bots ausgestaltet sein müssten, sind daher schnell die SNSs als Hauptverantwortliche auszumachen. In der andauernden gesellschaftlichen Risikoabwicklung blieb vor diesem Hintergrund die Verbreitung schadhafter Social Bots auch nicht ohne Folgen und führte in einigen SNSs zu einem Reputationsverlust. In jüngster Vergangenheit konnten zahlreiche Austritte aus SNSs direkt mit dem angestiegenen Aufkommen von Social Bots in Verbindung gebracht werden.[69] Entschließt sich ein SNS nun aus diesem oder anderweitigen Gründen gegen Social Bots vorzugehen, greifen viele technologische Kontrollmechanismen das zentrale Problem jedoch nicht bei der Wurzel. Etwaige Gegenmaßnahmen befinden sich, ähnlich der Entwicklung von Spam-Filtern und Antivirensoftware, in einem asymmetrischen Verfolgungsverhältnis, weil sich »die technischen Möglichkeiten zur Enttarnung von Social Bots […] noch im Entwicklungsstadium«[70] befinden. Bei diesem Verfahren entstehen zudem zusätzliche Privatheitskonflikte, weil zunächst mehr Bots in das Netzwerk eingeschleust werden, wodurch der Schutz der Daten derjenigen Nutzer/innen weiter schwindet, deren Profile zum Zwecke der Enttarnung von Social Bots analysiert werden müssen.[71] Eine Applikation, die – dem genannten Umstand zum Trotz –

68 Kind u.a. 2017: S. 32.

69 Dass übermäßig eingesetzte Bot-Technologien in SNSs auch zu sinkenden Werbeeinnahmen führen können, zeigt eine US-amerikanische Studie aus dem Jahr 2017. So belief sich der monetäre Verlust der untersuchten Werbetreibenden im Geschäftsjahr 2016 auf 7,2 Mrd. US-Dollar und im darauffolgenden Jahr auf 6,5 Mrd. US-Dollar (vgl. ANA/White Ops, Inc. 2017: S. 7).

70 Kind u.a. 2017: S. 7.

71 Vgl. Kind u.a. 2017: S. 62.

bereits seit längerer Zeit eine automatisierte Enttarnmethode anbietet, ist BotOrNot.[72] Hier zeigt sich jedoch ebenfalls ein Indiz für die aktuelle Ineffizienz rein technologischer Kontrollmechanismen, weil diese Applikation vor allem als Kontrollinstrument für Entwickler/innen nicht zugelassener Bots dient. Anhand der Parameter auf der Webseite wird von diesen getestet, ob die eingesetzte Bot-Technologie bereits routinemäßig erkannt wird oder ob sich der Einsatz ohne weiteren Programmieraufwand fortführen lässt.[73] Um die Asymmetrie zwischen der Entwicklung und der Enttarnung von Bot-Technologien auszugleichen, wird vermehrt auf eine technische Lösung verwiesen, nach der Twitter den »Entwicklern von Enttarnungsmechanismen höhere API-Bandbreiten zur Verfügung stellen«[74] könnte, wodurch der Identifikationsprozess beschleunigt werde. Die Bereitschaft von Twitter könnte dahingehend durch einen Verifikationsprozess gesteigert werden, der einen Bot als gutartig – also eben ausnahmslos diesem Zweck dienlich – ausweist. Obwohl diese Form der Authentifizierung die Informationsasymmetrie zum Teil ausgliche, würde dies jedoch als Kontrollform wenig am technologischen Verfolgungsaspekt an sich ändern und weiterhin nur Symptome beseitigen, da keine Garantie für den Erfolg der erkennbaren Bots gegeben werden kann. Eine effektivere und tiefgreifende Maßnahme gegen den Einfluss von Social Bots leitete Twitter 2016 selbst ein.[75] Mit einer kategorialen Veränderung in den Kommentarspalten sorgte der SNS dafür, dass nicht mehr nur die Anzahl der Bewertungen und Interaktionen entscheidet, welche Kommentare prominenter im Newsfeed bzw. unter einem Post angezeigt werden. Damit war es den Social Bots nicht mehr möglich, allein durch Spamming die Diskussionen unter brisanten Themen zu verhindern.[76] In der systemtheoretischen Betrachtung wirkt sich diese Maßnahme positiv auf die Autonomie der Gesellschaft aus, da von den Bots mehr abverlangt wird, um an der thematischen Interaktionsstruktur teilzunehmen, wodurch das Kommunikationspotential realer Personen indirekt gestärkt wird. In der Erklärung zur Modifikation des Algorithmus' von Seiten des Unternehmens wird jedoch deutlich, dass auch hier wiederum neue Abhängigkeiten geschaffen werden und sich das Gefahrenpotential lediglich auf eine Sinn-

72 Der kostenlose Service www.botornot.co erreicht bei der Identifikation von Bots auf Twitter eine selbstproklamierte Trefferquote von 95 % (vgl. Kind u.a. 2017: S. 52). Bei der Anmeldung autorisiert man die App dazu, das eigene Twitterprofil sowie die Follower/innen und Textnachrichten auszulesen.

73 Vgl. Mønsted u.a. 2017: S. 9.

74 Kind u.a. 2017: S. 53.

75 Die Änderung wurde 2015 zunächst für die Desktop-Applikation eingeführt, bevor diese ein Jahr später auch für die mobile Version des SNS übernommen wurde (vgl. Matsakis 2017).

76 *Spambots* sind auf Twitter nicht erlaubt, da Bot-Technologien bestimmten »Automatisierungsregeln« unterliegen: »Du darfst keine automatisierten Tweets oder Direktnachrichten senden, die Spam darstellen, oder dich anderweitig an Spam-Aktivitäten beteiligen.« (Twitter 2017a).

ebene verlagert: Im eigenen Hilfebereich der Webseite schreibt das Unternehmen: »Die Antworten werden so gruppiert, dass wir dir den besten Inhalt und das, was dich wahrscheinlich am meisten interessiert, zuerst anzeigen.«[77] Durch die Verweise auf »besten Inhalt« oder »wahrscheinlich am meisten« verweist Twitter darauf, dass es bei der Auswahl derjenigen Meinungen und Beiträge, die einen offenen und wahrheitsbezogenen Austausch ermöglichen sollen, auf eigene Bewertungsstandards zurückgreift, die aus den gespeicherten Daten der Nutzer/innen generiert werden. An der selbstreflexiven Bewertung von Bot-Technologien ändert sich damit nichts, da hier lediglich eine algorithmische Ebene addiert wird. Gleichzeitig vollzieht sich hier eine intransparente Vorbewertung digitaler Diskurse, die im großen Maße der Kontrolle der Nutzer/innen entzogen ist. Dieser Umstand zog zahlreiche Proteste nach sich, die sich im Netzwerk entluden. Dem Unternehmen wurde mitunter vorgeworfen, durch diese intransparente Maßnahme die Meinungsfreiheit zu untergraben und der Zensur den Weg zu ebnen.[78]

3.2 Objektive Identitätskontrolle im *front-end*

Wie effizient Social Bots nach erfolgter Integration in den SNSs agieren können, hängt unter anderem von der Komplexität der Kommunikationsarchitektur im *front-end* ab. Dort befindet sich die für die Nutzer/innen sichtbare und bedienbare Oberflächenstruktur, in der die erwähnten klickbaren Funktionsbereiche und Symbole angeordnet sind. Im *front-end* finden sich die öffentlich sichtbaren Gemeinschaften und Interessengruppen zusammen, die an der Konstruktion der öffentlichen Meinung beteiligt sind. Auch hier ist Twitter der Arbeitsweise von Social Bots besonders zuträglich. Während beispielsweise auf Facebook Kontakte durch Einladungen bzw. Anfragen zustande kommen (Invitemodell), entstehen die Verbindungen auf Twitter durch ein gegenseitiges Folgen der jeweiligen Profile (Followermodell).[79] Aufgrund der universellen Beobachtbarkeit von Profilen können sich Social Bots daher grundsätzlich unbemerkt einer Gruppe anschließen und an Diskussionen teilnehmen. In Gemeinschaften, in denen menschliche Akteure bereits über einen längeren Zeitraum mit Social Bots interagieren, wird

77 Twitter 2017b.

78 Nach eigenen Angaben möchte Twitter dadurch Hate Speech entgegenwirken und eine Möglichkeit haben, gewaltverherrlichende Inhalte zu löschen und Accounts zu suspendieren. In Protesten verwiesen Nutzer/innen auf eine vermeintlich willkürliche und subjektive Auswahl entsprechender Inhalte (vgl. Flynn 2017).

79 Vgl. Kind u.a. 2017: S. 47-49; das *Followermodell* verändert zudem die Erwartungen an den Kommunikationsprozess im Netzwerk (vgl. Marwick/Boyd 2011: S. 117f.).

die Identifikation falscher Identitäten immer weiter erschwert.[80] So weisen mitunter eine auffällig hohe Frequenz an Tweets, starke Aktivitäten zu Nachtzeiten oder eine anhaltend schnelle Reaktionsgeschwindigkeit auf Nennungen oder Kommentare darauf hin, dass ein Profil softwaregesteuert ist. Hierbei handelt es sich jedoch lediglich um Indizien, die auch aus der netzkulturellen Logik heraus *falsche Positive* darstellen können und daher nicht als Gesetzmäßigkeiten zur Eindämmung von Social Bots dienen sollten.[81] Gleichzeitig führte der unkomplizierte Zugang zu persönlichen Informationen in der Vergangenheit zu einem hohen Aufkommen von *Fake*-Profilen und Identitätsdiebstählen (*nicknapping*)[82], dem mittlerweile durch institutionelle Hilfe und dem Einsatz verschiedener Formen von *captcha*[83] entgegengewirkt wird.[84] Social Bots werden zu einem großen Teil anhand von Daten aus gestohlenen Profilen konstruiert, um deren Glaubwürdigkeit und Authentizität zu erhöhen.[85] Diesem Umstand hat Twitter in der Vergangenheit mit einem Verifikationsprogramm entgegenwirken wollen.[86] Unter bestimmten Bedingungen bekamen auf diese Weise »Accounts […] von öffentli-

80 Vgl. Ferrara u.a. 2016: S. 100.

81 Im Zuge einer umfassenden Deaktivierung von Social Bot Accounts im SNS Instagram (*Instagram rapture*) warnten Expert/en/innen vor vorschnellen Schlüssen bei dieser Form der Identifikation von Social Bots, da sich dort das Verhalten von Nutzer/n/innen mittlerweile ohnehin als äußerst mechanisch und rational (»bot-like«) darstelle (Eordogh 2015).

82 *Nicknapping* ist ein Scheinanglizismus, bestehend aus den englischen Begriffen für Pseudonym (*nickname*) und Entführung (*kidnapping*).

83 Captcha gehören zu den *challenge-response-tests*, mit denen Authentifizierungsverfahren im Internet durchgeführt werden. Durch eine Aufgabe, die auf den *Turing Test* zurückgeht, sollen reale Nutzer/innen von Computeralgorithmen unterschieden werden.

84 In Deutschland führte der Anstieg der Identitätsdiebstähle in der Digitalität dazu, dass das deutsche Auskunftunternehmen SCHUFA die Kategorie »Identitätsbetrugsopfer« in die interne Kartei aufnahm. Cyberkriminelle bedienen sich anderer – vermehrt prominenter – Identitäten, um beispielsweise eine große Gefolgschaft in SNSs aufzubauen oder bei Onlinehändlern auf deren Rechnung einzukaufen (vgl. Toller 2016).

85 So wurden Identitätsdiebstähle von mehr als 100.000 Profilen entdeckt, als eine Diskussion über die Abschaffung der Netzneutralität in den USA von der Federal Communications Commission (FCC) angestoßen wurde. Eine tatsächliche Diskussion kam im Internet nicht zustande, da die Meinungen realer Nutzer/innen im Kommentar-*spam* der Social Bots untergingen (siehe auch hier Kasparov 2015). »[W]hile some of these fake comments used made-up names and addresses, many misused the real names and addresses of actual people as part of the effort to undermine the integrity of the comment process.« (Schneiderman 2017).

86 Über ein Formular war es ab Mitte 2009 möglich, einen Antrag auf eine symbolische Verifikation zu stellen. Damit reagierte das Unternehmen vor allem auf mehrere Beschwerden prominenter Personen, die von zahlreichen Fake-Profilen mit ihrem Namen berichteten (vgl. Kanalley 2013). Auch Facebook führte im November 2016 ein vergleichbares Verifikationsverfahren ein (vgl. Facebook o. J).

chem Interesse«[87] ein symbolisches Identifikationsattribut neben dem Profilnamen (einen weißen Haken auf blauem Grund). Dies führte letztendlich zu einem Ereignis, das ein grundsätzliches Problem mit Verifikationsmechanismen in der Digitalität offenlegt und eine individuelle, gesellschaftliche Verantwortungsebene innerhalb der öffentlichen Meinung eröffnet. Das Unternehmen sah sich Anfeindungen ausgesetzt, als mehreren Personen die Verifikation zuteilwurde, die lediglich durch rechtsradikale Äußerungen oder kriminelle Handlungen in das Interesse der Öffentlichkeit gelangt seien.[88] Twitter stellte die Vergabe der Symbole unter folgender Begründung ein:

> We are conducting an initial review of verified accounts and will remove verification from accounts whose behavior does not fall within these new guidelines. We will continue to review and take action as we work towards a new program we are proud of.[89]

Legt man hier den Fokus auf die institutionelle Ebene, in der sich die Problematiken aus dem *back-end* und *front-end* letztendlich überschneiden, ist zu erkennen, wie stark die Identifikation einer Person an den Unternehmenswerten (*guidelines*) und den normativen Standards des Netzwerks Twitter orientiert ist. Der Hinweis von Twitter verweist auf die eingangs erwähnte innersystemische Legitimation integrierter Elemente, die hier beispielsweise an der wirtschaftlichen Operationalität des SNS orientiert ist. Vergleichbares zeigt sich auch in anderen SNSs und den Methoden der Drittanbieter, die sich der Enttarnung von Social Bots widmen. Die öffentlich einsehbaren Informationen und das Kommunikationsverhalten der Nutzer/innen werden von Algorithmen ausgelesen, die sich anhand einprogrammierter Zahlenwerte entscheiden, ob ein Profil als Social Bot eingestuft wird oder nicht.[90] Der Algorithmus des SNS YouTube schließt Videos aus der netzinternen Monetarisierung aus, die sich nicht an die Unternehmensrichtlinien

87 »Ein Account kann verifiziert werden, wenn festgestellt wird, dass er von öffentlichem Interesse ist. Dies sind in der Regel Accounts von Nutzern, die in den Bereichen Musik, Film, Mode, Regierung, Politik, Religion, Journalismus, Medien, Sport, Wirtschaft und anderen wichtigen Interessensbereichen tätig sind.« (Twitter o. J).

88 Twitter hatte beispielsweise das Profil von Jason Kessler verifiziert, der als Organisator der Demonstrationen in der US-amerikanischen Stadt Charlottesville im August 2017 mediale Bekanntheit erlangte (vgl. Flynn 2017).

89 Twitter 2017b. Twitter stellt zudem eine Beschwerdeplattform bereit, auf der sich Nutzer/innen zu ihren Inhalten äußern können, aufgrund derer sie aus dem Netzwerk verbannt wurden (vgl. Flynn 2017).

90 Die Webseite *Botswatch* verwendet Kategorien zur Unterscheidung von Menschen und Bots, die sich auf empirische Beobachtungen von Studien aus den USA stützen. So werden beispielsweise Twitter-Profile, die mehr als 50 Tweets am Tag absenden, automatisch als Bots ausgewiesen.

halten.[91] In gleicher Weise verfuhr auch Facebook, als sich das Unternehmen von menschlichen Editor/en/innen trennte und seitdem Algorithmen zur Identifikation von Social Bots und Fake News einsetzt.[92] Zudem macht der eingebaute Verifikationsmechanismus auf der personellen Ebene eine sichtbar subjektive und uneindeutige Unterscheidung, in der sich politische oder wirtschaftliche Interessen überschneiden.[93]

4. Social Bots als Gesellschaftsverantwortung

Aus beliebigen Themen können für alle Funktionssysteme durch den Einsatz von Social Bots Umweltereignisse generiert werden, da sich in der Digitalität mittlerweile eine algorithmisch einprogrammierte Erwartungsstruktur gebildet hat, die in den so eingegangenen festen Kopplungen neuartige kausale Reaktionen nach sich ziehen. Innerhalb dessen sind die Verantwortungsebenen systemindividuell verteilt und autonom organisiert, wodurch Social Bots grundsätzlich als Risiko wahrgenommen werden und das strukturelle Gefahrenpotential von den Systemen selbst nicht identifiziert wird. Die systemtheoretische Analyse machte deutlich, dass eine innersystemische Komplexitätserweiterung immer nur das Bestreben einzelner Systeme beschreiben kann, effektiver mit den Risiken einer ungewissen Zukunft umgehen zu können. Dies führt jedoch nicht zwangsweise dazu, dass auch das Gefahrenpotential, das mit den neuen Elementen und Verknüpfungen in der Umwelt der Systeme entsteht, jeweils erkannt, eingegrenzt oder sogar kontrolliert werden kann. Aufgrund der algorithmisierten Kopplungen konnte durch den gezielten Einsatz von Social Bots die zeitliche und sinnhafte (Re-)Produktion der öffentlichen Meinung und die Aufsicht über die thematische Grundstruktur der Gesellschaft dem Kontrollbereich des Systems der Massenmedien immer mehr entzogen werden. Erschwerend kommt hinzu, dass Social Bots auch jedes beliebige, bereits bestehende Thema mit einem Informationswert aufladen können und dadurch den Bewusstseinssystemen der Menschen über verschiedene Sinndimensionen künstlich erzeugte öffentliche Meinungen vermitteln können, anhand derer sich persönliche Erwartungsstrukturen

91 Der SNS YouTube kontrolliert die geteilten Inhalte im Netzwerk mittels Algorithmen im Hinblick auf die eigenen Unternehmensrichtlinien. »Today, 98 percent of the videos we remove for violent extremism are flagged by our machine-learning algorithms.« (Wojcicki 2017).

92 Vgl. Solon 2016.

93 Facebook unterscheidet zwischen einer »verifizierten Seite« und einem »verifizierten Profil«. Über ein blaues Symbol wird eine »Person des öffentlichen Lebens, [ein] Medienunternehmen oder [eine] Marke« verifiziert. Ist ein graues Symbol zu sehen, »bedeutet das, dass Facebook bestätigt hat, dass es sich um die echte Seite bzw. das echte Profil für dieses Unternehmen oder diese Organisation handelt« (Facebook o.J.).

bilden, die dann keinen Gegenwert in der Realität besitzen. Vor diesem Hintergrund sind grundlegende Anpassungen in der systemischen und menschlichen Identitätsarbeit notwendig. Das bedeutet, dass Funktionen neu ausgehandelt und dadurch Abhängigkeiten neu geordnet werden müssen. Nur so entwickeln sich Risiken, die letztendlich in einen autonom zu regelnden Verantwortungsbereich fallen. Beim System der Massenmedien zeigt sich dahingehend bereits eine solche Entwicklung: Journalistische Programme und Medieninstitutionen reagierten bisweilen mit einer Anpassung der eigenen Aufgabenbereiche auf den fortwährenden Verlust der zugeteilten Gesellschaftsfunktion, nämlich der eigenen Leitdifferenz entsprechend Informationen in Nichtinformationen zu prozessieren und kontinuierlich thematische Neuheiten und Ereignisse zu erzeugen. Die wachsende Reichweite von SNSs führte zu einer Unbeherrschbarkeit informationeller Neuigkeitswerte und verlagerte die funktionale Ausrichtung des Systems der Massenmedien von der Verarbeitung reiner Informationsinhalte hin zur Darstellung von Wahrheitsgehalten. Aus systemtheoretischer Sicht beschreibt diese Neuorientierung eine Umstellung von *Was*- auf *Wie*-Fragen – also auf eine Beobachtung zweiter Ordnung. Diese neu ausgehandelte Funktion verspricht äußerst stabilisierend für eine digitale Gesellschaft zu sein, in der es immer wichtiger wird, eine öffentliche Meinung zu immer größeren Themenkomplexen zu reproduzieren und nicht mehr nur über TV-Bildschirme und Zeitungen so schnell wie möglich eine rein technologisch vermittelte Wirklichkeit zu repräsentieren. Damit geht das System der Massenmedien nicht mehr nur der Frage nach, was die öffentliche Meinung ist, sondern vor allem *wie* diese gebildet wird. Durch eine auf diese Weise verstärkte Objektivität und vergrößerte Distanz zur gesellschaftlichen Themenstruktur erbringt das System wieder die durch andere Funktionssysteme vorgeschriebene Leistung, die sich letztendlich in einer funktionierenden demokratischen Gesellschaftsstruktur niederschlägt:

> Denn nur dann, wenn die öffentliche Meinung mehr bietet als nur ein zentralisiertes Echo politischer Aktivität, kann sich eine Politik entwickeln, die sich nicht nur als durchgesetzte Identität behauptet, sondern sich erst auf der Ebene des Beobachtens von Beobachtern schließt.[94]

Neben dieser strukturellen Anpassung, die, wie bei der Verkettung von Umweltereignissen gezeigt, zunehmend auch auf andere Systeme einwirken wird, besteht jedoch noch eine zusätzliche Herausforderung, die auf die unabgeschlossene Anpassung menschlicher Identitätsarbeit an die Digitalität verweist. Die Eigenheiten digitaler Sozialität, die pseudonymisierte Kommunikationspraxis und die netzkulturelle Konstruktion der öffentlichen Meinung begründen

94 Luhmann 2005: S. 173.

schließlich die Idee, den Sinn und den Einflussreichtum von Social Bots in besonderer Weise: Angefangen bei der Menge an Follower/n/innen, über die Anzahl an Likes und Kommentaren zu veröffentlichten Meinungen und Informationen bis hin zur technologisch erzeugten Qualität des Profilfotos werden alle Bewertungen mit sinnorientierten Motiven einer Person in Verbindung gebracht, da diese Elemente bislang als einzige, wirklich wirksame identitätsstiftende Werkzeuge zur Verfügung stehen. In der Konsequenz bedeutet dies, dass jedes einzelne Like als Persönlichkeitskomponente unmittelbar in das Medium der öffentlichen Meinung einfließt, über das letztendlich Social Bots ihren manipulativen Einfluss ausüben. *Nicknapping* und die Imitation realer Personen gelingen nur deshalb so effektiv, da sich die Programme dieser ohnehin nur schemenhaften und oberflächlichen Selbstdarstellung und Fremdbewertung in SNSs angleichen müssen. Die digitale Sozialität und die personelle Privatheit sind in der identitätsstiftenden Profilierung derart schwach ausgeprägt, dass einige wenige Kommunikationsakte genügen, um soziale Kontrollmechanismen auszuhebeln und Gemeinschaft zu erzeugen.[95] Vor diesem Hintergrund macht gerade die Brisanz gesellschaftlich polarisierender Themen die Identifikation von Social Bots im Zwischenmenschlichen ebenso notwendig wie unwahrscheinlich, weil bei der Verifikation von Profilen, denen eine Meinung zugewiesen wird, in der Digitalität keine Unterscheidung zwischen einer personalen Identität und einem beobachteten Verhalten gemacht wird. Diese fehlende Fähigkeit zur Differenzierung lässt alle selbstreferentiellen Versuche der Identitätskonstruktion scheitern und entledigt konfliktbereinigenden Gesellschaftskomponenten wie Toleranz, Vertrauen und Empathie in der Digitalität zunehmend ihrer sozialen Bindungskraft.[96] Vor diesem Hintergrund entwickelte sich die Vergabe der Verifikationssymbole auf Twitter (und anderen SNSs) zwangsläufig als ein internetkultureller Top-down-Prozess, in dem nun unter anderem Prominenz und Wirtschaftskraft als Legitimationsmoment bevorzugt wird und der zur Identifikation von Social Bots notwendige Verifikationsprozess einer Privilegierung gleichkommt, anstatt als gesellschaftliche Notwendigkeit angesehen zu werden, durch die die demokratische Teilhabe und eine identitätsstiftende Meinungs- und Willensbildung gesichert werden soll. Da die Algorithmen der SNSs diese, durch Social Bots kompromittierte Kopplung übernehmen und auswerten, ist die Produktion der öffentlichen Meinung anfällig für rein quantitative Aufmerksamkeitsfaktoren sowie für selbstverstärkende Netzwerkerregungen und politische Propaganda. Den SNSs gelang es somit indirekt, das zentrale themengenerierende Gesell-

95 Auch wenn diese privatheitssensible Kontrollebene in der vorliegenden Arbeit nur marginal behandelt wurde, kann für den Schutz vor Identitätsdiebstahl auf einige Vorteile der Blockchain-Technologie verwiesen werden (ausführlich dazu Pinto 2018).

96 Zur Notwendigkeit von Differenzen bei der Identitätskonstruktion siehe Fußnote 19.

schaftsattribut ›öffentliches Interesse‹ für sich zu vereinnahmen. Die Entscheidung von Twitter, sich über eigene Normierungen aus der gesellschaftlichen Leistungsverantwortung zurückzuziehen und bei der Vergabe der Verifikationssymbole auf die wirtschaftliche Unternehmenstätigkeit zu verweisen, wird im Hinblick auf das destruktive Potential digitaler Protestbewegungen und etwaigen Imageschäden zwar nachvollziehbar, aber sie offenbart auch eine soziale Trägheit im Zuge disruptiver und dynamischer Modernisierungsprozesse, die die skizzierten institutionellen und zwischenmenschlichen Problemebenen zusammenführen: Eine rein unternehmerisch – oder auch politisch – motivierte Selektion von Meinungen, die Twitter und andere SNSs für Personen und Institutionen vornehmen, beschreibt ein Relikt aus der Zeit analoger systemischer Informationsverarbeitung, in welcher es tatsächlich private Interessen und Themen in regional und zeitlich abgrenzbaren Lebensbereichen gab, auf die sich Verbreitungsmedien aufgrund der begrenzten Ressourcen fokussieren mussten und deren Informationsgehalt mit der Zeit versiegte. In ähnlicher Weise verhält es sich mit persönlichen Meinungen, die jedem Menschen in der Digitalität in derart mannigfaltiger und ungefilterter Fülle begegnen, dass sich neue Kategorien und Hilfsmittel zur Einordnung, Verarbeitung und Gewichtung von Gründen und Ansichten herausbilden müssen. Die anhaltende Fülle von Einflüssen sorgt unter dem Druck der steigenden Individualisierung dafür, dass sich beispielsweise die Anzahl an Bewertungen und Follower/n/innen als meinungsgewichtende Elemente in der Digitalität verankern und tradierte Mechanismen zur Konstitution von Expert/en/innentum und legitimiertem Wissen, wie Erfahrung, Alter oder Ausbildung, mehr und mehr ersetzt. Beide Entwicklungen haben Einfluss auf die Autonomie sowohl psychischer als auch sozialer Systeme und beschreiben einen Anstieg der Umweltabhängigkeit bei der Handhabung gesellschaftlicher Themen. Wohlgemerkt verweist dieser Anstieg dabei lediglich auf die Notwendigkeit einer Neukalibrierung von Autonomie und damit auf einen Wert von Privatheit, der etwas ultimativ Schützenswertes im stetigen gesellschaftlichen Wandel beschreibt. Der Verlust von Privatheit zeigt sich hier dann beispielsweise in der Beziehung jedes einzelnen Menschen zum Wert freier Meinungs- und Willensbildung, die aus funktionsanalytischer Sicht wiederum über die autonome Operationalität des Systems der Massenmedien mit der Gesellschaft als Ganzes verbunden ist. Meinungen entstehen in ungestörten kommunikativen Auseinandersetzungen und exponieren sich in komplexer sinnhafter Weise aus dem Privaten ins Öffentliche. So wie sich dann im Medium der öffentlichen Meinung ein niemals versiegender Strom privater Interessen und Einstellungen kondensiert, so wird auch in den Newsfeeds der SNSs das digitale Gedächtnis einer Internetgesellschaft dokumentiert, aus dem sich realweltlicher Konsens und Dissens in allen gesellschaftlichen Teilbereichen ablesen lässt. Solange in dieser Struktur eine rein algorithmische Verbreitung und Hierarchisierung von Themen möglich ist, sind Social

Bots eine Gefahr für den Zufluss realitätsnaher, wahrheitsgetreuer und verlässlicher Informationen zu gesellschaftlich verhandelten Themen. Eine Hierarchisierung von Inhalten oder auch die Möglichkeit, eigene personelle Vorlieben in eine sinnhafte Vorselektion einbauen zu können, ist aufgrund der stetig ansteigenden Informationsflut und der damit einhergehenden Komplexität gesellschaftlicher Ereignisse grundsätzlich notwendig. Die Einstellungen, Programmierweisen und Auswertungen, die diese Vorselektion gewährleisten, müssen jedoch so objektiv und transparent wie möglich ausgestaltet sein, da adäquate Kriterien nicht von einem Funktionssystem alleine erstellt werden können, sondern der andauernden Prüfung und Gewährleistung der digitalen Gesellschaft bedürfen. Ein transparenter Verifikationsprozess digitaler Profile versetzt Social Bots als kontingenzlose Technologien in einen kalkulierbaren Risikobereich, dem die Systeme eigenständig und in autonomer Ausgestaltung begegnen können. Dort sind sie als intern eingebundene Programme erkennbar, die weiterhin wertvolle systemspezifische Aufgaben erledigen und auf diese Weise soziale Anerkennung finden. Die Kontrollmechanismen in den SNSs müssen im Bereich menschlicher Kontrolle sein, damit die algorithmischen Kausalitäten zwischen den Systemen unterbrochen werden, bevor sich ein zu großes Gefahrenpotential entwickeln kann. Nur wenn Social Bots nicht eigens dazu imstande sind, Ereignisse zu erzeugen, bleibt die Steuerung von Umweltabhängigkeit und damit die Aufrechterhaltung von Systemautonomie im Bereich der autopoietischen Operationalität der Gesellschaft. Menschen in Administrator/en/innenpositionen einzusetzen, ist riskant; Algorithmen zu vertrauen, ist gefährlich.

Literatur

ANA/White Ops, Inc. 2017: *Bot Baseline 2016-2017. Fraud in Digital Advertising*. URL: https://cdn2.hubspot.net/hubfs/3400937/White%20Papers/ANA_WO_Bot Baseline2016-2017.pdf?t=1508188810458&__hstc=&__hssc=&hsCtaTracking =abd901f1-8be1-4466-95f0-b741c1a814ec%7C6ddb32cc-c64c-4511-9f26-2aa6f-4bf511a (zuletzt abgerufen am: 15.03.2019).

Angwin, Julia 2016: *Make Algorithms Accountable*. In: *The New York Times*. 01.08.2016. URL: https://www.nytimes.com/2016/08/01/opinion/make-algorithms-accountable.html?_r=1 (zuletzt abgerufen am: 15.03.2019).

Bollmer, Grant/Rodley, Chris 2017: *Speculations on the sociality of socialbots*. In: Gehl, Robert W./Bakardjieva, Maria (Hg.): *Socialbots and their friends. Digital media and the automation of sociality*. New York, S. 147-163.

Dachwitz, Ingo u.a. 2018: *FAQ: Was wir über den Skandal um Facebook und Cambridge Analytica wissen*. In: *netzpolitik.org*. 21.03.2018. URL: https://netzpoli

tik.org/2018/cambridge-analytica-was-wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen/ (zuletzt abgerufen am: 15.03.2019).

Eordogh, Fruzsina 2015: *Inside an Instagram Bot Farm*. In: *Motherboard*. 10.08.2015. URL: https://motherboard.vice.com/en_us/article/4x3zy9/inside-an-instagram-bot-farm (zuletzt abgerufen am: 15.03.2019).

Facebook o.J.: *Was ist eine verifizierte Seite und ein verifiziertes Profil?* URL: https://de-de.facebook.com/help/196050490547892?helpref=popular_topics (zuletzt abgerufen am: 20.07.2018).

Ferrara, Emilio u.a. 2016: *The rise of social bots*. In: *Communications of the ACM*. 59.7., 2016, S. 96-104.

Flynn, Kerry 2017: *The ›Twitter Purge‹: Neo-Nazi reckoning has begun*. In: *Mashable*. 18.12.2017. URL: https://mashable.com/2017/12/18/twitter-purge-neo-nazi-reckoning-new-rules-hate-speech/?utm_cid=mash-com-fb-main-link#2afFibxTsSq1 (zuletzt abgerufen am: 15.03.2019).

Gavison, Ruth 1980: *Privacy and the Limits of Law*. In: *The Yale Law Journal*. 89.3., 1980, S. 421-471.

Grigonis, Hillary 2018: *9 things to know about Facebook privacy and Cambridge Analytica*. In: *Digital Trends*. 05.04.2018. URL: https://www.digitaltrends.com/social-media/what-facebook-users-should-know-about-cambridge-analytica-and-privacy/ (zuletzt abgerufen am: 15.03.2019).

Kanalley, Craig 2013: *Why Twitter Verifies Users: The History Behind the Blue Checkmark*. In: *HuffPost*. 03.12.2013 (zuletzt aktualisiert am 12.04.2013) URL: https://www.huffingtonpost.com/craig-kanalley/twitter-verified-accounts_b_2863282.html (zuletzt abgerufen am: 15.03.2019).

Kasparov, Garry 2015: *Winter Is Coming: Why Vladimir Putin and the Enemies of the Free World Must Be Stopped*. New York.

Kind, Sonja u.a. 2017: *TA-Vorstudie: Social Bots*. In: *TAB-Horizon-Scanning*. 3., 2017, S. 1-84.

Luhmann, Niklas 2017: *Die Realität der Massenmedien*. Wiesbaden 5. Aufl.

Luhmann, Niklas 2015: *Die Gesellschaft der Gesellschaft*. Frankfurt a.M. 9. Aufl.

Luhmann, Niklas 2005: *Soziologische Aufklärung 5. Konstruktivistische Perspektiven*. Wiesbaden 3. Aufl.

Luhmann, Niklas 1998: *Die Wissenschaft der Gesellschaft*. Frankfurt a.M. 3. Aufl.

Luhmann, Niklas 1995: *Soziologische Aufklärung 6. Die Soziologie und der Mensch*. Opladen 3. Aufl.

Luhmann, Niklas 1993: *Soziale Systeme. Grundriß einer allgemeinen Theorie*. Frankfurt a.M. 4. Aufl.

Marwick, Alice M./Boyd, Danah 2011: *I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience*. In: *New Media & Society*. 13.1., 2011, S. 114-133.

Matsakis, Louise 2017: *How Twitter defeated Trump's bot army*. In: *Mashable*. 02.02.2017. URL: https://mashable.com/2017/02/02/trump-bots-twitter-replies-change/?utm_cid=mash-com-fb-main-link#.pQ4V63gBkqS (zuletzt abgerufen am: 15.03.2019).

Mønsted, Bjarke u.a. 2017: *Evidence of complex contagion of information in social media. An experiment using Twitter bots*. In: *PLoS ONE*. 12.9., 2017, S. 1-12.

Needle, Sarah 2016: *How Does Twitter Decide What Is Trending?* In: *ReThink Media*. 13.07.2016. URL: https://rethinkmedia.org/blog/how-does-twitter-decide-what-trending (zuletzt abgerufen am: 15.03.2019).

Nissenbaum, Helen 2010: *Privacy in Context. Technology, Policy, and the Integrity of Social Life*. Stanford.

Pinto, Rohan 2018: *How Blockchain Can Solve Identity Management Problems*. In: *Forbes*. 27.07.2018. URL: https://www.forbes.com/sites/forbestechcouncil/2018/07/27/how-blockchain-can-solve-identity-management-problems/#32de6f6513f5 (zuletzt abgerufen am: 15.03.2019).

Ratkiewicz, Jacob u.a. 2011: *Detecting and Tracking Political Abuse in Social Media*. In: Adamic, Lada A. u.a. (Hg.): *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media*. Menlo Park, S. 297-304.

Regan, Priscilla M. 2015: *Privacy and the Common Good: Revisited*. In: Rössler, Beate/Mokrosinska, Dorota (Hg.): *Social Dimensions of Privacy. Interdisciplinary Perspectives*. Cambridge, S. 50-70.

Reinsch, Melanie 2016: *Social Bots: Parteien in Deutschland wollen auf technische Wahlkampfhelfer verzichten*. In: *Berliner Zeitung*. 13.12.2016. URL: https://www.berliner-zeitung.de/politik/social-bots-parteien-in-deutschland-wollen-auf-technische-wahlkampfhelfer-verzichten-25278052# (zuletzt abgerufen am: 15.03.2019).

Rössler, Beate 2001: *Der Wert des Privaten*. Frankfurt a.M.

Rosen, Aliza 2017: *Tweeting Made Easier*. In: *Twitter Blog*. 07.11.2017. URL: https://blog.twitter.com/official/en_us/topics/product/2017/tweetingmadeeasier.html (zuletzt abgerufen am: 15.03.2019).

Rosenbach, Marcel/Traufetter, Gerald 2017: *Betreiben von Social Bots soll unter Strafe stehen*. In: *SPIEGEL ONLINE*. 21.01.2017. URL: www.spiegel.de/netzwelt/netzpolitik/social-bots-laender-wollen-gegen-meinungsroboter-im-internet-vorgehen-a-1130937.html (zuletzt abgerufen am: 15.03.2019).

Schneiderman, Eric 2017: *An Open Letter to the FCC*. In: *Medium*. 21.11.2017. URL: https://medium.com/@AGSchneiderman/an-open-letter-to-the-fcc-b867a763850a (zuletzt abgerufen am: 15.03.2019).

Singer, Peter W./Brooking, Emerson T. 2018: *LikeWar: The Weaponization of Social Media*. Boston.

Solon, Olivia 2016: *In firing human editors, Facebook has lost the fight against fake news*. In: *The Guardian*. 29.08.2016. URL: https://www.theguardian.com/tech

nology/2016/aug/29/facebook-trending-news-editors-fake-news-stories (zuletzt abgerufen am: 15.03.2019).

Stieglitz, Stefan u.a. 2017: *Do Social Bots (Still) Act Different to Humans? – Comparing Metrics of Social Bots with Those of Humans*. In: Meiselwitz, Gabriele (Hg.): *Social Computing and Social Media. Human Behavior*. Cham, S. 379-395.

Tagesschau 2018: *Novi – Nachrichten im Chatformat*. URL: https://www.tagesschau.de/inland/novi-103.html (zuletzt abgerufen am: 15.03.2019).

Toller, Andreas 2016: *Neuer Schufa-Eintrag hilft gegen Identitätsklau*. In: *Wirtschafts-Woche*. 01.09.2016. URL: https://www.wiwo.de/finanzen/steuern-recht/betrug-im-internet-neuer-schufa-eintrag-hilft-gegen-identitaetsklau/14481964.html (zuletzt abgerufen am: 15.03.2019).

Twitter o.J.: *Informationen zu verifizierten Accounts*. URL: https://help.twitter.com/de/managing-your-account/about-twitter-verified-accounts (zuletzt abgerufen am: 22.01.2018).

Twitter 2017a: *Automatisierungsregeln*. URL: https://help.twitter.com/de/rules-and-policies/twitter-automation (zuletzt abgerufen am: 15.03.2019).

Twitter 2017b: *We are conducting an initial review of verified accounts*. URL: https://twitter.com/TwitterSupport/status/930926295034224641 (zuletzt abgerufen am: 15.03.2019).

Varol, Onur u.a. 2017: *Online Human-Bot Interactions: Detection, Estimation, and Characterization*. In: Ruths, Derek (Hg.): *Proceedings of the Eleventh International AAAI Conference on Web and Social Media*. Palo Alto, S. 280-289.

Wojcicki, Susan 2017: *Expanding our work against abuse of our platform*. In: *Youtube Official Blog*. 04.12.2017. URL: https://youtube.googleblog.com/2017/12/expanding-our-work-against-abuse-of-our.html (zuletzt abgerufen am: 15.03.2019).

Woolley, Samuel C./Howard, Philip N. 2017: *Computational Propaganda Worldwide: Executive Summary*. Working Paper No. 2017.11. Oxford. URL: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf (zuletzt abgerufen am: 15.03.2019).